Quelques revêtements définis sur $\mathbb{Q}$

Jean-Marc Couveignes*
Algorithmique Arithmétique Expérimentale, UMR 9936 CNRS
Université de Bordeaux

Résumé

Nous décrivons des familles de revêtements de la sphère moins trois points et nous étudions leurs propriétés. En particulier, nous en donnons une description topologique et un modèle algébrique. Ces revêtements fournissent une illustration non triviale du théorème de Belyi et de ses conséquences dans le cas simple des courbes de genre zéro. Nous exhibons des exemples de mauvaise réduction et d'obstruction à la descente pour un revêtement.

1 Introduction

On appelle *fonction de Belyi* une fonction algébrique f d'une courbe $\mathcal{C}$ lisse projective définie sur $\mathbb{C}$, à valeurs dans $\mathbb{P}_1$, non ramifiée en dehors de $\{0, 1, \infty\}$. La paire $(\mathcal{C}, f)$ est appelée *paire de Belyi*.

Deux paires de Belyi $(\mathcal{C}_i, f_i)$ pour $i \in \{1, 2\}$ sont dites isomorphes s'il existe un isomorphisme $i : \mathcal{C}_1 \to \mathcal{C}_2$ tel que $f_1 = f_2 \circ i$.

Si l'on considère la surface de Riemann $\mathcal{C}(\mathbb{C})$ associée à la courbe $\mathcal{C}$ on obtient un revêtement topologique $\mathcal{C}(\mathbb{C}) \to \mathbb{P}_1(\mathbb{C})$ ramifié au dessus de $\{0, 1, \infty\}$ induit par f.

À tout revêtement topologique de $\mathbb{P}_1$ ramifié au dessus de $\{0, 1, \infty\}$ on associe un graphe en prenant l'image réciproque du segment $[0, 1]$ de $\mathbb{P}_1$ par le revêtement. La donnée de ce graphe sur la surface de Riemann est équivalente à celle de la monodromie du revêtement. Elle en fournit une représentation commode (voir la section 3 de cet article et l'introduction de [20]).

Ainsi, partant d'une classe d'isomorphisme de paires de Belyi, on obtient un graphe sur une surface de Riemann. Un tel graphe est appelé un *dessin d'enfant* selon la terminologie de Grothendieck dans [25]. Pour une introduction à la théorie des dessins d'enfants voir [11, 20].

Il y a une correspondance biunivoque entre les dessins d'enfants et les classes d'isomorphismes de paires de Belyi.

Un dessin d'enfant peut donc être dénoté par une paire de Belyi (modèle algébrique) ou par une description combinatoire (monodromie ou graphe sur une surface de Riemann). C'est un problème difficile que de passer d'une représentation à une autre.

*Membre de l'Option Recherche du Corps des Ingénieurs de l'Armement

En général, connaissant la monodromie, on peut calculer un modèle algébrique au prix de gros efforts de calcul ([3, 37]). En sens inverse, partant d'une fonction de Belyi on peut numériquement *dessiner* le graphe préimage du ségment $[0, 1]$ sur la surface de Riemann associée mais il est difficile d'en déduire *rigoureusement* la monodromie.

On sait aussi qu'il est possible d'associer à un dessin un certain nombre d'invariants géométriques ou arithmétiques tels que la classe d'isomorphisme de la courbe qui le sous-tend, le corps des modules, les nombres premiers de mauvaise réduction etc. Il est intéressant de calculer ces invariants pour un grand nombre d'exemples afin de mieux comprendre leurs liens avec la combinatoire du dessin. On cherche donc à expliciter la correspondance *fonction de Belyi/dessin* pour des familles assez vastes de dessins. Malheureusement on ne connaît que peu de dessins explicitement (voir [8, 7]) et moins encore de familles. Les l-revêtements pour un entier premier l donné sont décrits dans [1, 2].

Dans cet article nous construisons une famille assez riche de revêtements de genre 0 de la sphère et nous calculons un modèle algébrique pour ces revêtements. Cela nous permet de fournir des exemples non triviaux de la correspondance entre fonctions de Belyi et dessins. Nous étudions les divers invariants associés à ces dessins et nous illustrons un certain nombre de phénomènes tels que l'opposition *corps des modules/corps de définition* ou encore la mauvaise réduction.

Dans la section suivante nous rappellerons quelques définitions. La troisième section décrit quelques familles de dessins connues, dues à Belyi et à d'autres. Dans la quatrième section on rappelle quelques propriétés des espaces de Hurwitz associés aux revêtements de la sphère moins quatre points. Le fait principal est énoncé dans la cinquième section. Les trois sections suivantes utilisent ce résultat pour illustrer divers phénomènes comme l'existence d'une fonction de Belyi sans automorphismes caractérisant une courbe à isomorphisme près (section 6), la mauvaise réduction des courbes (section 7), les obstructions à l'existence d'un modèle sur le corps des modules (section 8).

Enfin les sections neuf et dix contiennent la preuve des faits principaux.

Nous remercions Joseph Oesterlé pour ses conseils et ses commentaires et pour avoir attiré notre attention sur les questions abordées dans cet article. Les conseils du rapporteur, de Qing Liu et de Michel Matignon nous ont beaucoup aidé pour la rédaction de la section 7. Cette section a aussi bénéficié de la conversation de Frans Oort, Irène Bouw et Frits Beukers que nous remercions.

La construction principale de cet article a été présentée dans [16] et annoncée dans [15].

2 Rappels sur les revêtements de la sphère moins trois points

Nous commençons par quelques rappels de vocabulaire concernant les revêtements. Le lecteur doit prendre garde à la polysémie de certains termes tels que *corps de définition* ou *corps des modules*. Nous tachons pour notre part d'éviter toute équivoque en rappelant ci-dessous une terminologie précise que nous empruntons à divers auteurs tels que Oesterlé, Fried [21], Harbater [28], Malle et Matzat [32].

Le groupe des automorphismes de $\mathbb{C}$ agit sur les paires de Belyi par conjugaison des coefficients. Cette action est compatible avec la relation d'équivalence et définit une action de $Aut(\mathbb{C})$ sur les dessins. En fait, on montre que tout dessin a un nombre fini de conjugués et que tout dessin admet une paire de Belyi définie sur le sous-corps $\bar{\mathbb{Q}} \subset \mathbb{C}$. Ainsi, l'action de $Aut(\mathbb{C})$ se limite à une action de Γ, le groupe de Galois absolu de $\mathbb{Q}$.

Le stabilisateur $\Gamma_{\mathbf{D}}$ d'un dessin $\mathbf{D}$ dans Γ est appelé *groupe des modules* du dessin. Le sous corps $\mathbb{K}_{\mathbf{D}}$ de $\bar{\mathbb{Q}} \subset \mathbb{C}$ fixé par $\Gamma_{\mathbf{D}}$ est appelé *corps des modules* du dessin.

Le groupe d'automorphismes $Aut(\mathbf{D})$ d'un dessin $\mathbf{D}$ est le groupe d'automorphismes d'une paire de Belyi de ce dessin.

Si une paire de Belyi est définie sur un corps de nombres $\mathbb{K} \subset \mathbb{C}$ on dit que $\mathbb{K}$ est *un corps de définition* du dessin $\mathbf{D}$ associé. Tout corps de définition de $\mathbf{D}$ contient le corps des modules $\mathbb{K}_{\mathbf{D}}$. En fait, Coombes et Harbater ont prouvé dans [12] que le corps des modules est l'intersection de tous les corps de définition.

Si $Aut(\mathbf{D})$ est trivial, alors le corps des modules est un corps de définition. Plus précisément, il existe une unique $\mathbb{K}_{\mathbf{D}}$-classe d'équivalence de paires de Belyi associées à $\mathbf{D}$. C'est la descente de Weil, [41]. Plus généralement, on définit le *dessin réduit* $\mathbf{D}_0$ d'un dessin $\mathbf{D}$ comme le quotient de $\mathbf{D}$ par $Aut(\mathbf{D})$ et on montre ([4, 14, 18]) que le corps des modules de $\mathbf{D}$ est un corps de définition de son dessin réduit et qu'il existe une $\mathbb{K}_{\mathbf{D}}$-classe d'équivalence canonique de paires de Belyi $(\mathcal{C}(\mathbf{D}), f)$ associée à $\mathbf{D}_0$ vu comme dessin réduit de $\mathbf{D}$. Ici $\mathcal{C}(\mathbf{D})$ est une courbe bien définie à $\mathbb{K}_{\mathbf{D}}$-isomorphisme près.

Dans le cas d'un dessin de corps des modules $\mathbb{Q}$, on peut ainsi associer à $\mathbf{D}$ une $\mathbb{Q}$-classe d'isomorphisme de courbes lisses projectives. C'est la classe de la courbe $\mathcal{C}(\mathbf{D})$ portant le dessin réduit. En particulier, si $\mathbf{D}$ est sans automorphismes, c'est simplement la classe associée à un modèle défini sur $\mathbb{Q}$ du dessin $\mathbf{D}$.

Réciproquement, toute $\mathbb{Q}$-classe d'isomorphisme de courbes algébriques lisses projectives est obtenue ainsi. En effet, pour toute courbe lisse projective $\mathcal{C}$ définie sur $\mathbb{Q}$, il existe une fonction de Belyi sans automorphismes de $\mathcal{C}$ dans $\mathbb{P}_1$ et définie sur $\mathbb{Q}$. À cette fonction est associé un dessin et donc une décomposition cellulaire de la surface de Riemann sous-tendue par $\mathcal{C}$, caractéristiques de la classe de $\mathbb{Q}$-isomorphisme de $\mathcal{C}$.

La preuve que nous en donnons dans [15] ne fournit pas de procédé raisonnable pour construire une telle fonction explicitement. On aimerait pourtant disposer d'un grand nombre d'exemples non triviaux de la situation que nous venons de décrire. Nous avons donné dans [14] un premier exemple de dessin associé à la conique d'équation $x^2+y^2+z^2=0$ sur $\mathbb{Q}$. Nous proposons dans la section 5 une construction générique qui produira des dessins associés à toutes les coniques définies sur $\mathbb{Q}$.

3 Représentation de familles de dessins

Dans cette section nous illustrons la correspondance entre paires de Belyi et graphes sur des surfaces de Riemann à l'aide des polynômes de Belyi.

La démonstration du théorème de Belyi ([6]) repose en effet sur l'utilisation répétée d'une famille de dessins de genre 0. Pour présenter agréablement de telles familles, nous introduisons quelques conventions naturelles.

Le lecteur peut se reporter à l'introduction et au premier article de [20].

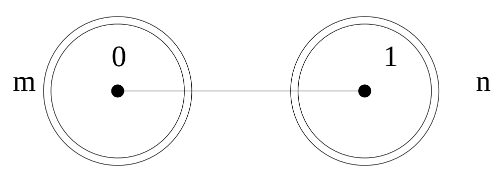
Nous considérons la famille des polynômes (de Belyi) indexés par deux entiers naturels positifs m et n

$$A_{m,n}(X) = (\frac{m}{m+n})^{-m}(\frac{n}{m+n})^{-n}X^m(1-X)^n.$$

On vérifie aisément que l'application correspondante est non ramifiée en dehors de $\{0,1,\infty\}$. Dans le cas $m=3$, $n=4$ on obtient le dessin suivant:

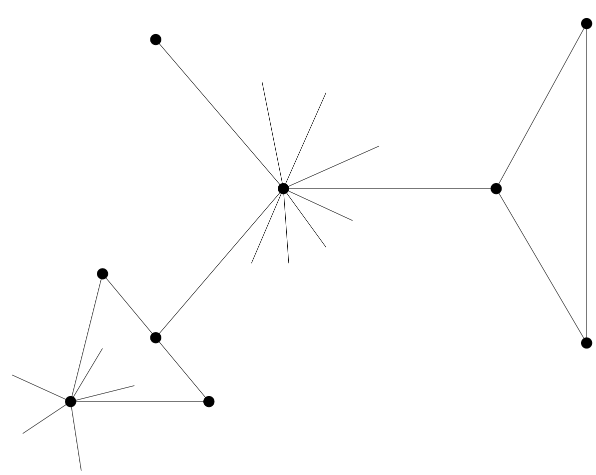
Observons que les points au dessus de 0 sont dénotés par des ronds noirs. Les points au dessus de 1 sont les 5 extrémités libres des segments (non ramifiés) ainsi que le point 3/7 sur le segment $[0,1]$, qui est ramifié d'ordre 2.

Nous dessinerons le cas général de la façon suivante.

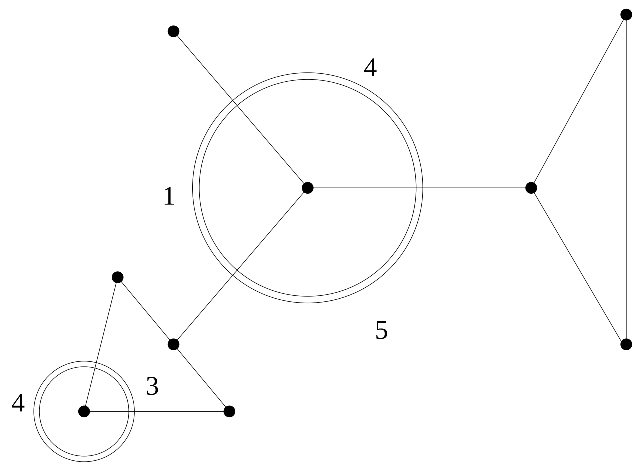


Ici, les doubles cercles autour de 0 et 1 remplacent $m-1$ et $n-1$ segments respectivement. Le m écrit près de 0 signifie que le secteur angulaire correspondant est découpé en m parties et donc qu'il y a $m-1$ segments issus de 0 (sans compter le segment $[0,1]$).

Nous donnons maintenant un exemple plus gratuit.



Avec les notations que nous venons d'introduire, ce dessin peut se représenter de la façon suivante.



L'usage de cette notation pour les multiplicités permet de *dessiner* des familles de revêtements.

4 Rappels sur les revêtements de la sphère moins quatre points

Dans cette section nous rappelons comment l'étude des revêtements de la sphère moins quatre points produit des revêtements de la sphère moins trois points. Pour une introduction à ces questions voir [21, 32].

Une première remarque concerne l'espace des modules des sphères moins n points $M_{0,n}$. L'application d'oubli d'un point $M_{0,n} \leftarrow M_{0,n+1}$ fait de $M_{0,n+1}$ la courbe universelle à n points marqués, comme fibré au dessus de $M_{0,n}$ (voir [23]).

Ainsi, un revêtement de la sphère moins $n+1$ points est un fibré au dessus d'un revêtement de $M_{0,n}$. En particulier, un revêtement de la sphère moins quatre points est fibré au dessus d'un revêtement de $M_{0,4} = \mathbb{P}_1 - \{0,1,\infty\}$ ([17]). C'est ce dernier revêtement qui nous intéresse. On peut le décrire aisément à partir de la théorie des tresses de Hurwitz.

En effet, considérons aussi les espaces de configurations naïfs $X_{0,n} = {\mathbb{P}_1}^n - \Delta_n$ où Δ_n est la variété discriminant. L'application "oubli" d'un point définit une fibration localement triviale $X_{0,n} \leftarrow X_{0,n+1}$. Un revêtement de la sphère moins $n+1$ points sera donné comme un revêtement de la courbe universelle $X_{0,n} \leftarrow X_{0,n+1}$ par une courbe $\mathcal{H} \leftarrow \mathcal{T}$

$$\begin{tikzcd}
\mathcal{H} \arrow[d, "\lambda"] & \mathcal{T} \arrow[l, "G"'] \arrow[d, "\phi"] \\
X_{0,n} & X_{0,n+1} \arrow[l]
\end{tikzcd}$$

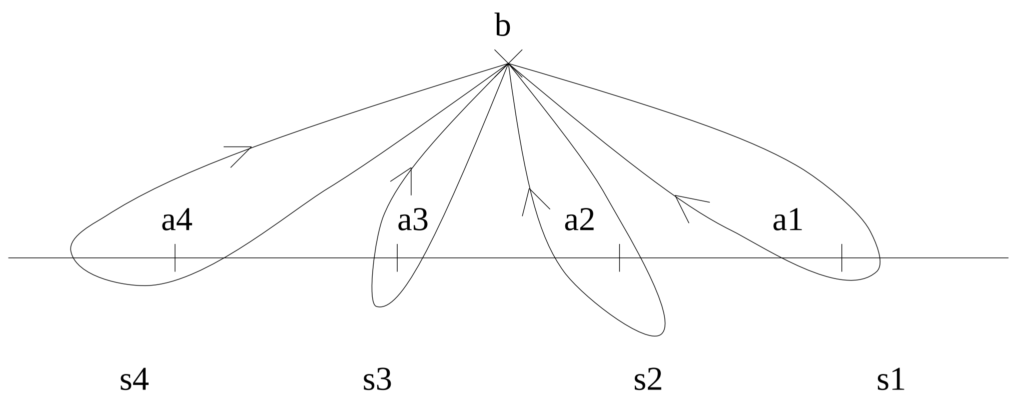
On dit que $\mathcal{H}$ est un espace de Hurwitz.

La séquence exacte d'homotopie ([9] page 14) associée à la fibration $X_{0,n} \leftarrow X_{0,n+1}$ induit une action du groupe fondamental de $X_{0,n}$ sur celui de la sphère moins n points à automorphismes intérieurs près. En fait, Artin a prouvé que la sequence exacte d'homotopie est scindée et que l'action induite est fidèle ([27] page

25). Cela implique que les revêtements de $X_{0,n}$ sont tous des espaces de Hurwitz de revêtements de $X_{0,n+1}$. Il est donc raisonnable de les décrire sous cette forme.

Nous décrivons plus explicitement l'action des tresses d'après Hurwitz. Supposons à nouveau que $n = 4$ et soit $A = (a_1, a_2, a_3, a_4)$ le point de $X_{0,4}$ correspondant à $\mathbb{P}_1(\mathbb{C}) - \{a_1, a_2, a_3, a_4\}$ où les a_i sont des nombres réels placés dans l'ordre décroissant.

Soit $R \in \lambda^{-1}(A)$ un point de $\mathcal{H}$ au dessus de A. On lui associe par restriction le revêtement $\phi : G^{-1}(R) \to \mathbb{P}_1(\mathbb{C}) - \{a_1, a_2, a_3, a_4\}$. Pour décrire ce dernier revêtement choisissons un point base b dans le demi-plan supérieur et la base (s_1, s_2, s_3, s_4) dessinée ci-dessous



Pour tout revêtement de $\mathbb{P}_1(\mathbb{C}) - \{a_1, a_2, a_3, a_4\}$, les s_i induisent des permutations $(\sigma_1, \sigma_2, \sigma_3, \sigma_4)$ de la fibre au dessus de b. On numérote arbitrairement les points de cette fibre et on obtient des permutations de S_D où D est le degré du revêtement ϕ. On a les relations

$$s_1 s_2 s_3 s_4 = 1,$$

et

$$\sigma_4 \sigma_3 \sigma_2 \sigma_1 = 1.$$

On remarque l'inversion de l'ordre des lettres: la composition des lacets se fait de gauche à droite et celle des permutations de droite à gauche.

Les quatre permutations σ_i caractérisent la classe d'isomorphisme topologique du revêtement. Il existe une correspondance biunivoque entre les revêtements de $\mathbb{P}_1(\mathbb{C}) - \{a_1, a_2, a_3, a_4\}$ à isomorphisme topologique près et les sous groupes d'indice fini de $\pi_1(\mathbb{P}_1(\mathbb{C}) - \{a_1, a_2, a_3, a_4\}, b)$ à automorphisme intérieur près.

Soient maintenant a_1', a_2', a_3', a_4' des points infiniment voisins des a_i. Il existe un isomorphisme canonique de $\pi_1(\mathbb{P}_1(\mathbb{C}) - \{a_1, a_2, a_3, a_4\}, b)$ dans $\pi_1(\mathbb{P}_1(\mathbb{C}) - \{a_1', a_2', a_3', a_4'\}, b)$ défini par élargissement des trous autour des a_i. Il existe donc une correspondance entre revêtements de ces deux espaces et on peut définir des revêtements voisins et des déformations de revêtements le long de chemins continus dans l'espace des sphères privées de quatre points distincts $X_{0,4} = \mathbb{P}_1^4 - \Delta$. On note $\mathcal{B}_{0,4}$ le π_1 de cet espace en prenant pour base le quadruplet $A = (a_1, a_2, a_3, a_4)$ choisi plus haut. Ce groupe est appelé groupe des tresses colorées à quatre brins. On définit trois tresses notées $t_{1,2}$, $t_{2,3}$, et $t_{3,4}$. Par exemple, $t_{1,2}$ est définie pour $u \in [0, 1]$ par

$t_{1,2}(0) = t_{1,2}(1) = (a_1, a_2, a_3, a_4)$ et les deux premiers points du quadruplet $t_{1,2}(u)$ tournent dans le sens des aiguilles d'une montre le long du cercle de diamètre $[a_1, a_2]$ soit

$$t_{1,2}(u) = (\frac{a_1 + a_2}{2} + \frac{a_1 - a_2}{2}e^{-2i\pi u}, \frac{a_1 + a_2}{2} - \frac{a_1 - a_2}{2}e^{-2i\pi u}, a_3, a_4).$$

Les trois tresses $t_{1,2}$, $t_{2,3}$ et $t_{3,4}$ engendrent $\mathcal{B}_{0,4}$.

Il a été observé par Hurwitz dans [30] que partant d'un revêtement de monodromie $(\sigma_1, \sigma_2, \sigma_3, \sigma_4)$ et appliquant la tresse $t_{1,2}$ on obtient un revêtement de monodromie $({}^{\sigma_2}\sigma_1, {}^{\sigma_2\sigma_1}\sigma_2, \sigma_3, \sigma_4)$. Ici la notation ${}^{a}b$ signifie aba^{-1}. Voir aussi [21, 32].

Supposons alors que les points de la fibre $\lambda^{-1}(A)$ correspondent à des revêtements de $\mathbb{P}_1(\mathbb{C}) - \{a_1, a_2, a_3, a_4\}$ deux à deux non isomorphes. Cette dernière condition est un critère de minimalité pour $\mathcal{H}$. Elle revient à dire que $\mathcal{H}$ est une plus petite base possible.

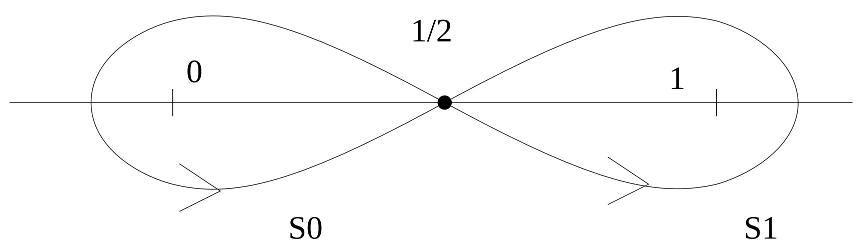
Alors la règle de Hurwitz décrite ci-dessus suffit à déterminer la monodromie de λ.

Pour finir notons que l'espace de configurations naïf $X_{0,4}$ est de dimension 4 alors que l'espace des modules $M_{0,4}$ est une courbe. En fait $M_{0,4}$ n'est autre que $\mathbb{P}_1 - \{0, 1, \infty\}$. On a une application de $X_{0,4}$ dans $M_{0,4}$ qui a (x, y, z, t) associe le birapport $[x, t, y, z] = (y - x)(z - t)/(y - t)(z - x)$ et il est naturel d'en chercher une section, ce qui revient à normaliser les quatre valeurs de ramification.

La section la plus simple est $I : \mathbb{P}_1(\mathbb{C}) - \{0, 1, \infty\} \to \mathbb{P}_1^4 - \Delta$ définie par $I(\lambda) = (\infty, 1, \lambda, 0)$.

On normalise le revêtement ϕ en restreignant λ à l'image de I. On obtient alors un revêtement $\lambda : \mathcal{C} \to \mathbb{P}_1(\mathbb{C}) - \{0, 1, \infty\}$ où $\mathcal{C}$ est une courbe

Pour calculer la monodromie de cette restriction considérons la base (S_0, S_1) suivante de $\pi_1(\mathbb{P}_1(\mathbb{C}) - \{0, 1, \infty\}, \frac{1}{2})$.



Soit $I^* : \pi_1(\mathbb{P}_1(\mathbb{C}) - \{0, 1, \infty\}, 1/2) \to \pi_1(\mathbb{P}_1^4 - \Delta, (\infty, 1, 1/2, 0))$ l'application induite par I sur les π_1. Alors on a trivialement,

$$\begin{aligned} I^*(S_0) &= t_{3,4}^{-1} = t_{1,2}^{-1} \\ I^*(S_1) &= t_{2,3}^{-1} \end{aligned}$$

et cela nous donne la monodromie recherchée.

5 Une famille de revêtements de genre 0

Venons en maintenant à notre construction. Nous décrirons d'abord une paire de Belyi $(\mathcal{C}_{m,n,p,q}, \lambda_{m,n,p,q})$ indexée par quatre paramètres entiers. Ensuite nous dessinerons le graphe associé. Enfin nous décrirons une autre famille de paires de Belyi $(\mathcal{K}_{m,n,p}, \nu_{m,n,p})$ et les dessins associés.

5.1 Fonctions de Belyi paramétrant des sphères moins quatre points avec multiplicités

Nous commençons par décrire des revêtements de la sphère ramifiés au dessus de quatre points.

Soient m, n, p, q quatre entiers relatifs deux à deux distincts, non nuls et de sommes non nulles (c'est à dire que la somme de tout ensemble non vide de ces nombres est non nulle). Soient a, b, c, d quatre indéterminées. Appelons $\mathcal{C}_{m,n,p,q}$ la courbe de $\mathbb{P}_3$ donnée par les équations

$$\begin{aligned} ma + nb + pc + qd &= 0 \qquad (1) \\ ma^2 + nb^2 + pc^2 + qd^2 &= 0 \qquad (2) \end{aligned}$$

Pour tout point $P = (a, b, c, d)$ de $\mathcal{C}_{m,n,p,q}$ on définit[1] ϕ_P la fraction rationnelle suivante

$$\phi_P(X) = (1 - aX)^m (1 - bX)^n (1 - cX)^p (1 - dX)^q.$$

La forme de ϕ_P et les équations 1 et 2 entraînent que $\phi_P(0) = 1$ et que ϕ_P est ramifiée d'ordre au moins 3 en $X = 0$. La fonction est peut être aussi ramifiée en $X = 1/a$, $1/b$, $1/c$, $1/d$ et ∞, ces points étant au dessus de 0 ou ∞. On obtient un autre point singulier en $X = \delta_P$ en dérivant ϕ_P

$$\delta_P = \frac{(n + p + q).a^{-1} + (m + p + q).b^{-1} + (m + n + q).c^{-1} + (m + n + p).d^{-1}}{(m + n + p + q)}.$$

Si les 7 valeurs a^{-1}, b^{-1}, c^{-1}, d^{-1}, ∞, 0, δ_P sont deux à deux distinctes, alors on dit que le point P est régulier. Dans ce cas, il n'y a pas d'autre point de ramification et l'indice de ramification en $X = 0$ est exactement 3 (formule de Hurwitz).

Le point δ_P est au dessus de $\phi_P(\delta_P) = \lambda_P = \lambda_{m,n,p,q}(P)$ et $\lambda_{m,n,p,q}$ définit une application de $\mathcal{C}_{m,n,p,q}$ dans $\mathbb{P}_1$.

Nous avons le

Fait 1 *Avec les notations ci-dessus la fonction $\lambda_{m,n,p,q} : \mathcal{C}_{m,n,p,q} \to \mathbb{P}_1$ est non ramifiée en dehors de $\{0, 1, \infty\}$.*

[1] à composition à droite près par une application linéaire $X \mapsto AX$

Nous observons que puisque m, n, p et q sont deux à deux distincts, si P et Q sont deux points réguliers distincts de $\mathcal{C}_{m,n,p,q}$, les revêtements ϕ_P et ϕ_Q ne sont pas isomorphes. En effet, deux revêtements isomorphes de $\mathbb{P}_1$ par $\mathbb{P}_1$ se correspondent à une homographie près (automorphisme de $\mathbb{P}_1$). Mais nous avons éliminé cette indétermination en normalisant selon les conditions que (i)-l'unique point de multiplicité $m+n+p+q$ soit en $X=\infty$ et (ii)-l'unique point de multiplicité 3 au dessus de 1 soit en $X=0$ et (iii)-l'unique point de multiplicité m au dessus de $\{0,\infty\}$ soit en $X=a^{-1}$. Cela signifie que $\mathcal{C}_{m,n,p,q}$ est bien la base minimale pour définir les ϕ_P. En particulier $\lambda_{m,n,p,q}$ est non ramifiée en dehors de $\{0,1,\infty\}$. □

Il reste à voir que $\lambda_{m,n,p,q}$ un revêtement sans automorphismes.

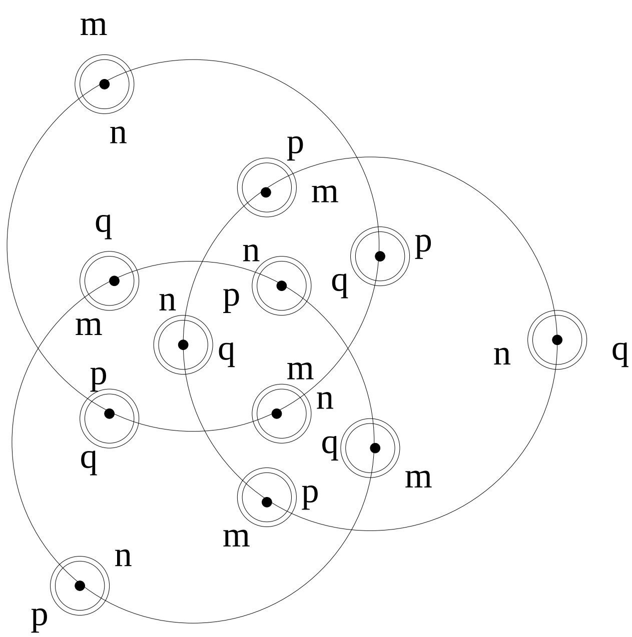
Pour cela, nous calculerons la monodromie de $\lambda_{m,n,p,q} : \mathcal{C}_{m,n,p,q} \to \mathbb{P}_1$ vu comme espace de Hurwitz du revêtement ϕ_P comme expliqué dans la section précédente.

Observons que dans [33] et [32] on trouve des critères de rigidité ou du moins de rationalité de l'espace de Hurwitz en vue de résoudre une instance du problème inverse de Galois. Ici, nous sommes au contraire intéressés par des espaces de Hurwitz non rationnels.

Afin d'exprimer simplement la monodromie des revêtements décrits ci-dessus nous présentons deux familles de dessins.

5.2 Le chardon, ou octaèdre fleuri

Soient m, n, p et q quatre entiers positifs. On note $\mathbf{D}_{m,n,p,q}$ le dessin suivant.



On remarque que les multiplicités au dessus de 0 sont les sommes de deux nombres distincts parmi m, n, p, q. Les multiplicités au dessus de ∞ sont les sommes de trois nombres distincts. Au dessus de 1 on trouve 6 points de multiplicité 4. Tous les autres points sont non-ramifiés. Au total, le degré du dessin est $6(m+n+p+q)$.

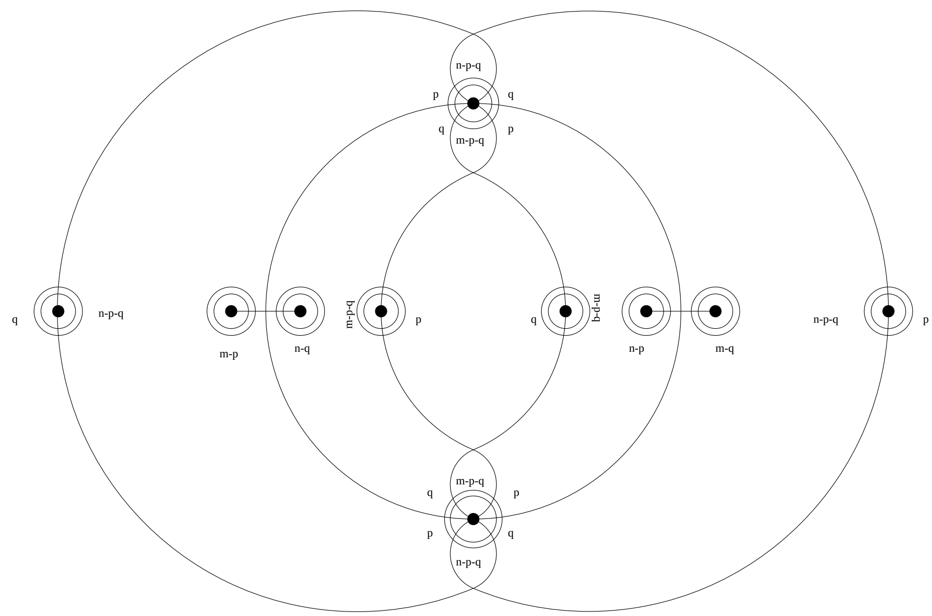
Nous énonçons le

Fait 2 *Soient m, n, p, q quatre entiers positifs deux à deux distincts. Alors la paire de Belyi $(\mathcal{C}_{m,n,p,q}, \lambda_{m,n,p,q})$ correspond au dessin $\mathbf{D}_{m,n,p,q}$ et ce dessin n'a pas d'automorphismes.*

Ce fait sera prouvé dans la section 9.

5.3 La pomme

Soient maintenant m, n, p, q quatre entiers positifs tels que $m > p+q$ et $n > p+q$. Supposons de plus que $m \neq n$ et $p \neq q$. Considérons le dessin $\mathbf{E}_{m,n,p,q}$ suivant



On observe que le degré de $\mathbf{E}_{m,n,p,q}$ est $6(m+n) - 4(p+q)$. Nous avons le

Fait 3 *La paire de Belyi $(\mathcal{C}_{m,n,-p,-q}, \lambda_{m,n,-p,-q})$ correspond au dessin $\mathbf{E}_{m,n,p,q}$ et ce dessin n'a pas d'automorphismes.*

Ce fait sera prouvé dans la section 10.

5.4 Le trièdre fleuri

Dans cette section nous décrivons une famille plus simple que la précédente. Elle ne sera utilisée qu'une fois dans la suite de cet article. Les preuves correspondantes ne seront pas données. Elles s'obtiennent aisément avec les méthodes de cet article.

Soient m, n, p trois entiers positifs deux à deux distincts. Soient a, b et c trois indéterminées. Appelons $\mathcal{K}_{m,n,p}$ la droite de $\mathbb{P}_2$ d'équation

$$ma + nb + pc = 0.$$

Pour tout point $P = (a, b, c)$ de $\mathcal{K}_{m,n,p}$ on définit, à composition à droite près par une application linéaire, le polynôme

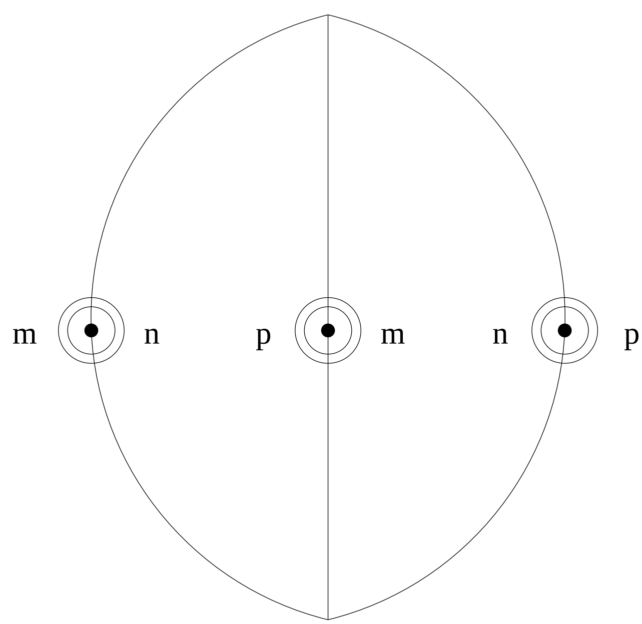
$$\psi_P(X) = (1 - aX)^m (1 - bX)^n (1 - cX)^p.$$

On a $\psi_P(0) = 1$ et ψ_P est ramifié d'ordre au moins deux en $X = 0$. Il peut être aussi ramifié en $1/a$, $1/b$, $1/c$ et ∞. Ces points sont au dessus de 0 et ∞. Il reste un dernier point de ramification obtenu en dérivant ψ_P

$$\kappa_P = \frac{(n+p).a^{-1} + (m+p).b^{-1} + (m+n).c^{-1}}{m+n+p}.$$

Ce point est au dessus de $\psi_P(\kappa_P) = \nu_{m,n,p}(P)$ et $\nu_{m,n,p}$ définit une fonction de $\mathcal{K}_{m,n,p}$ dans $\mathbb{P}_1$ non ramifiée en dehors de $\{0, 1, \infty\}$.

Cette fonction est sans automorphismes et elle est associée au dessin $\mathbf{U}_{m,n,p}$ suivant, de degré $2(m+n+p)$



Nous décrivons maintenant les fibres de $\nu_{m,n,p}$ au dessus de 0 et ∞.

Il existe un seul point $A_1 = (-p, -p, m+n)$ de $\mathcal{K}_{m,n,p}$ tel que $a = b$. De même, on définit $A_2 = (-n, m+p, -n)$ et $A_3 = (n+p, -m, -m)$. Les trois points A_1, A_2 et A_3 sont au dessus de 0 (exercice).

Il existe un seul point $B_1 = (-n, m, 0)$ de $\mathcal{K}_{m,n,p}$ tel que $c = 0$. De même, on définit $B_2 = (-p, 0, m)$ et $B_3 = (0, -p, n)$. Les trois points B_1, B_2 et B_3 sont au dessus de ∞ (exercice).

L'application qui envoie $P = (a, b, c)$ sur $r = a/c$ définit un isomorphisme entre $\mathcal{K}_{m,n,p}$ et $\mathbb{P}_1$. Les images des six points ci-dessus par cette bijection sont

$$(\frac{-p}{m+n}, 1, -\frac{n+p}{m}, \infty, -\frac{p}{m}, 0). \tag{3}$$

L'équation $\kappa_P = 0$ définit clairement les deux points singuliers au dessus de 1. Posant $r = a/c$, l'équation en r correspondante est

$$m(m+n)r^2 + 2mpr + p(n+p) = 0$$

de discriminant $-4mnp(m+n+p)$.

On appelle C_1 et C_2 les points de $\mathcal{K}_{m,n,p}$ correspondants. Il y a $2(m+n+p)-6$ points simples au dessus de 1. On les notes H_i pour $1 \leq i \leq 2(m+n+p)-6$.

6 Caractérisation des coniques par un revêtement

Comme on l'a rappelé dans l'introduction, à tout dessin est associée une courbe définie sur son corps des modules. Il est intéressant de chercher un exemple de cette situation pour toutes les coniques définies sur $\mathbb{Q}$. Toute conique est naturellement revêtement de la droite moins deux points mais ce revêtement est Galoisien et il a donc des automorphismes. En revanche les dessins construits ci-dessus sont dépourvus d'automorphismes. Cependant, il sont associés à des coniques $\mathcal{C}_{m,n,p,q}$ qui ne sont pas sous la forme de Legendre.

Il nous reste donc à montrer que les deux familles de dessins ci-dessus suffisent à caractériser toutes les coniques définies sur $\mathbb{Q}$. C'est à dire:

Théorème 1

- *Toute courbe de genre 0 définie sur $\mathbb{Q}$ et sans point réel est isomorphe à une $\mathcal{C}_{m,n,p,q}$ pour m, n, p, q positifs deux à deux distincts.*
- *Toute courbe de genre 0 définie sur $\mathbb{Q}$ et munie d'un point réel est isomorphe à une $\mathcal{C}_{m,n,-p,-q}$ pour m, n positifs distincts, p, q positifs distincts et $m > n > p+q$.*

Toute courbe de genre 0 est isomorphe à une conique de Legendre $\mathcal{L}_{a,b,c}$ d'équation

$$aX^2 + bY^2 + cZ^2 = 0$$

avec a, b, c entiers et abc sans facteurs carrés.

Nous commençons par calculer un modèle de Legendre pour la courbe $\mathcal{C}_{m,n,p,q}$ sous l'hypothèse que m, n, p, q sont de sommes non nulles. On trouve que $\mathcal{C}_{m,n,p,q}$ est isomorphe à $\mathcal{L}_{mn(m+n+p),p,q(m+n)(m+n+p+q)}$ et de même pour toutes les coniques de Legendre obtenues par permutations des quatre entiers. Ceci se voit aisément en éliminant l'inconnue d dans l' équation (2) grâce à l'équation (1) puis en réduisant la forme quadratique obtenue en somme de carrés avec l'algorithme de Gauss.

Fait 4 *Si m, n, p, q sont des entiers de sommes non nulles alors la courbe $\mathcal{C}_{m,n,p,q}$ est isomorphe à la conique de Legendre $\mathcal{L}_{mn(m+n+p),p,q(m+n)(m+n+p+q)}$.*

Soit maintenant une conique de Legendre quelconque sans point réel, $\mathcal{L}_{a,b,c}$ avec a, b, c positifs et abc sans facteurs carrés. Nous cherchons à montrer que cette conique est isomorphe à une courbe $\mathcal{C}_{m,n,p,q}$ pour m, n, p et q positifs distincts. Pour cela il suffit de prouver l'existence de $4+7$ *rationnels* non nuls m, n, p, q, U, V, W, X, Y, Z, T satisfaisant le système suivant

$$\begin{aligned} m &= U^2 \\ m+n &= V^2 \end{aligned}$$

$$
\begin{aligned}
m+n+p &= W^2 \\
m+n+p+q &= X^2 \\
n &= aY^2 \\
p &= bZ^2 \\
q &= cT^2
\end{aligned}
$$

En effet si ce système a des solutions rationnelles il a des solutions entières car il est homogène. Si on substitue les valeurs de m, n, p et q correspondant à une telle solution dans la conique de Legendre donnée au fait 4 on obtient une courbe isomorphe à $\mathcal{L}_{a,b,c}$ car la classe d'isomorphisme d'une courbe de Legendre dépend seulement de ses coefficients *modulo les carrés* dans $\mathbb{Q}^*$.

Or le système ci-dessus a de nombreuses solutions. Considérons en effet l'équation $U^2 + aY^2 = V^2$ en U, Y et V. Elle admet une infinité de solutions rationnelles. Choisissons-en une telle que $UYV \neq 0$ et posons $m = U^2$, $n = aY^2$. Considérons alors l'équation $V^2 + bZ^2 = W^2$ en Z et W. Elle admet une infinité de solutions rationnelles. Choisissons en une telle que $ZW \neq 0$ et $bZ^2 \notin \{m, n\}$. On pose alors $p = bZ^2$. Pour finir, on considère l'équation $W^2 + cT^2 = X^2$ en X et T. Elle a une infinité de solutions. On demande de plus que $TX \neq 0$ et $cT^2 \notin \{m, n, p\}$. On pose $q = cT^2$ et on a alors formé des m, n, p, q distincts.

Soit maintenant une conique de Legendre avec point réel quelconque, $\mathcal{L}_{a,-b,-c}$ avec a, b, c positifs et abc sans facteurs carrés. Nous cherchons à montrer que cette conique est isomorphe à une courbe $\mathcal{C}_{m,n,-p,-q}$ pour m, n, p, q positifs et $m > p+q$ et $n > p+q$. Pour cela, il suffit de prouver l'existence de $4+7$ rationnels non nuls m, n, p, q, U, V, W, X, Y, Z, T satisfaisant le système suivant

$$
\begin{aligned}
m &= U^2 \\
m+n &= V^2 \\
m+n-p &= W^2 \\
m+n-p-q &= X^2 \\
n &= aY^2 \\
-p &= -bZ^2 \\
-q &= -cT^2
\end{aligned}
$$

On procède exactement comme plus haut pour U, Y, V, m, n. Il suffit alors d'observer que l'équation $V^2 + bZ^2 = W^2$ a des solutions rationnelles (Z, W) avec ZW non nul et bZ^2 arbitrairement proche de 0 (se souvenir que le lieu rationnel d'une conique est vide ou bien dense dans son lieu réel). On termine de même. □

Remarque Comme on le voit dans la preuve, la correspondance entre coniques de Legendre et courbes $\mathcal{C}_{m,n,p,q}$ n'est pas biunivoque.

Remarque Les courbes $\mathcal{C}_{m,n,p,q}$ que nous avons introduites portent des dessins rationnels sans automorphismes de petit degré puisque sous les conditions des faits 2 et 3 ce degré est bornée par $6max(|m|, |n|, |p|, |q|)$. C'est ce qu'une utilisation directe du théorème de Belyi ne laisse pas soupçonner.

7 Mauvaises réductions

Dans cette section on cherche à illustrer le phénomène de mauvaise réduction d'un dessin modulo un idéal premier $\mathfrak{p}$ de son corps des modules. Nous avons vu qu'un dessin définit une classe d'isomorphisme de revêtements et de courbes sur un corps de nombres $\mathbb{K}$ donné. Nous pouvons donc considérer les idéaux premiers $\mathfrak{p} \subset \mathcal{O}_{\mathbb{K}}$ de mauvaise réduction de la courbe $\mathcal{C}(\mathbf{D})$ associée au dessin $\mathbf{D}$. On peut aussi se poser la question de la potentielle bonne réduction d'un revêtement Galoisien. Nous considérerons des surfaces arithmétiques sur $\mathcal{O}_{\mathbb{K}}$ (schémas intègres, normaux, plats et de type fini sur $\mathcal{O}_{\mathbb{K}}$ dont la fibre générique est une courbe lisse sur $\mathbb{K}$). Nous supposerons toujours que les surfaces sont propres. En revanche, les morphismes peuvent être ramifiés. Pour une introduction à ces questions on peut consulter [22] et [40].

Nous allons procéder à quelques rappels. La substance théorique de cette section est classique et se trouve essentiellement dans les articles [22, 19]. Voir aussi [10, 31]. Nous remercions Michel Matignon, Qing Liu et Frans Oort qui ont attiré notre attention sur ces références. Notre objectif est de prouver la mauvaise réduction sans trop de calculs.

Définition 1 *Soit $\mathbb{K}$ un corps de nombres, $\mathcal{O}_{\mathbb{K}}$ son anneau d'entiers et $\mathfrak{p}$ idéal premier de $\mathcal{O}_{\mathbb{K}}$. Soit $\mathcal{C}$ une courbe projective lisse et géométriquement connexe définie sur $\mathbb{K}$.*

- *Un modèle de $\mathcal{C}$ est une surface arithmétique $\mathcal{C}^0$ sur $\mathcal{O}_{\mathbb{K}}$ de fibre générique $\mathcal{C}$.*
- *Nous dirons que $\mathcal{C}$ a bonne réduction en $\mathfrak{p}$ si et seulement si elle admet un modèle dont la fibre au dessus de $\mathfrak{p}$ soit lisse et géométriquement connexe.*
- *Nous dirons que $\mathcal{C}$ a bonne réduction possible en $\mathfrak{p}$ si et seulement si elle est isomorphe sur une extension finie $\mathbb{L}$ de $\mathbb{K}$ à une courbe ayant bonne réduction en tous les premiers de $\mathcal{O}_{\mathbb{L}}$ au dessus de $\mathfrak{p}$.*

  Si une courbe n'a pas bonne réduction possible nous disons qu'elle a mauvaise réduction nécessaire.

Remarque Nous aurons à considérer des courbes de genre 0 et c'est pourquoi nous ne pouvons invoquer le modèle minimal de la courbe dans la définition ci-dessus. Si le genre est positif, la courbe a bonne réduction si et seulement la fibre spéciale de son modèle minimal est lisse et géométriquement connexe.

Nous aurons aussi à considérer des réductions de revêtements Galoisiens de courbes.

Définition 2 *Soit $\mathbb{K}$ un corps de nombres, $\mathcal{O}_{\mathbb{K}}$ son anneau d'entiers et $\mathfrak{p}$ idéal premier de $\mathcal{O}_{\mathbb{K}}$ et $\mathbf{k}$ le corps résiduel. Soient $\mathcal{C}$ une courbe algébrique projective lisse définie sur $\mathbb{K}$ et G un groupe fini d'automorphismes de $\mathcal{C}$ tous définis sur $\mathbb{K}$. Soit $\mathcal{D}$ la courbe quotient. Soit $\phi : \mathcal{C} \xrightarrow{G} \mathcal{D}$ le G-revêtement galoisien ramifié associé.*

- *Un modèle de* $\mathcal{C} \xrightarrow{G} \mathcal{D}$ *est la donnée d'un modèle* $\mathcal{C}^0$ *de* $\mathcal{C}$ *et d'un modèle* $\mathcal{D}^0$ *de* $\mathcal{D}$ *ainsi que d'un morphisme fini galoisien* $\phi^0 : \mathcal{C}^0 \xrightarrow{G} \mathcal{D}^0$ *qui induise le morphisme* ϕ *sur les fibres génériques.*

- *Nous dirons que* ϕ *a bonne réduction en* $\mathfrak{p}$ *si et seulement s'il admet un modèle* $\phi^0 : \mathcal{C}^0 \xrightarrow{G} \mathcal{D}^0$ *tel que les fibres spéciales* $\mathcal{C}_{\mathbf{k}}$ *et* $\mathcal{D}_{\mathbf{k}}$ *soient lisses et géométriquement connexes et* ϕ^0 *induise un G-revêtement galoisien* $\phi_{\mathbf{k}} : \mathcal{C}_{\mathbf{k}} \xrightarrow{G} \mathcal{D}_{\mathbf{k}}$. *En particulier* ϕ^0 *est modéré en codimension un (voir [22]).*

- *Nous dirons que* ϕ *a bonne réduction possible en* $\mathfrak{p}$ *si et seulement s'il est isomorphe sur une extension finie* $\mathbb{L}$ *de* $\mathbb{K}$ *à un revêtement ayant bonne réduction en tous les premiers de* $\mathcal{O}_{\mathbb{L}}$ *au dessus de* $\mathfrak{p}$.

  Si un G-revêtement n'a pas bonne réduction possible nous disons qu'il a mauvaise réduction nécessaire.

Remarque Si le genre de $\mathcal{C}$ est positif il est naturel de prendre pour $\mathcal{C}^0$ le modèle minimal de $\mathcal{C}$. De par son unicité ce modèle hérite du groupe d'automorphismes G et on peut le quotienter pour obtenir $\phi^0 : \mathcal{C}^0 \xrightarrow{G} \mathcal{D}^0$

La bonne réduction d'un revêtement implique la bonne réduction des courbes.
D'autre part

Théorème 2 *Soit* $\mathbb{K}$ *un corps de nombres,* $\mathcal{O}_{\mathbb{K}}$ *son anneau d'entiers,* $\mathfrak{p}$ *un idéal premier de* $\mathcal{O}_{\mathbb{K}}$, $\mathbf{k}$ *le corps résiduel et soit* p *l'entier premier rationnel au dessous de* $\mathfrak{p}$. *Soit* G *un groupe fini sans* p*-sous-groupe normal non trivial et* $\phi^0 : \mathcal{C}^0 \xrightarrow{G} \mathcal{D}^0$ *un revêtement Galoisien de surfaces arithmétiques. Si les fibres spéciales* $\mathcal{C}_{\mathbf{k}}$ *et* $\mathcal{D}_{\mathbf{k}}$ *sont lisses et géométriquement connexes alors* $\phi_{\mathbf{k}}$ *est un G-revêtement Galoisien.*

C'est le Lemme 2.4. de S. Beckmann. En fait, ce résultat est vrai sans aucune restriction sur le groupe G pourvu que le genre de $\mathcal{C}^0$ soit plus grand que 1 (il suffit que $\mathcal{C}^0$ soit stable). C'est alors le théorème I.11 de [19]. La bonne réduction de $\mathcal{D}_{\mathbf{k}}$ est alors conséquence de la bonne réduction de $\mathcal{C}_{\mathbf{k}}$. On a donc le

Théorème 3 *Soit* $\mathbb{K}$ *un corps de nombres,* $\mathcal{O}_{\mathbb{K}}$ *son anneau d'entiers,* $\mathfrak{p}$ *un idéal premier de* $\mathcal{O}_{\mathbb{K}}$, $\mathbf{k}$ *le corps résiduel. Soit* $\phi^0 : \mathcal{C}^0 \xrightarrow{G} \mathcal{D}^0$ *un revêtement Galoisien de surfaces arithmétiques. Si la fibre spéciale* $\mathcal{C}_{\mathbf{k}}$ *est lisse et géométriquement connexe et de genre plus grand que* 1 *alors la fibre spéciale* $\mathcal{D}_{\mathbf{k}}$ *est aussi lisse et géométriquement connexe et* $\phi_{\mathbf{k}}$ *est un G-revêtement Galoisien.*

Ce dernier énoncé pose une équivalence entre bonnes réductions des courbes et des revêtements Galoisiens. Notons cependant que l'on ne sait rien *a priori* sur le modèle $\mathcal{D}^0$ donné par le dessin et en particulier sur la géométrie du lieu de ramification. Avant d'illustrer ce point nous rappelons la

Définition 3 *Soit* $\mathcal{D}^0$ *une surface arithmétique et* $(P_i^0)_i$ *une collection finie de diviseurs premiers horizontaux. On dit que la somme* $\sum_i P_i^0$ *est un diviseur simple si les intersections* $P_{i,\mathbf{k}}$ *des* P_i^0 *avec la fibre spéciale* $\mathcal{D}_{\mathbf{k}}$ *sont deux à deux distinctes.*

Il peut se faire qu'un revêtement ramifié au dessus de ℓ points ait bonne réduction mais que le lieu de ramification du modèle correspondant soit non simple. Dans ce cas, les fibres singulières formeront un revêtement Galoisien de même groupe de Galois mais ramifié en un nombre de points plus petit que ℓ.

Par exemple le polynôme de Belyi $A_{2,1}(X) = 27/4X^2(1-X)$ définit une extension $\mathbb{Q}(Y) \subset \mathcal{F} = \mathbb{Q}[X]/ < A_{2,1}(X)-Y >$ de degré 3, non ramifiée en dehors de $\{0, 1, \infty\}$. La normalisation de $\mathbb{P}_{1/\mathbb{Z}}$ dans $\mathcal{F}$ est un revêtement de surfaces arithmétiques non ramifié en dehors de $D = 0^0+1^0+\infty^0$ où 0^0, 1^0 et ∞^0 sont les fermetures (disjointes) de 0, 1, ∞ dans $\mathbb{P}_{1/\mathbb{Z}}$. Mais cette normalisation n'est pas lisse au dessus de $p = 2$. Elle est constituée de deux droites simples. La première est un revêtement de $\mathbb{P}_1$ inséparable de degré 2 et la deuxième est le revêtement trivial.

En revanche, posons $\tilde{A}_{2,1}(X) = X^2(1 - X)$ le polynôme non ramifié en dehors de $\{0, 4/27, \infty\}$. Sa réduction modulo 2 donne un revêtement séparable de $\mathbb{P}_1$ non ramifié en dehors de $\{0, \infty\}$. Il y a donc bonne réduction mais le revêtement spécial est ramifié au dessus de deux points seulement. Nous dirons que la réduction est bonne mais pas *simple*.

Observons que le groupe de Galois de $\tilde{A}_{2,1}(X) - Y$ est $\mathcal{S}_3$. On obtient donc par réduction modulo 2 un revêtement de $\mathbb{P}_{1/\bar{\mathbb{F}}_2} - \{0, \infty\}$ de groupe de Galois $\mathcal{S}_3$. Cela implique que $\mathcal{S}_3$ est engendré par ses éléments d'ordre 2 (direction “facile” de la conjecture d'Abhyankar [26, XIII] et [29]) ce qui est bien le cas.

Il est important de savoir comment se comporte le lieu de ramification dans la fibre singulière. Soit $\phi : \mathcal{C} \xrightarrow{G} \mathcal{D}$ un revêtement Galoisien. Au prix d'une extension des scalaires on peut supposer que le lieu de ramification se décompose en une somme $D = \sum_i D_i$ de points rationnels sur $\mathcal{D}$. On suppose qu'il existe un modèle $\mathcal{C}^0$ de $\mathcal{C}$ dont la fibre spéciale soit lisse et géométriquement connexe et un revêtement non ramifié en $\mathfrak{p}$

$$\phi^0 : \mathcal{C}^0 \to \mathcal{D}^0.$$

On considère les prolongements D_i^0 des D_i sur $\mathcal{D}^0$. Si $D_{i,\mathbf{k}}$ est distinct des $D_{j,\mathbf{k}}$ pour tous les $j \neq i$ on dit que D_i est un point simple de ramification pour ϕ_0. Le diviseur D se décompose en parties simple D et non simple N soit $D = S + N$.

Définition 4 *Dans ces conditions, soit une famille finie $(P_i)_{i\in I}$ de points rationnels deux à deux distincts sur $\mathcal{C}$. On note $Q_i = \phi(P_i)$*

On dit que $(P_i)_i$ est admissible relativement à ϕ^0 si pour tout $i \neq j$ dans I on a

- $Q_{i,\mathbf{k}} \neq Q_{j,\mathbf{k}}$
- *ou bien* $Q_i = Q_j \notin N$

On a le

Théorème 4 *Soient $\mathcal{C}^0$ et $\mathcal{D}^0$ deux surfaces arithmétiques de fibres spéciales $\mathcal{C}_\mathbf{k}$ et $\mathcal{D}_\mathbf{k}$ lisses et géométriquement connexes. Si $\phi^0 : \mathcal{C}^0 \to \mathcal{D}^0$ est un revêtement non ramifié en $\mathfrak{p}$ et si $(P_i)_i$ est une famille de points rationnels sur $\mathcal{C}$ admissible relativement à ϕ^0 alors les $P_{i,\mathbf{k}}$ sont deux à deux distincts.*

En effet si $Q_{i,\mathbf{k}} \neq Q_{j,\mathbf{k}}$ alors $P_{i,\mathbf{k}} \neq P_{j,\mathbf{k}}$.

Si $Q_i = Q_j \notin N$ alors suivant [22, sections 2 et 3] nous considérons l'anneau local A de $Q_{i,\mathbf{k}}$ et B sa clôture dans le corps des fractions de $\mathcal{C}^0$, obtenue par restriction de ϕ^0 puisque $\mathcal{C}^0$ est normale. Nous appelons Δ le discriminant de l'extension $A \subset B$ et π une uniformisante de $\mathfrak{p}$ (on étend les scalaires au localisé R de $\mathcal{O}_{\mathbb{K}}$ en $\mathfrak{p}$). Le point Q_i définit un idéal minimal de A d'équation locale f. L'idéal (f, π) est l'idéal maximal de A. Puisque $Q_i \notin N$ le discriminant Δ est égal à $f^m u$ où u est une *unité* de A. On en déduit que la multiplicité de (f) dans Δ est égale à la multiplicité de (f, π) dans (Δ, π). Par le théorème 2.3.b. de [22] on en déduit que le diviseur préimage de Q_i^0 par ϕ^0 est simple sur $\mathcal{C}^0$. Voir la preuve de 3.3. dans [22]. $\square$

Dans le cas d'un revêtement de $\mathbb{P}_1 - \{0, 1, \infty\}$ on doit considérer des revêtements d'un modèle $\mathcal{D}^0$ de $\mathbb{P}_1$ ramifiés au dessus de $D = D_0 + D_1 + D_\infty$ où D_0, D_1 et D_∞ sont trois diviseurs premiers de $\mathcal{D}^0$.

Si D est simple on dit que $\mathcal{D}^0$ est de type $< \{0\}, \{1\}, \{\infty\} >$.

Si $D_{0,\mathbf{k}} = D_{1,\mathbf{k}} = D_{\infty,\mathbf{k}}$ on dit que $\mathcal{D}^0$ est de type $< \{0, 1, \infty\} >$.

Si $D_{0,\mathbf{k}} = D_{1,\mathbf{k}} \neq D_{\infty,\mathbf{k}}$ on dit que $\mathcal{D}^0$ est de type $< \{0, 1\}, \{\infty\} >$.

Un revêtement Galoisien de groupe G, de fibre spéciale lisse et géom. connexe, non ramifié en $\mathfrak{p}$ et de type $< \{0, 1, \infty\} >$ donne par réduction un revêtement Galoisien de groupe G de $\mathbb{P}_{1/\bar{\mathbb{F}}_p}$ non ramifié en dehors de ∞. En particulier, G doit être engendré par ses éléments d'ordre p.

Si le revêtement est de type $< \{0, 1\}, \{\infty\} >$ alors $G/p(G)$ doit être cyclique où $p(G)$ est le sous-groupe caractéristique de G engendré par les éléments d'ordre p.

Dans l'exemple précédent le polynôme $\tilde{A}_{2,1}(X) - Y$ définit un revêtement étale de $\mathbb{P}_{1/\mathbb{Z}} - D$ avec $D = D_0 + D_1 + D_\infty$ et $D_0 = 0^0$, $D_1 = (4/27)^0$ et $D_\infty = \infty^0$. Observons que la fibre générique de $\mathbb{P}_{1/\mathbb{Z}} - D$ est bien isomorphe à $\mathbb{P}_{1/\mathbb{Q}} - \{0, 1, \infty\}$ comme il se doit mais $\mathbb{P}_{1/\mathbb{Z}} - D$ n'est pas isomorphe à $\mathbb{P}_{1/\mathbb{Z}} - \{0^0, 1^0, \infty^0\}$.

Pour reformuler le théorème précédent on utilisera la

Définition 5 *Soit $\mathbb{K}$ un corps de nombres, $\mathcal{O}_{\mathbb{K}}$ son anneau d'entiers et $\mathfrak{p}$ un idéal premier de $\mathcal{O}_{\mathbb{K}}$ et $\mathbf{k}$ le corps résiduel.*

Une courbe pointée $\dot{\mathcal{C}} = (\mathcal{C}, (P_i)_{i \in I})$ est la donnée d'une courbe $\mathcal{C}$ algébrique projective, lisse, géométriquement connexe, définie sur $\mathbb{K}$ et d'une famille finie de points $\mathbb{K}$-rationnels deux à deux distincts $(P_i)_{i \in I}$ sur $\mathcal{C}$.

- *Un modèle de $\dot{\mathcal{C}}$ est la donnée d'un modèle $\mathcal{C}^0$ de $\mathcal{C}$ et d'une famille de diviseurs premier horizontaux P_i^0 de $\mathcal{C}$ tels que P_i^0 soit la clôture de P_i dans $\mathcal{C}^0$.*

- *Nous dirons que $\dot{\mathcal{C}}$ a bonne réduction en $\mathfrak{p}$ si et seulement si elle admet un modèle $(\mathcal{C}^0, (P_i^0)_i)$ tel que la fibre spéciale soit lisse et que les diviseurs P_i^0 ne se coupent pas dans la fibre spéciale.*

- *Nous dirons que $\dot{\mathcal{C}}$ a bonne réduction possible en $\mathfrak{p}$ si et seulement si elle est isomorphe sur une extension finie $\mathbb{L}$ de $\mathbb{K}$ à une courbe pointée ayant bonne réduction en tous les premiers de $\mathcal{O}_{\mathbb{L}}$ au dessus de $\mathfrak{p}$.*

  Si une courbe pointée n'a pas bonne réduction possible nous disons qu'elle a mauvaise réduction nécessaire.

La conclusion du théorème 4 est alors que $\dot{\mathcal{C}} = (\mathcal{C}, (P_i)_i)$ a bonne réduction.

Nous sommes en mesure d'énoncer des critères de mauvaise réduction.

Théorème 5 *Soit $\mathbb{K}$ un corps de nombres, $\mathcal{O}_{\mathbb{K}}$ son anneau d'entiers, $\mathfrak{p}$ un idéal premier de $\mathcal{O}_{\mathbb{K}}$ et soit p l'entier premier rationnel au dessous de $\mathfrak{p}$. Soit G un groupe fini tel que $G \neq p(G)$. Soit $\mathcal{C}$ une courbe projective lisse géométriquement connexe définie sur $\mathbb{K}$ et de genre plus grand que 1. Soit $\phi : \mathcal{C} \xrightarrow{G} \mathbb{P}_1$ un G-revêtement Galoisien défini sur $\mathbb{K}$ et non ramifié en dehors de $\{0, 1, \infty\}$. Soit H un sous groupe de G et $\mathcal{E} = \mathcal{C}/H$ la courbe quotient. Le revêtement ϕ se décompose en $\mathcal{C} \xrightarrow{H} \mathcal{E} \xrightarrow{\psi} \mathbb{P}_1$. Si les courbes pointées $(\mathcal{E}, \psi^{-1}\{0\})$, $(\mathcal{E}, \psi^{-1}\{1\})$, $(\mathcal{E}, \psi^{-1}\{\infty\})$ ont mauvaise réduction nécessaire alors $\mathcal{C}$ a mauvaise réduction nécessaire.*

En effet, soit $\mathcal{C}^0$ le modèle minimal de $\mathcal{C}$ et $\phi^0 : \mathcal{C}^0 \to \mathcal{D}^0$ le revêtement quotient. $\mathcal{D}^0$ est un modèle de $\mathbb{P}_1$ de type $< \{0, 1, \infty\} >$ sinon l'une des courbes pointées ci-dessus aurait bonne réduction. Le revêtement des fibres spéciales $\phi_{\mathbf{k}}$ est donc Galoisien de groupe G au dessus de la droite affine sur $\bar{\mathbb{F}}_p$. Ceci contredit l'hypothèse que $G \neq p(G)$. $\square$

Ce théorème ne fournit qu'une illustration possible des techniques présentées.

Il est bien sûr beaucoup plus simple de considérer le revêtement ϕ que sa clôture Galoisienne pour décider de la bonne ou mauvaise réduction.

Il est naturel de se demander s'il existe des règles simples permettant de deviner la structure algébrique associée à un dessin donné par une description combinatoire telle qu'un couple de permutations. En particulier, les places de mauvaise réduction de la courbe peuvent elles être lues sur le dessin? [D']après Grothendieck, S. Beckmann a prouvé dans [5] que les premiers de mauvaise réduction d'un revêtement divisent l'ordre du groupe de Galois géométrique G. Dans [38] Serre demande si les premiers p de mauvaise réduction de la courbe associée à un G-revêtement rigide de $\mathbb{P}_1 - \{0, 1, \infty\}$ doivent diviser l'ordre de ramification d'un des points singulier du revêtement.

Il est facile d'estimer les nombres premiers de mauvaise réduction d'une courbe lorsque son genre est zéro comme nous le rappellerons dans le prochain paragraphe. Cela nous permettra de construire un revêtement $\phi : \mathcal{C} \to \mathbb{P}_1$ non ramifié en dehors de $\{0, 1, \infty\}$, sans automorphismes et défini sur $\mathbb{Q}$ tel que la courbe $\mathcal{C}$ ait mauvaise réduction en un nombre premier p étranger à tous les indices de ramification de ϕ.

De même il est facile de caractériser le bonne réduction potentielle d'une courbe de genre zéro marquée. Cela nous permettra de construire un G-revêtement galoisien défini sur $\mathbb{Q}$

$$\phi : \mathcal{C} \to \mathbb{P}_1$$

non ramifié en dehors de $\{0, 1, \infty\}$ tel que la courbe $\mathcal{C}$ ait mauvaise réduction *nécessaire* en un nombre premier p étranger à tous les indices de ramification de ϕ.

7.1 Bonne réduction des coniques

Nous étudions la bonne réduction de courbes de genre 0. Ces courbes sont isomorphes à des coniques planes (Riemann-Roch). Toute conique plane se met sous forme de

Legendre $\mathcal{L}_{a,b,c}$

$$aX^2 + bY^2 + cZ^2 = 0,$$

avec a, b, c premiers entre eux deux à deux.

Une telle courbe a un point rationnel si et seulement si elle est isomorphe à $\mathbb{P}_{1/\mathbb{Q}}$. Il existe un algorithme polynômial, essentiellement dû à Lagrange (voir [35]) qui décide de l'existence d'un tel point et en produit un s'il en existe.

Les nombres premiers de mauvaise réduction se lisent aisément sur un modèle de Legendre. En effet,

Théorème 6 *Soit p un nombre premier impair. Une courbe lisse projective définie sur $\mathbb{Q}$ et de genre zéro a des points sur $\mathbb{Q}_p$ si et seulement si elle a bonne réduction en p.*

Supposons que pour p un nombre premier impair la courbe $\mathcal{C}$ n'a pas de point sur $\mathbb{Q}_p$. Alors, pour tout modèle lisse projectif associé à $\mathcal{C}$, la fibre au dessus de p est singulière. En effet, si elle était régulière, ce serait une courbe lisse de genre 0 sur $\mathbb{F}_p$ et elle aurait des points lisses rationnels, contradiction.

Réciproquement, supposons que $\mathcal{C}$ ait des points sur $\mathbb{Q}_p$ avec p un nombre premier impair. Alors $\mathcal{C}$ admet un modèle de Legendre dont la fibre au dessus de p soit régulière.

En effet, $\mathcal{C}$ a un modèle de Legendre

$$aX^2 + bY^2 + cZ^2 = 0,$$

avec abc sans facteur carré.

Si p est premier à abc alors la fibre au dessus de p est régulière. Si $p|a$ et $-bc$ n'est pas un carré modulo p, alors la courbe n'a pas de points sur $\mathbb{Q}_p$, contradiction. Si enfin $p|a$ et $-bc$ est un carré modulo p, alors la fibre au dessus de p du modèle de Legendre $\mathcal{L}_{a,b,c}$ est singulière mais il existe un autre modèle pour $\mathcal{C}$ dont la fibre au dessus de p est régulière.

Pour prouver cela, on remarque qu'il existe un entier $e \geq 0$ et un entier δ tels que δ^2 soit congru à $-bc$ modulo p^{2e+1} et pas modulo p^{2e+2}. On a alors un entier λ premier à p tel que

$$\delta^2 + bc = \lambda p^{2e+1}. \tag{4}$$

On observe aussi qu'en posant $a = pA$, l'équation de notre conique se réécrit sous la forme

$$(bY)^2 + bcZ^2 = -pbAX^2. \tag{5}$$

Si l'on multiplie maintenant 3 et 4, appliquant la multiplicativité des normes, on trouve une nouvelle équation de Legendre pour la conique:

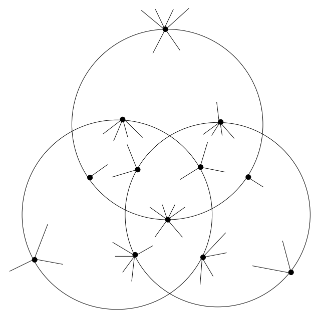
$$U^2 + bcV^2 = -\lambda bAW^2,$$

et comme λ est premier à p ce dernier modèle a bonne réduction en p. $\square$

Nous en venons maintenant à un exemple précis. Considérons la courbe $\mathcal{C}_{1,2,3,5}$. Elle est isomorphe à $\mathcal{L}_{1,1,55}$ par le fait 4 et elle a mauvaise réduction en 11 car -1 n'est pas résidu quadratique modulo 11. Et pourtant, les ordres de ramification du dessin $\mathcal{D}_{1,2,3,5}$ sont 1 et 4 au dessus de 1, $1+2=3$, $1+3=4$, $1+5=6$, $2+3=5$, $2+5=7$, et $3+5=8$ au dessus de 0 et $1+2+3=6$, $2+3+5=10$, $3+5+1=9$ et $5+1+2=8$ au dessus de ∞.

Ainsi 11 est un premier de mauvaise réduction de $\mathcal{C}_{1,2,3,5}$ qui est étranger aux ordres de ramifications de $\mathbf{D}_{1,2,3,5}$.

Nous représentons ce dessin ci-dessous.



Observons que si $\mathcal{E} \stackrel{\mu}{\to} \mathbb{P}_1$ est la clôture Galoisienne de $\mathcal{C}_{1,2,3,5} \stackrel{\lambda_{1,2,3,5}}{\to} \mathbb{P}_1$ alors $\mathcal{E}$ est définie sur $\mathbb{Q}$ et a mauvaise réduction en 11. En effet $\mathcal{C}_{1,2,3,5}$ a mauvaise réduction en 11 et elle est un quotient de $\mathcal{E}$. Voir [36, appendice]. En revanche $\mathcal{E}$ comme $\mathcal{C}_{1,2,3,5}$ peuvent avoir potentiellement bonne réduction en 11.

7.2 Bonne réduction potentielle de courbes pointées de genre 0

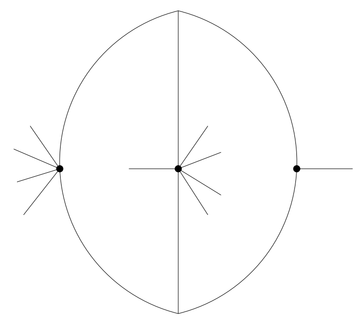
Soit $\mathcal{C}$ une courbe de genre zéro définie sur un corps de nombres $\mathbb{K}$ et P_1, P_2, P_3, P_4 quatre points distincts de $\mathcal{C}$. On définit le birapport $[P_1, P_2, P_3, P_4]$ comme le birapport des images des P_i par n'importe quel isomorphisme de $\mathcal{C}$ sur $\mathbb{P}_1$ (après une éventuelle extension des scalaires). Si les quatre points sont définis sur $\mathbb{K}$, leur birapport est un élément de $\mathbb{K}-\{0,1\}$. Soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}_{\mathbb{K}}$. On dit qu'un élément x de $\mathbb{K}-\{0,1\}$ est régulier modulo $\mathfrak{p}$ si et seulement si la valuation en $\mathfrak{p}$ de $x(x-1)$ est nulle. On a le

Théorème 7 *Soit $\mathbb{K}$ un corps de nombres, $\mathcal{O}_{\mathbb{K}}$ son anneau d'entiers, et $\mathfrak{p}$ un idéal premier de $\mathcal{O}_{\mathbb{K}}$ tel que $2, 3 \notin \mathfrak{p}$. Soit I un ensemble fini de cardinalité au moins 4. Une courbe marquée $\dot{\mathcal{C}} = (\mathcal{C}, (P_i)_{i\in I})$ de genre 0 définie sur $\mathbb{K}$ a potentiellement bonne réduction en $\mathfrak{p}$ si et seulement si tous les birapports formés à partir de quatre points distincts quelconques parmi les P_i sont non singuliers modulo $\mathfrak{p}$.*

Il suffit de le prouver pour le cas où la cardinalité de I est 4. Soit alors $\beta = [P_1, P_2, P_3, P_4]$. Après extension de $\mathbb{K}$, la courbe $\dot{\mathcal{C}}$ est isomorphe à $(\mathbb{P}_1, (0, 1, \infty, \beta))$ et la proposition est alors équivalente à un résultat similaire pour les courbes elliptiques. Voir [39]. Considérons le revêtement $E_j \stackrel{\delta}{\to} \mathbb{P}_1$ de degré 2 de $\mathbb{P}_1$ ramifié au dessus de 0, 1, ∞ et β. Si $(\mathbb{P}_1, (0, 1, \infty, \beta))$ a bonne réduction potentielle alors δ a bonne réduction potentielle car $2 \notin \mathfrak{p}$ ([22, 5]) et donc E_j aussi. On en déduit que l'invariant $j = 12^3(\beta^2 - \beta + 1)^3/\beta^2(\beta - 1)^2$ est $\mathfrak{p}$-intégral et donc β est régulier modulo $\mathfrak{p}$. Réciproquement, si β est régulier la courbe $(\mathbb{P}_1, (0, 1, \infty, \beta))$ a pour modèle régulier $(\mathbb{P}_{1/\mathcal{O}_{\mathbb{K}}}, (0^0, 1^0, \infty^0, \beta^0))$ où 0^0, 1^0, ∞^0 et β^0 sont les fermetures (disjointes) de 0, 1, ∞ et λ dans $\mathbb{P}_{1/\mathcal{O}_{\mathbb{K}}}$. $\square$

Nous donnons maintenant un exemple.

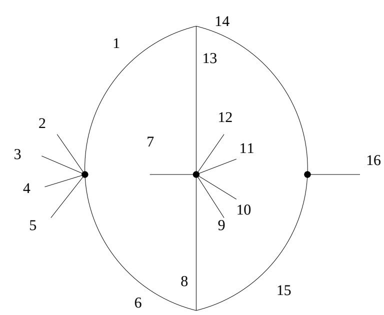
Considérons le revêtement $\nu_{1,2,5} : \mathcal{K}_{1,2,5} \to \mathbb{P}_1$. C'est un revêtement de genre zéro et de degré 16. Il correspond au dessin suivant.



Sa monodromie est donnée par

$$\Sigma_0 = (1, 2, 3, 4, 5, 6)(7, 8, 9, 10, 11, 12, 13)(14, 15, 16) \text{ et } \Sigma_1 = (1, 13, 14)(6, 15, 8)$$

si l'on numérote les drapeaux comme ci-dessous (voir [20, 13]).



Les multiplicités sont 1,3 au dessus de 1 et 3, 6, 7 au dessus de 0 et ∞. Le groupe de Galois géométrique du revêtement est le groupe de permutation engendré par Σ_0 et Σ_1. On vérifie à l'aide d'un ordinateur que ces deux permutations engendrent le groupe complet de permutations de degré 16. Soit G ce groupe et $p = 5$. Alors $p(G)$ est contenu dans le groupe alterné $\mathcal{A}_{16}$ car tout cycle de longueur 5 est pair. En fait $p(G) = \mathcal{A}_{16}$ mais peu importe.

La fonction de $\mathcal{K}_{1,2,5}$ dans $\mathbb{P}_1$ qui à (a, b, c) associe $r = a/c$ est un isomorphisme. En composant $\nu_{1,2,5}$ avec cet isomorphisme on obtient la fraction rationnelle de Belyi

$$\nu(r) = -\frac{5^5}{2^{26}} \frac{(r+7)^7 (r-1)^6 (3r+5)^3}{r^7 (5+r)^6}.$$

Considérons l'extension de corps de fonctions associée à ce revêtement $\mathbb{Q}(T) \subset \mathcal{F} \subset \mathbb{M}$ où $\mathbb{M}$ est une clôture algébrique de $\mathbb{Q}(T)$. Soit $\mathcal{G}$ la clôture galoisienne de $\mathcal{F}$

dans $\mathbb{M}$. Alors $\mathcal{G}$ est une extension régulière de $\mathbb{Q}(T)$. En effet, l'extension $\mathbb{Q}(T) \subset \mathcal{F}$ est régulière de degré $d = 16$ et sans automorphismes et de plus son groupe de Galois géométrique est autonormalisateur dans le groupe symétrique $\mathcal{S}_d$ (puisqu'il est $\mathcal{S}_d$ lui même.) On en déduit par un résultat classique [21, 34, 24] que $\mathbb{Q}(T) \subset \mathcal{G}$ est régulière. Appelons $\mathcal{E}$ la courbe associée à $\mathcal{G}$. C'est un G-revêtement galoisien de $\mathbb{P}_1$ défini sur $\mathbb{Q}$ et non ramifié en dehors de $\{0, 1, \infty\}$

$$\gamma : \mathcal{E} \to \mathbb{P}_1$$

et le revêtement se factorise

$$\mathcal{E} \to \mathcal{K}_{1,2,5} \overset{\nu_{1,2,5}}{\to} \mathbb{P}_1.$$

Les multiplicités de γ sont 3 au dessus de 1 et 42 au dessus de 0 et ∞ (p.p.c.m. des multiplicités de $\nu_{1,2,5}$).

Supposons que $\mathcal{E}$ ait bonne réduction. Soit $\mathcal{E}_0$ son modèle minimal et $\phi^0 : \mathcal{E}^0 \overset{G}{\to} \mathcal{D}^0$ le revêtement associé. Nous allons aboutir à une contradiction quel que soit le type de $\mathcal{D}^0$.

- Si le type est $< \{0, 1, \infty\} >$ alors $\phi_{\mathbf{k}}$ est Galoisien de groupe G au dessus de la droite affine. Contradiction car $G \neq p(G)$.

- Si le type est $< \{0\}, \{1\}, \{\infty\} >$ ou $< \{\infty\}, \{0, 1\} >$ ou $< \{0, 1\}, \{\infty\} >$ alors la famille

  $$(A_2, B_1, B_2, B_3)$$

  de $\mathcal{K}_{1,2,5}$ est admissible et donc la courbe pointée $(\mathcal{K}_{1,2,5}, (A_2, B_1, B_2, B_3))$ a bonne réduction. Or le birapport associé est

  $$[B_2, A_2, B_3, B_1] = [-\frac{p}{m}, 1, 0, \infty] = -\frac{p}{m} = -5$$

  qui est singulier modulo 5.

- Si le type est $< \{0\}, \{1, \infty\} >$ alors la famille

  $$(A_1, A_2, A_3, B_3)$$

  est admissible. Mais le birapport correspondant est

  $$[A_1, A_2, A_3, B_1] = [\frac{-p}{m+n}, 1, -\frac{n+p}{m}, 0] = -\frac{n}{p} = -2/5$$

  qui est singulier modulo 5.

- Si le type est $< \{0, \infty\}, \{1\} >$ alors la famille

  $$(B_1, C_1, C_2, H_i)$$

  est admissible pour tout $1 \leq i \leq 2(m + n + p) - 6 = 10$.

La valeur de r correspondant à B_1 est ∞.

Les valeurs r_1 et r_2 de r correspondant à C_1 et C_2 sont les deux solutions de l'équation

$$3r^2 + 10r + 35 = 0.$$

On a $r_2 = -10/3 - r_1$.

Les valeurs ρ_i de r correspondant aux H_i sont solutions du polynôme

$$\begin{aligned}\Pi(X) \quad = \quad & 7503125 - 30441250X + 33644625X^2 + 17565800X^3 - 53431750X^4 + 12542580X^5 + 28736890X^6 \\ & + 10429032X^7 + 1640625X^8 + 118750X^9 + 3125X^{10}\end{aligned}$$

Les birraports $b_i = [\infty, r_1, r_2, \rho_i]$ sont donc solutions du polynôme

$$\Pi((r_2 - r_1)X + r_1).$$

Les birapports $\tilde{b}_i = [\infty, r_2, r_1, \rho_i]$ sont donc solutions du polynôme

$$\Pi((r_1 - r_2)X + r_2).$$

Le produit des deux polynômes ci-dessus est, après division par le coefficient dominant

$$\begin{aligned}\Gamma(X) \quad = \quad & X^{20} - 10X^{19} + 279/5X^{18} - 1086/5X^{17} + 49703298/78125X^{16} - 113938884/78125X^{15} \\ & + 26220369850347/9765625000X^{14} - 39488780202429/9765625000X^{13} + 394366699065213/78125000000X^{12} \\ & - 205871262669331/39062500000X^{11} + 722898354089341/156250000000X^{10} - 534624636430827/156250000000X^9 \\ & + 665294142776769/312500000000X^8 - 43318486307817/39062500000X^7 + 598939655323671/1250000000000X^6 \\ & - 211503911544909/1250000000000X^5 + 954562620324429/20000000000000X^4 - 20749599941553/2000000000000X^3 \\ & + 3274088662971/2000000000000X^2 - 26795786661/160000000000X + 26795786661/3200000000000\end{aligned}$$

dont le coefficient constant est

$$2^{-16}3^{13}5^{-11}7^5.$$

Or toutes les racines de Γ devraient être régulières modulo les premiers au dessus de 5. Contradiction.

Ainsi la courbe $\mathcal{E}$ est définie sur $\mathbb{Q}$ ainsi que tous ses automorphismes et elle a mauvaise réduction en $p = 5$. L'application quotient $\gamma : \mathcal{E} \to \mathbb{P}_1$ est non ramifiée en dehors de trois points et ses indices de ramification sont premiers à 5.

8 Corps des modules et corps de définition

Dans cette section nous construisons une famille de dessins de corps des modules $\mathbb{Q}$ et sans modèle défini sur $\mathbb{Q}$. Nous nous contenterons de généraliser une construction présentée dans [14] et que nous rappelons brièvement. Voir aussi [18]. Dans [14] on a prouvé le

Fait 5 *Soit* $\mathbf{L}$ *un dessin de genre* 0 *et de corps des modules* $\mathbb{Q}$. *Supposons que le groupe* $Aut(\mathbf{L})$ *des automorphismes de* $\mathbf{L}$ *est d'ordre deux et soit* $\mathfrak{a}$ *l'automorphisme d'ordre deux. On note* $\mathbf{D}$ *le dessin quotient* $\mathbf{L}/\,Aut(\mathbf{L})$. *Son corps des modules est* $\mathbb{Q}$ *et il admet un modèle canonique sur* $\mathbb{Q}$ *comme dessin quotient de* $\mathbf{L}$. *On note* $\mathcal{C}(\mathbf{L})$ *la courbe associée (à* $\mathbb{Q}$ *isomorphisme près). Alors* $\mathbf{L}$ *a un modèle défini sur* $\mathbb{Q}$ *si et seulement si* $\mathcal{C}(\mathbf{L})$ *a un point rationnel.*

Nous allons ici partir d'un des dessins sans automorphismes $\mathbf{D}_{m,n,p,q}$ ou $\mathbf{E}_{m,n,p,q}$ construits ci-dessus. Nous observons que si $m > n > p > q$ le dessin $\mathbf{D}_{m,n,p,q}$ a exactement deux faces (points au dessus de ∞) de multiplicités $m+n+p$. De même sous les conditions du fait 3 le dessin $\mathbf{E}_{m,n,p,q}$ a seulement deux sommets (points au dessus de 0) de multiplicités $m+n$.

Dans tous les cas on note $\mathbf{D}$ le dessin choisi (soit $\mathbf{D}_{m,n,p,q}$ soit $\mathbf{E}_{m,n,p,q}$) et $\lambda : \mathcal{C} \to \mathbb{P}_1$ la fonction de Belyi définie sur $\mathbb{Q}$ correspondante. On appelle X et Y les deux points de $\mathcal{C}$ que l'on vient de décrire. Ils forment une paire $\{X,Y\}$ définie sur $\mathbb{Q}$ car X et Y sont les deux seuls points de multiplicité $m+n+p$ ou $m+n$ selon le cas. Composons alors le revêtement λ avec un revêtement cyclique de degré 2 de $\mathcal{C}$ ramifié au dessus de $\{X,Y\}$. On obtient un dessin $\mathbf{L}$ de corps des *modules* $\mathbb{Q}$, extension cyclique de degré deux du dessin $\mathbf{D}$.

Montrons que $Aut(\mathbf{L})$ est d'ordre 2. Par construction il existe un automorphisme $\mathfrak{a}$ d'ordre 2. On appelle x (resp. y) l'unique point de $\mathbf{L}$ au dessus de X (resp. Y). Les points x et y sont eux aussi uniques par leur multiplicité (tous les autres points ont des multiplicités strictement plus petites). Ils sont donc fixés ou échangés par tout élément de $\mathfrak{b} \in Aut(\mathbf{L})$. On en déduit que $\mathfrak{b}\mathfrak{a}\mathfrak{b}^{-1}$ a x et y pour point fixe. Il est donc égal à $\mathfrak{a}$. Ainsi $\mathfrak{a}$ est dans le centre de $Aut(\mathbf{L})$. Et donc $Aut(\mathbf{L})/ < \mathfrak{a} >$ est le groupe d'automorphismes de $\mathbf{D}$ et donc il est trivial.

Nous appliquons alors le fait 5.

9 Monodromie du chardon

Dans cette section nous prouvons le fait 2 en calculant la monodromie de $\lambda_{m,n,p,q}$ sous la condition que les m, n, p, q sont positifs et deux à deux distincts et nous montrons que $\lambda_{m,n,p,q}$ n'a pas d'automorphismes dans ce cas.

Cette monodromie se déduit de l'action des tresses sur les revêtements ϕ_P ramifiés au dessus de quatre points donnés a_1, a_2, a_3, a_4 comme expliqué dans la section 4. Tous les calculs de cette section sont immédiats et peuvent être vérifiés mentalement par le lecteur.

Posons $D = m+n+p+q$. Notre premier souci sera d'énumérer les revêtements ϕ_P, c'est à dire de calculer dans la base (s_1, s_2, s_3, s_4) de

$$\pi_1(\mathbb{P}_1(\mathbb{C}) - \{a_1, a_2, a_3, a_4\}, b)$$
la monodromie de tous les revêtements de type ϕ_P. Cela nous conduira à définir une nomenclature adaptée.

Revenant aux considérations de la section 5.2 et se souvenant de la formule de Hurwitz nous observons que les types de décomposition des fibres singulières de ϕ_P sont génériquement

- (D) au dessus de ∞.
- $(3, 1^{D-3})$ au dessus de 1.
- $(2, 1^{D-2})$ au dessus de λ_P.
- (m, n, p, q) au dessus de 0.

Nous disons qu'un revêtement est de type $\mathcal{T}$ si ses types de décomposition sont comme ci-dessus. Un quadruplet de permutations $(\sigma_1, \sigma_2, \sigma_3, \sigma_4)$ sera dit de type $\mathcal{T}$ si les types des permutations sont comme indiqué ci-dessus et si leur produit est égal à 1. Un vecteur de permutations sera dit transitif si le groupe engendré par les quatre permutations agit transitivement sur $[1..D]$. Nous disons que deux vecteurs $(\sigma_i)_i$ et $(\sigma'_i)_i$ sont conjugués s'il existe une permutation τ telle que $\sigma'_i = {}^\tau\sigma_i$. L'action des tresses est compatible avec la relation de conjugaison.

Nous montrerons en particulier qu'il y a $6(m+n+p+q)$ classes de conjugaison de vecteurs de type $\mathcal{T}$ et que l'action des tresses est transitive sur ces classes. Ceci prouvera que la famille ϕ_P définit un espace de Hurwitz irréductible au sens de [21] et nous donnera la monodromie de $\lambda_{m,n,p,q}$. Nous serons alors en mesure de prouver que $\lambda_{m,n,p,q}$ n'a pas d'automorphismes. Au passage, nous aurons prouvé l'irréductibilité de $\mathcal{C}_{m,n,p,q}$.

Le principe de ce calcul a été donné dans la section 4. Les revêtements ϕ_P ramifiés au dessus de $A = (a_1, a_2, a_3, a_4)$ correspondent aux points de la fibre $\lambda^{-1}_{m,n,p,q}(A)$ et l'action des tresses sur ces revêtements donne la monodromie de $\lambda_{m,n,p,q}$.

Observons d'abord que le groupe de Galois géométrique d'un revêtement de type $\mathcal{T}$ est le groupe complet de permutations S_D car il contient une transposition et un cycle complet. Pour décrire tous les revêtements de type $\mathcal{T}$ nous devons décrire tous les vecteurs de quatre permutations de type $\mathcal{T}$ à conjugaison près par un élément de S_D et leur donner un nom.

Nous commençons avec la

Définition 6 *Pour tout k résidu modulo $m+n$ on note $f_{m+n,p,q,\{k,k+m\}}$ le quadruplet $(\sigma_1, \sigma_2, \sigma_3, \sigma_4)$ avec*

$$\begin{aligned}
\sigma_1 &= [1, 2, ..., m+n+p+q], \\
\sigma_2 &= [1, m+n+p+1, m+n+1], \\
\sigma_3 &= [k \bmod m+n, k+m \bmod m+n], \\
\sigma_4 &= (\sigma_3\sigma_2\sigma_1)^{-1}.
\end{aligned}$$

On dit que les $m+n$ vecteurs définis ainsi forment la famille $F_{m+n,p,q}$.

Nous prendrons toujours pour représenter une classe de congruence le plus petit membre strictement positif.

Il y a $m+n$ vecteurs dans la famille $F_{m+n,p,q}$. On définit de même 12 familles distinctes similaires à $F_{m+n,p,q}$ obtenues en permutant m, n, p et q dans la définition ci-dessus. On a le

Fait 6 *Tout vecteur de type $\mathcal{T}$ appartient (à conjugaison près) à l'une des douze familles listées dans le tableau suivant avec leurs cardinalités.*

Famille	*Cardinalité*
$F_{m+n,p,q}$	$m+n$
$F_{m+n,q,p}$	$m+n$
$F_{n+p,q,m}$	$n+p$
$F_{n+p,m,q}$	$n+p$
$F_{p+q,m,n}$	$p+q$
$F_{p+q,n,m}$	$p+q$
$F_{q+m,n,p}$	$q+m$
$F_{q+m,p,n}$	$q+m$
$F_{m+p,n,q}$	$m+p$
$F_{m+p,q,n}$	$m+p$
$F_{q+n,m,p}$	$q+n$
$F_{q+n,p,m}$	$q+n$

Il y a donc $6(m+n+p+q)$ vecteurs dans $\mathcal{T}$ à équivalence près.

Pour prouver le fait 6, nous utiliserons les lemmes immédiats suivants.

Lemme 1 *Soient m et n deux entiers positifs, alors le produit de permutations* $[1, 1+m] \times [1, 2, ..., m+n]$ *vaut* $[1, 2, ..., m][m+1, ..., m+n]$.

Lemme 2 *Soient m, n et p trois entiers positifs, alors le produit* $[1, 1+m, 1+m+n] \times [1, 2, ..., m+n+p]$ *est un cycle de taille $m+n+p$. En revanche le produit* $[1, 1+m+n, 1+m][1, 2, ..., m+n+p]$ *est égal à* $[1, 2, ..., m][m+1, m+2, ..., m+n][m+n+1, ..., m+n+p]$.

Le lemme 1 s'interprète en disant qu'une transposition coupe un cycle en deux morceaux.

Le lemme 2 dit qu'un cycle de longueur trois coupe un cycle en trois morceaux s'il est orienté à l'inverse de ce cycle.

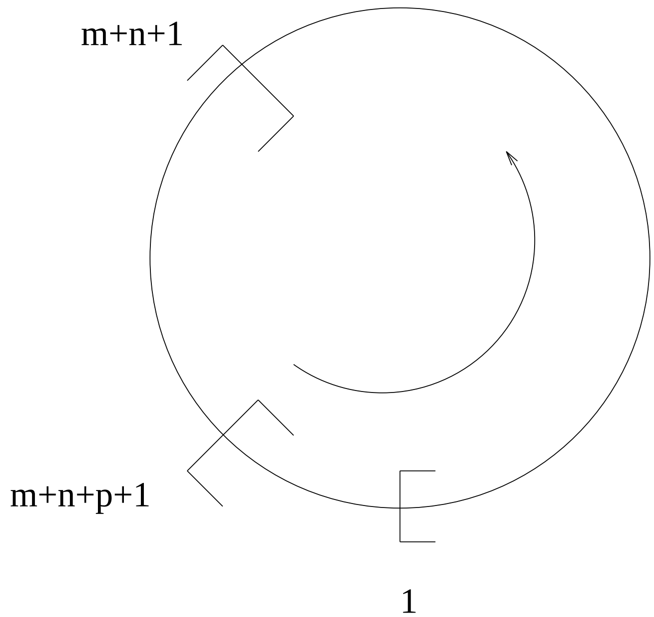
On cherche alors des quadruplets de permutations (à conjugaison près)

$$(\sigma_1, \sigma_2, \sigma_3, \sigma_4)$$

tels que $\sigma_4\sigma_3\sigma_2\sigma_1 = 1$, avec σ_1 cycle d'ordre D, σ_2 cycle d'ordre 3, σ_3 transposition et σ_4 de type (m, n, p, q). On peut toujours choisir $\sigma_1 = [1, 2, 3, ..., D]$.

Partant d'un cycle σ_1 et multipliant par des cycles σ_2 et σ_3 de longueurs 3 et 2 respectivement on doit obtenir un produit de 4 cycles disjoints de longueurs m, n, p et q. On utilise les Lemmes 1 et 2.

Il faut que σ_2 coupe σ_1 en trois cycles de taille $m+n$, p, q dans cet ordre (par exemple) puis que σ_3 coupe le gros cycle de taille $m+n$ en deux cycles de taille m et n. Il existe une unique normalisation telle que 1 soit le début du gros morceaux comme le montre le dessin suivant.



Dans cet exemple le quadruplet est de la famille $F_{m+n,p,q}$. On voit que $\sigma_2\sigma_1$ est fait de trois cycles de tailles $(m+n,p,q)$ dans cet ordre et que σ_3 coupe le cycle de longueur $m+n$ en deux cycles de taille m et n. Il y a $m+n$ tels vecteurs à équivalence près selon l'endroit où σ_3 coupe le cycle de longueur $m+n$ dans $\sigma_2\sigma_1$.

Nous étudions maintenant l'action du groupe de tresses à quatre brins sur ces vecteurs, ce qui nous donnera la monodromie de l'application $\lambda_{m,n,p,q}$.

9.1 Action de $t_{1,2}$

Soit donc $f_{m+n,p,q,\{k,k+m\}} = (\sigma_1,\sigma_2,\sigma_3,\sigma_4)$ donné comme plus haut. On note que $({}^{\sigma_2\sigma_1}\sigma_1, {}^{\sigma_2\sigma_1}\sigma_2, \sigma_3, \sigma_4)$ est conjugué à $(\sigma_1, \sigma_2, {}^{(\sigma_2\sigma_1)^{-1}}\sigma_3, {}^{(\sigma_2\sigma_1)^{-1}}\sigma_4)$. On calcule alors

$$\begin{aligned} \sigma_2\sigma_1 &= [1,2,...,m+n][m+n+1,...,m+n+p][m+n+p+1,...,m+n+p+q] \\ {}^{(\sigma_2\sigma_1)^{-1}}\sigma_3 &= [k-1 \bmod m+n, k-1+m \bmod m+n] \end{aligned}$$

Et donc

$$\boxed{t_{1,2}(f_{m+n,p,q,\{k,k+m\}}) = f_{m+n,p,q,\{k-1,k-1+m\}}.}$$

Dans cette formule et dans les suivantes le signe $=$ doit être lu *conjugué à*. Les familles correspondent donc aux cycles de $t_{1,2}$.

9.2 Action de $t_{2,3}$

Observons que si σ_2 et σ_3 commutent, l'action de $t_{2,3}$ est triviale. Nous considérons donc seulement le cas où $1 \in \{k, k+m\}$.

Nous commençons par l'action de $t_{2,3}$ sur $f_{m+n,p,q,\{1,1+m\}}$.

On a

$$\begin{aligned} \sigma_2 &= [1, m+n+p+1, m+n+1] \\ \sigma_3 &= [1, m+1] \\ \sigma_3\sigma_2 &= [1, m+n+p+1, m+n+1, m+1] \\ {}^{\sigma_3\sigma_2}\sigma_2 &= [m+n+p+1, m+n+1, m+1] \\ {}^{\sigma_3\sigma_2}\sigma_3 &= [1, m+n+p+1] \end{aligned}$$

Conjuguons alors le vecteur obtenu par σ_1^q. On trouve le vecteur

$$(\sigma_1, [1, m+n+q+1, m+q+1], [1, 1+q], *)$$

c'est à dire

$$\boxed{t_{2,3}(f_{m+n,p,q,\{1,1+m\}}) = f_{q+m,n,p,\{1,1+q\}}.}$$

De même, en permutant m et n on trouve

$$\boxed{t_{2,3}(f_{n+m,p,q,\{1,1+n\}}) = f_{q+n,m,p,\{1,1+q\}}.}$$

Nous écrivons alors les cycles de $t_{2,3}$ en itérant la règle précédente:

$$[f_{m+n,p,q,\{1,1+m\}}, f_{q+m,n,p,\{1,1+q\}}, f_{p+q,m,n,\{1,1+p\}}, f_{n+p,q,m,\{1,1+n\}}]. \tag{6}$$

9.3 Preuve du Fait 2

Un examen attentif de la monodromie que nous venons de calculer prouve la première partie du fait 2. On pourra se reporter à l'article de Leila Schneps dans [20] pour voir comment reconstituer le graphe d'un dessin à partir de sa monodromie. Le plus simple est encore de se munir d'une feuille de papier, d'un crayon et d'une gomme et de se souvenir que le graphe recherché est constitué de drapeaux (composantes connexes de la préimage du segment ouvert $]0,1[$) et que les lacets S_0 et S_1 font tourner les drapeaux autour de leur hampe et de leur pointe respectivement.

Pour montrer que $\mathbf{D}_{m,n,p,q}$ n'a pas d'automorphisme non trivial il suffit de voir que le centralisateur dans S_D du groupe engendré par $t_{1,2}$ et $t_{2,3}$ (vues comme permutations des D vecteurs de type $\mathcal{T}$) est trivial.

Soit donc $\omega \in \mathcal{Z}_{S_D}(< t_{1,2}, t_{2,3} >)$. La commutation avec $t_{1,2}$ impose que ω fixe la famille $F_{m+n,p,q}$ ou bien l'échange avec $F_{m+n,q,p}$. Si ω fixe toutes les familles alors il est facile de prouver que $\omega = 1$ sinon supposons que ω échange les familles $F_{m+n,p,q}$ et $F_{m+n,q,p}$. Si m, n, p, q sont deux à deux distincts, la commutation avec $t_{2,3}$ impose que $\omega(f_{m+n,p,q,\{1,1+m\}}) = f_{m+n,q,p,\{1,1+m\}}$. Alors l'image par ω du cycle donné en 5 est

$$[f_{m+n,q,p,\{1,1+m\}}, f_{p+m,n,q,\{1,1+p\}}, f_{q+p,m,n,\{1,1+q\}}, f_{n+q,p,m,\{1,1+n\}}].$$

En particulier on a $\omega(f_{p+q,m,n,\{1,1+p\}}) = f_{q+p,m,n,\{1,1+q\}}$ mais ceci est incompatible avec l'action de $t_{1,2}$, contradiction.

La preuve ci-dessus est très incomplète. Ce qui nous guide dans cette preuve et devrait guider le lecteur, c'est l'observation du dessin de la section 5.2., car un automorphisme ω doit induire une symétrie de ce dessin.

10 Monodromie de la pomme

Dans cette section nous prouvons le fait 3 ce qui revient à calculer la monodromie de $\lambda_{m,n,-p,-q}$ sous la condition que m, n, p, q sont positifs et $m > p + q$, $n > p + q$.

Nous procédons comme à la section précédente sans donner tous les détails. Les calculs sont un peu plus délicats ici. Aussi nous devrons solliciter plus encore l'imagination du lecteur.

Les types de décompositions sont,

- $(p, q, m + n - p - q)$ au dessus de ∞.
- $(3, 1^{D-3})$ au dessus de 1.
- $(2, 1^{D-2})$ au dessus de λ_P.
- (m, n) au dessus de 0.

Nous dirons qu'un revêtement est de type $\mathcal{U}$ si ses types de décompositions sont comme ci-dessus. Nous montrerons qu'il y a $6(m + n) - 4(p + q)$ classes de vecteurs transitifs de type $\mathcal{U}$ et nous calculerons l'action des tresses sur ces classes (elle est transitive dans ce cas). Nous en déduirons la monodromie de $\lambda_{m,n,-p,-q}$ et l'irréductibilité de $\mathcal{C}_{m,n,-p,-q}$. Notons qu'il n'est pas tout à fait évident que tous les vecteurs de type $\mathcal{U}$ engendrent le même groupe. C'est pourtant le cas puisqu'ils sont conjugués par action des tresses comme nous le verrons (le groupe en question est d'ailleurs S_D lui même). Comme dans le cas du chardon, les $6(m + n) - 4(p + q)$ vecteurs se répartiront en familles (dix) mais cette fois les familles seront elles mêmes groupées en trois clans.

Nous donnons les définitions correspondantes.

Définition 7 *Pour k un résidu modulo $m+n$ on note $a^+_{\{k,k+m\}}$ le quadruplet $(\sigma_1, \sigma_2, \sigma_3, \sigma_4)$ avec*

$$\begin{aligned}
\sigma_1 &= [1, 2, ..., m + n - p - q][m + n - p - q + 1, ..., m + n - q][m + n - q + 1, ..., m + n] \\
\sigma_2 &= [1, m + n - p - q + 1, m + n - q + 1], \\
\sigma_3 &= [k \bmod m + n, k + m \bmod m + n], \\
\sigma_4 &= (\sigma_3\sigma_2\sigma_1)^{-1}.
\end{aligned}$$

Les $m + n$ vecteurs ainsi définis forment la famille A^+.

Définition 8 *Pour k un résidu modulo $m+n$ on note $a^-_{\{k,k+m\}}$ le quadruplet $(\sigma_1, \sigma_2, \sigma_3, \sigma_4)$ avec*

$$\begin{aligned}
\sigma_1 &= [1,2,...,m+n-p-q][m+n-p-q+1,...,m+n-p][m+n-p+1,...,m+n] \\
\sigma_2 &= [1, m+n-p-q+1, m+n-p+1], \\
\sigma_3 &= [k \bmod m+n, k+m \bmod m+n], \\
\sigma_4 &= (\sigma_3\sigma_2\sigma_1)^{-1}.
\end{aligned}$$

Les $m+n$ vecteurs ainsi définis forment la famille A^-.

Définition 9 *Pour k un résidu modulo $n-q$ on note $b_{m,p,k}$ le quadruplet $(\sigma_1, \sigma_2, \sigma_3, \sigma_4)$ avec*

$$\begin{aligned}
\sigma_1 &= [1,2,...,m+n-p-q][m+n-p-q+1,...,m+n-q][m+n-q+1,...,m+n] \\
\sigma_2 &= [1, m-p+1, m+n-p-q+1], \\
\sigma_3 &= [m+n-q+1, m-p+k], \\
\sigma_4 &= (\sigma_3\sigma_2\sigma_1)^{-1}.
\end{aligned}$$

Les $n-q$ vecteurs ainsi définis forment la famille $B_{m,p}$.

On définit de même les familles $B_{m,q}$, $B_{n,p}$, $B_{n,q}$.

Définition 10 *Pour k un résidu modulo $n-q$ on note $c_{m,p,k}$ le quadruplet on note $c_{m,p,k}$ le quadruplet $(\sigma_1, \sigma_2, \sigma_3, \sigma_4)$ avec*

$$\begin{aligned}
\sigma_1 &= [1,2,...,m+n-p-q][m+n-p-q+1,...,m+n-q][m+n-q+1,...,m+n] \\
\sigma_2 &= [1, m+n-p-q+1, m+1], \\
\sigma_3 &= [m+n-q+1, m+k], \\
\sigma_4 &= (\sigma_3\sigma_2\sigma_1)^{-1}.
\end{aligned}$$

Les $n-q$ vecteurs ainsi définis forment la famille $C_{m,p}$.

On définit de même les familles $C_{m,q}$, $C_{n,p}$, $C_{n,q}$.

Fait 7 *Tout vecteur de type $\mathcal{U}$ appartient à l'une des dix familles listées dans le tableau suivant avec leurs cardinalités.*

Famille	*Cardinalité*
A^+	$m+n$
A^-	$m+n$
$B_{m,p}$	$n-q$
$B_{m,q}$	$n-p$
$B_{n,p}$	$m-q$
$B_{n,q}$	$m-p$
$C_{m,p}$	$n-q$
$C_{m,q}$	$n-p$
$C_{n,p}$	$m-q$
$C_{n,q}$	$m-p$

Il y a donc $6(m+n)-4(p+q)$ vecteurs dans $\mathcal{T}$ à équivalence près.

On dit que les quatre familles $B_{m,p}$, $B_{m,q}$, $B_{n,p}$, $B_{n,q}$ forment le clan B. De même les quatre familles $C_{m,p}$, $C_{m,q}$, $C_{n,p}$, $C_{n,q}$ forment le clan C.

Pour prouver le fait 7 nous avons besoin de décrire le produit d'une permutation contenant trois cycles et d'un cycle d'ordre 3. Si le cycle d'ordre 3 permute trois valeurs contenues dans les trois cycles, alors le produit est un unique grand cycle. Si les trois valeurs du 3-cycle sont dans un seul cycle, nous sommes ramenés au Lemme 2. Reste à examiner le dernier cas:

Lemme 3 *Soient m, n, p trois entiers positifs, alors le produit de permutations* $[1, m+n+1, m+1] * [1, 2, ..., m+n][m+n+1, ..., m+n+p]$
vaut $[1, 2, ..., m][m+1, ..., m+n, m+n+1, ..., m+n+p]$.

Ce lemme signifie que l'on voit grossir un cycle aux dépens de l'autre.

Cherchons maintenant des quadruplets transitifs de permutations de type $\mathcal{U}$.

Le principe est toujours le même: on "part" d'une permutation produit de trois cycles disjoints et on "arrive" à une permutation produit de deux cycles disjoints en la multipliant successivement par deux cycles de longueurs 3 et 2. L'action de ces deux cycles est donnée par les lemmes 1,2 et 3.

Il n'est pas possible que σ_2 permute trois valeurs dans un même cycle de σ_1 (le quadruplet ne serait pas transitif).

Si σ_2 permute trois valeurs prises dans les trois cycles de σ_1 alors le vecteur est dans la famille A^+ lorsque les trois valeurs appartiennent dans l'ordre aux cycles de longueurs p, q, $m+n-p-q$ et dans la famille A^- lorsque les trois valeurs appartiennent dans l'ordre aux cycles de longueurs q, p, $m+n-p-q$.

Lorsque σ_2 allonge un cycle de σ_1 aux dépens d'un autre, le cycle raccourci est nécessairement celui de longueur $m+n-p-q$. Si la longueur du cycle rallongé appartient à $\{m, n\}$ alors le vecteur est du clan B. Si la longueur du cycle raccourci appartient à $\{m, n\}$ alors le vecteur est du clan C.

Une famille du clan B est notée $B_{m,p}$ pour signifier que le cycle de longueur p de σ_1 est allongé au détriment de celui de longueur $m+n-p-q$ et donne un cycle de longueur m de σ_4.

Une famille du clan C est notée $C_{m,p}$ pour signifier que le cycle de longueur $m+n-p-q$ de σ_1 est raccourci au profit du cycle de longueur p, et donne un cycle de longueur m de σ_4.

10.1 Action de $t_{1,2}$

Il est aisé de voir que

$$\boxed{t_{1,2}(a^+_{\{k,k+m\}}) = t_{1,2}(a^+_{\{k-1,k-1+m\}})}$$

et

$$\boxed{t_{1,2}(a^-_{\{k,k+m\}}) = t_{1,2}(a^-_{\{k-1,k-1+m\}}).}$$

On montre aussi que

$$\boxed{t_{1,2}(b_{m,p,k}) = b_{m,p,k-1}}$$

où comme nous l'avons déjà dit k et $k-1$ sont des classes modulo $n-q$ (de préférence le plus petit représentant positif). Pour démontrer cette dernière égalité on doit observer que le cycle $[m+n-q+1, ..., m+n]$ commute avec σ_1 et σ_2.

De même

$$\boxed{t_{1,2}(c_{m,p,k}) = c_{m,p,k-1}.}$$

10.2 Action de $t_{2,3}$ sur le clan B

Dans la monodromie de $b_{m,p,k}$, σ_2 et σ_3 commutent sauf si $k=1$. On a alors,

$$\begin{aligned}
\sigma_2 &= [1, m-p+1, m+n-p-q+1],\\
\sigma_3 &= [m+n-q+1, m-p+1],\\
\sigma_3\sigma_2 &= [1, m+n-q+1, m-p+1, m+n-p-q+1],\\
{}^{\sigma_3\sigma_2}\sigma_2 &= [m+n-q+1, m+n-p-q+1, 1]\\
{}^{\sigma_3\sigma_2}\sigma_3 &= [m-p+1, m+n-p-q+1].
\end{aligned}$$

Ainsi,

$$\boxed{t_{2,3}(b_{m,p,1}) = a^-_{\{m-p+1, m+n-p+1\}}.}$$

10.3 Action de $t_{2,3}$ sur le clan C

Dans la monodromie de $c_{m,p,k}$, σ_2 et σ_3 commutent sauf si $k=1$ ou $k=n-p-q+1$.

—Si $k=1$ on a,

$$\begin{aligned}
\sigma_2 &= [1, m+n-p-q+1, m+1],\\
\sigma_3 &= [m+n-q+1, m+1],\\
\sigma_3\sigma_2 &= [1, m+n-p-q+1, m+n-q+1, m+1],\\
{}^{\sigma_3\sigma_2}\sigma_2 &= [m+n-p-q+1, m+n-q+1, 1]\\
{}^{\sigma_3\sigma_2}\sigma_3 &= [m+1, 1].
\end{aligned}$$

Donc

$$\boxed{t_{2,3}(c_{m,p,1}) = a^+_{\{1,1+m\}}.}$$

—Si $k=n-p-q+1$ on a,

$$\begin{aligned}
\sigma_2 &= [1, m+n-p-q+1, m+1],\\
\sigma_3 &= [m+n-q+1, m+n-p-q+1],\\
\sigma_3\sigma_2 &= [1, m+n-q+1, m+n-p-q+1, m+1],\\
{}^{\sigma_3\sigma_2}\sigma_2 &= [m+n-q+1, m+1, 1]\\
{}^{\sigma_3\sigma_2}\sigma_3 &= [m+n-p-q+1, m+1].
\end{aligned}$$

Donc

$$\boxed{t_{2,3}(c_{m,p,n-p-q+1}) = c_{m,q,1}.}$$

10.4 Action de $t_{2,3}$ sur le clan A

Nous considérons d'abord la famille A^+. Dans la monodromie de $a^+_{\{k,m+k\}}$, σ_2 et σ_3 commutent sauf si $k \in \{1, 1+n-p-q, 1+n-q, 1+n, 1+m+n-p-q, 1+m+n-q\}$

—Si $k = 1$ on a,

$$\begin{aligned}
\sigma_2 &= [1, m+n-p-q+1, m+n-q+1],\\
\sigma_3 &= [1, 1+m],\\
\sigma_3\sigma_2 &= [1, m+n-p-q+1, m+n-q+1, m+1],\\
\sigma_2^{\sigma_3\sigma_2} &= [m+n-p-q+1, m+n-q+1, m+1]\\
\sigma_3^{\sigma_3\sigma_2} &= [m+n-p-q+1, 1].
\end{aligned}$$

Donc

$$\boxed{t_{2,3}(a^+_{\{1,1+m\}}) = a^+_{\{n-p-q+1,m+n-p-q+1\}}.}$$

—Si $k = n-p-q+1$ on a,

$$\begin{aligned}
\sigma_2 &= [1, m+n-p-q+1, m+n-q+1],\\
\sigma_3 &= [n-p-q+1, m+n-p-q+1],\\
\sigma_3\sigma_2 &= [1, n-p-q+1, m+n-p-q+1, m+n-q+1],\\
\sigma_2^{\sigma_3\sigma_2} &= [n-p-q+1, m+n-q+1, 1]\\
\sigma_3^{\sigma_3\sigma_2} &= [m+n-p-q+1, m+n-q+1].
\end{aligned}$$

Donc

$$\boxed{t_{2,3}(a^+_{\{n-p-q+1,m+n-p-q+1\}}) = c_{m,q,n-p-q+1}.}$$

—Si $k = 1+n-q$ on a,

$$\begin{aligned}
\sigma_2 &= [1, m+n-p-q+1, m+n-q+1],\\
\sigma_3 &= [n-q+1, m+n-q+1],\\
\sigma_3\sigma_2 &= [1, m+n-p-q+1, n-q+1, m+n-q+1],\\
\sigma_2^{\sigma_3\sigma_2} &= [m+n-p-q+1, n-q+1, 1]\\
\sigma_3^{\sigma_3\sigma_2} &= [m+n-q+1, 1].
\end{aligned}$$

Donc

$$\boxed{t_{2,3}(a^+_{\{n-q+1,m+n-q+1\}}) = b_{m,p,1}.}$$

—Si $k = 1 + n$ on a,

$$\begin{array}{rcl}
\sigma_2 & = & [1, m+n-p-q+1, m+n-q+1], \\
\sigma_3 & = & [n+1, 1], \\
\sigma_3\sigma_2 & = & [1, m+n-p-q+1, m+n-q+1, n+1], \\
{}^{\sigma_3\sigma_2}\sigma_2 & = & [m+n-p-q+1, m+n-q+1, n+1] \\
{}^{\sigma_3\sigma_2}\sigma_3 & = & [1, m+n-p-q+1].
\end{array}$$

Donc

$$\boxed{t_{2,3}(a^+_{\{1,1+n\}}) = a^+_{\{m+n-p-q+1, m-p-q+1\}}.}$$

—Si $k = 1 + m + n - p - q$ on a,

$$\begin{array}{rcl}
\sigma_2 & = & [1, m+n-p-q+1, m+n-q+1], \\
\sigma_3 & = & [m+n-p-q+1, m-p-q+1], \\
\sigma_3\sigma_2 & = & [1, m-p-q+1, m+n-p-q+1, m+n-q+1], \\
{}^{\sigma_3\sigma_2}\sigma_2 & = & [m-p-q+1, m+n-q+1, 1] \\
{}^{\sigma_3\sigma_2}\sigma_3 & = & [m+n-q+1, m+n-p-q+1].
\end{array}$$

Donc

$$\boxed{t_{2,3}(a^+_{\{m+n-p-q+1, m-p-q+1\}}) = c_{n,q,m-p-q+1}.}$$

—Si $k = 1 + m + n - q$ on a,

$$\begin{array}{rcl}
\sigma_2 & = & [1, m+n-p-q+1, m+n-q+1], \\
\sigma_3 & = & [m+n-q+1, m-q+1], \\
\sigma_3\sigma_2 & = & [1, m+n-p-q+1, m-q+1, m+n-q+1], \\
{}^{\sigma_3\sigma_2}\sigma_2 & = & [m+n-p-q+1, m-q+1, 1] \\
{}^{\sigma_3\sigma_2}\sigma_3 & = & [1, m+n-q+1].
\end{array}$$

Donc

$$\boxed{t_{2,3}(a^+_{\{m+n-q+1, m-q+1\}}) = b_{n,p,1}.}$$

Les cycles de $t_{2,3}$ sont alors

$$\begin{array}{l}
[a^+_{\{1,1+m\}}, a^+_{\{n-p-q+1, m+n-p-q+1\}}, c_{m,q,n-p-q+1}, c_{m,p,1}] \\
[a^+_{\{n-q+1, m+n-q+1\}}, b_{m,p,1}, a^-_{\{m-p+1, m+n-p+1\}}, b_{n,q,1}] \\
[a^+_{\{1,1+n\}}, a^+_{\{m+n-p-q+1, m-p-q+1\}}, c_{n,q,m-p-q+1}, c_{n,p,1}] \\
[a^+_{\{m+n-q+1, m-q+1\}}, b_{n,p,1}, a^-_{n-p+1, m+n-p+1}, b_{m,q,1}] \\
[a^-_{\{1,1+m\}}, a^-_{\{n-p-q+1, m+n-p-q+1\}}, c_{m,p,n-p-q+1}, c_{m,q,1}] \\
[a^-_{\{1,1+n\}}, a^-_{\{m+n-p-q+1, m-p-q+1\}}, c_{n,p,m-p-q+1}, c_{n,q,1}]
\end{array}$$

La preuve du fait 3 est alors aisée et laissée en exercice au lecteur. On procède selon le même principe que pour le fait 2.

11 Conclusion

Nous avons construit des dessins sans automorphismes associés à toutes les classes d'isomorphisme de courbes de genre 0 et nous avons illustré quelques phénomènes classiques de la théorie des revêtement avec ces exemples. Les revêtements sont construits comme espaces de modules de certains revêtements de la sphère moins quatre points. La mauvaise réduction de courbes de genre élevé a été démontrée par la considération de courbes de genre 0 pointées associées.

Bibliographie

[1] G. Anderson and Y. Ihara. Pro-l branched coverings of $\mathbb{P}_1$ and higher circular units, part 1. *Ann. of Math.*, 128:271–293, 1988.

[2] G. Anderson and Y. Ihara. Pro-l branched coverings of $\mathbb{P}_1$ and higher circular units, part 2. *Int'l Math. J.*, 1:119–148, 1990.

[3] A. O. L. Atkin and H.P.F. Swinnerton-Dyer. Modular forms over non-congruence subgroups. In *Proceedings of symposia in pure mathematics*, volume 19. AMS, 1971.

[4] W.L. Baily. On the theory of theta functions, the moduli of abelian varieties and the moduli of curves. *Ann. of Math.*, 75:342–381, 1962.

[5] Sybilla Beckmann. Ramified primes in the field of moduli of branched coverings of curves. *Journal of Algebra*, 125:236–255, 1989.

[6] G.V. Belyi. On Galois extensions of the maximal cyclotomic field. *Izvestiya Ak. Nauk. SSSR, ser. mat.*, 43:2:269–276, 1979.

[7] J. Bétréma and A. Zvonkin. Une vraie forme d'arbre planaire. In *TAP-SOFT'93*, volume 668. Springer Verlag, 1993.

[8] Bryan Birch. Noncongruence subgroups, covers and drawings. In Leila Schneps, editor, *The Grothendieck Theory of Dessins d'Enfants*, volume 200 of *Lecture Notes in Math.* Cambridge University Press, 1994.

[9] Joan S. Birman. *Braids, Links, and Mapping Class Groups.* Princeton University Press, 1974.

[10] I. Bouw. Quotients of tame fundamental groups of affine curves. *Preprint of Universiteit Utrecht*, 961, 1996.

[11] Henri Cohen. Dessins d'enfant, a long explanation and some fun. *sci.math.research*, 1995.

[12] Kevin Coombes and David Harbater. Hurwitz families and arithmetic Galois groups. *Duke mathematical journal*, 52:821–839, 1985.

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

[14] Jean-Marc Couveignes. Calcul et rationalité de fonctions de Belyi en genre 0. *Annales de l'Institut Fourier*, 44(1):1–38, 1994.

[15] Jean-Marc Couveignes. À propos du théorème de Belyi. *Journal de théorie des nombres de Bordeaux*, 8:93–99, 1996.

[16] Jean-Marc Couveignes. Quelques revêtements définis sur $\mathbb{Q}$. *Prépublications du Département d'Informatique de l'École Normale Supérieure*, Mai 1995.

[17] P. Debès and M. D. Fried. Nonrigid construction in Galois Theory. *Pacific Journal of Math*, 163:81–122, 1994.

[18] Pierre Debes and Michel Emsalem. On fields of moduli of curves. 1996.

[19] P. Deligne and D. Mumford. The irreducibility of the space of curves of given genus. *Pub. Math. IHES*, pages 75–109, 1969.

[20] Leila Schneps edt. *The theory of Grothendieck's dessins d'enfant*. Cambridge University Press, 1994.

[21] Michael D. Fried. Fields of definition of function fields and Hurwitz families–Groups as Galois groups. *Comm. Alg.*, 5:17–82, 1977.

[22] W. Fulton. Hurwitz schemes and irreducibility of moduli of algebraic curves. *Ann. Math.*, pages 542–575, 1969.

[23] L. Gerritzen, F. Herrlich, and M. van der Put. Stable n-pointed trees of projective line. *Ind. Math.*, 50:131–163, 1988.

[24] Louis Granboulan. Construction d'une extension régulière de $\mathbb{Q}(t)$. *Experimental Math.*, pages 1–13, 1996.

[25] Alexandre Grothendieck. Esquisse d'un programme. *Non publié.*

[26] Alexandre Grothendieck. *Revêtements étales et groupe fondamental.* Springer Verlag, 1971.

[27] L.V. Hansen. *Braids and Coverings*. Cambridge University Press, 1980.

[28] David Harbater. *Galois coverings of the arithmetic line*, volume 1240 of *Lect. Notes in Math.*, pages 165–195. Springer Verlag, 1987.

[29] David Harbater. Abhyankar's conjecture on Galois groups over curves. *Invent. Math.*, 117:1–25, 1994.

[30] A. Hurwitz. Über Riemann'sche Flächen mit gegebenem Verzweigungspunkten. *Math. Annalen*, 39:1–61, 1891.

[31] Yasutaka Ihara. Horizontal divisors on arithmetic surfaces associated with belyi uniformization. In L. Schneps, editor, *The Grothendieck theory of dessins d'enfants*. Cambridge University Press, 1994.

[32] G. Malle and B. H. Matzat. Action of Braids. In *Inverse Galois Theory*, chapter 3. 1993. Preprint. University of Heidelberg.

[33] B. H. Matzat. Braids and decomposition groups. In Sinnou David, editor, *Séminaire de théorie des nombres, Paris, 1991-1992*. Birkhäuser, 1993.

[34] B.H. Matzat. *Konstructive Galoistheorie*. Springer, 1987.

[35] L. J. Mordell. *Diophantine equations*. Academic Press, 1969.

[36] M. Raynaud. *p-groupes et réduction semi-stable des courbes*, pages 179–197. Birkhauser, 1990.

[37] Leila Schneps. Dessins d'enfant on the riemann sphere. In Leila Schneps, editor, *The Grothendieck Theory of Dessins d'Enfants*, volume 200 of *Lecture Notes in Math.* Cambridge University Press, 1994.

[38] Jean-Pierre Serre. *Topics in Galois theory*. Jones and Bartlett, 1992.

[39] J. H. Silverman. *The arithmetic of elliptic curves*. Springer, 1986.

[40] J. H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Springer, 1994.

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