ANNALES DE L'INSTITUT FOURIER

FEDOR PAKOVITCH

Combinatoire des arbres planaires et arithmétique des courbes hyperelliptiques

Annales de l'institut Fourier, tome 48, n° 2 (1998), p. 323-351

<http://www.numdam.org/item?id=AIF_1998__48_2_323_0>

Ann. Inst. Fourier, Grenoble
48, 2 (1998), 323–351

COMBINATOIRE DES ARBRES PLANAIRES ET ARITHMÉTIQUE DES COURBES HYPERELLIPTIQUES

par Fedor PAKOVITCH

INTRODUCTION

Le but de cet article est de proposer une nouvelle méthode pour des études dans le cadre de la théorie des «dessins d'enfants» de A. Grothendieck de certaines questions concernant l'action du groupe de Galois absolu $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ sur l'ensemble des arbres planaires.

Le point de départ est une stratification spéciale de l'ensemble des paires composées d'un polynôme et d'un segment telle qu'il existe une correspondance bijective entre les classes d'équivalence affine des paires qui se trouvent dans g-ième strate et pour lesquelles le degré du polynôme est égal à n, et les classes d'isomorphisme des paires se composant d'une courbe hyperelliptique de genre g et d'un point de n-division. En utilisant la stratification ci-dessus on définit l'application φ qui associe à chaque arbre planaire à n arêtes λ ayant un nombre de sommets de valence impaire $2g+2$, une courbe hyperelliptique H de genre g avec un point de n-division; la courbe H est définie sur un corps de nombres, *corps des modules* de l'arbre λ. L'ordre *exact* du point de n-division associé à un arbre λ est un invariant de l'action du groupe de Galois absolu $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ sur l'ensemble des arbres. On calcule cet invariant à partir de la structure *combinatoire* d'un arbre λ.

Grâce à cette construction, on établit un lien entre la théorie de la torsion des courbes hyperelliptiques et celle des «dessins d'enfants». En

Mots-clés : Fonctions de Belyi – Dessins d'enfants – Torsion des courbes – Corps des modules – Théorie de Galois.
Classification math. : 11G05 – 11R32 – 14C22 – 14H30 – 30F10.

particulier, dans le cas où $g = 1$, en utilisant les résultats correspondants sur la torsion des courbes *elliptiques*, on obtient des estimations *inférieures* sur les degrés des corps des modules des arbres de certaines classes. D'autre part, en utilisant l'application φ on obtient des séries intéressantes d'exemples de diviseurs rationnels de torsion sur des courbes hyperelliptiques définies sur des corps de nombres.

L'auteur a le plaisir de remercier B. Edixhoven, A. Marin, G. Shabat, M. Zaidenberg et A. Zvonkin pour des discussions de questions diverses à propos de cet article.

1. STRATIFICATION ABÉLIENNE

1.1. Stratification abélienne. Définitions géométrique, algébrique et analytique.

Soient $P(z)$ un polynôme complexe et $I = [a, b]$ le segment qui joint les points distincts $a, b \in \mathbb{C}$. Désignons par $u_1, u_2, \ldots, u_k$ toutes les valeurs critiques du polynôme $P(z)$ qui sont à l'intérieur de I, et posons

$$u_0 = a, \quad u_{k+1} = b.$$

Afin d'étudier pour la paire $\sigma = (P, I)$ une géométrie de l'ensemble $P^{-1}(I)$, il est commode de le regarder comme un graphe planaire G_σ, de sommets les images réciproques des points u_i, $i = 0, \ldots, k+1$, et d'arêtes les images réciproques des intervalles ouverts $]u_i, u_{i+1}[$, $i = 0, \ldots, k$. Il est clair que la valence de chaque sommet du graphe G_σ de coordonnée x, est égale à la multiplicité de la valeur du polynôme au point x, si $P(x) \in \{a, b\}$, et au double de la multiplicité, si $P(x) \in \{u_1, \ldots, u_k\}$. Une propriété importante du graphe G_σ consiste en l'absence de circuits [ShZv]. En effet, puisque sans restreindre la généralité on peut supposer que $I \subset \mathbb{R}$, s'il existait des circuits, la fonction harmonique sur tout le plan complexe Im $P(z)$ serait égale à zéro sur ces circuits, et, donc, serait égale à zéro à l'intérieur des domaines que les circuits bordent, ce qui est impossible.

On rappelle qu'un graphe planaire s'appelle linéaire s'il est homéomorphe à un segment.

PROPOSITION-DÉFINITION. — *On dira qu'une paire $\sigma = (P, I)$ composée d'un polynôme $P(z)$ et d'un segment $I = [a, b]$, $a \neq b$, se trouve dans la g-ième strate de la stratification abélienne, si n'importe laquelle des conditions suivantes équivalentes est satisfaite :*

1) *Le graphe* $G_\sigma = P^{-1}(I)$ *est une union de* $g+1$ *sous-graphes linéaires sans arêtes communes, mais n'est pas une union de* g *tels sous-graphes.*

2) *L'ensemble des points dans* $P^{-1}\{a,b\}$ *pour les valeurs desquels* $P(z)$ *a une multiplicité impaire est de cardinal* $2g+2$.

3) *Il existe des polynômes unitaires* $R_\sigma(z)$, $q_\sigma(z)$, $\deg R_\sigma(z) = 2g+2$, $\deg q_\sigma(z) = g$, *tels que* $R_\sigma(z)$ n'a *que des racines simples et que* $P(z)$ *satisfait l'équation d'Abel*

$$(1.1.1) \qquad \big(P(z)-a\big)\big(P(z)-b\big) = \Big(\frac{P'(z)}{nq_\sigma(z)}\Big)^2 R_\sigma(z),$$

où $n = \deg P(z)$.

Démonstration. — L'équivalence 1) $\Leftrightarrow$ 2) n'est qu'une traduction de l'assertion suivante : le graphe planaire sans circuits G est réunion de $g+1$ sous-graphes linéaires sans arêtes communes, mais n'est pas réunion de g tels sous-graphes, si et seulement si G contient $2g+2$ sommets de valence impaire. Soit $G = \bigcup_{i=1}^{k} G_i$ une partition du graphe G en des sous-graphes linéaires G_i sans arêtes communes avec k minimal. Pour chaque sommet s, on note $e(s)$ et $i(s)$ le nombre de G_i ayant s comme extrémité et point intérieur respectivement. Puisque la partition $G = \bigcup_{i=1}^{k} G_i$ est minimale, on a $e(s) \leq 1$, car si s était extrémité de G_{k-1} et G_k, on aurait $G = \bigcup_{i=1}^{k-1} G'_i$ avec $G'_i = G_i$ pour $i < k-1$ et $G'_{k-1} = G_{k-1} \cup G_k$. Pour la valence du sommet s, on a $v(s) = e(s) + 2i(s)$ donc $v(s)$ est impaire si et seulement si $e(s) = 1$. Puisque chaque graphe linéaire a deux extrémités, on conclut que le nombre de sommets de valence impaire est le double du nombre des sous-graphes linéaires de toute partition minimale.

2) $\Rightarrow$ 3). Désignons par $R_\sigma(z)$ le polynôme unitaire qui a comme racines tous les points de l'ensemble $P^{-1}\{a,b\}$ en lesquels $P(z)$ a une multiplicité impaire. Puisque $(P(z)-a)(P(z)-b)/R_\sigma(z)$ est un carré dans $\mathbb{C}[z]$, on a l'équation

$$(1.1.2) \qquad \big(P(z)-a\big)\big(P(z)-b\big) = Q^2(z)R_\sigma(z).$$

En dérivant cette équation, on obtient

$$(1.1.3) \qquad P'(z)\big(2P(z)-(a+b)\big) = Q(z)\big(2Q'(z)R_\sigma(z) + Q(z)R'_\sigma(z)\big).$$

Puisque chaque diviseur de $Q(z)$ est soit diviseur de $P(z) - a$, soit diviseur de $P(z) - b$, le polynôme $Q(z)$ est premier avec

$$2P(z) - (a+b) = \big(P(z) - a\big) + \big(P(z) - b\big).$$

Donc, l'équation (1.1.3) implique que $Q(z) \mid P'(z)$. Si on pose maintenant

$$q_\sigma(z) = \frac{P'(z)}{nQ(z)},$$

on retrouve l'équation (1).

L'implication 3) $\Rightarrow$ 2) est évidente. □

On désigne par Σ l'ensemble de toutes les paires (P, I) composées d'un polynôme $P(z)$ et d'un segment $I = [a, b]$, $a \neq b$, et par $\Sigma_{g,n}$ le sous-ensemble de Σ se composant des paires $\sigma = (P, I)$ qui se trouvent dans la g-ième strate de la stratification abélienne et pour lesquelles $\deg P(z) = n$. Les paires $\sigma = (P, I), \widehat{\sigma} = (\widehat{P}, \hat{I}) \in \Sigma$ seront dites équivalentes s'il existe des fonctions linéaires γ_1, γ_2 telles que

$$P(z) = \gamma_1\big(\widehat{P}(\gamma_2(z))\big) \quad \text{et} \quad I = \gamma_1(\hat{I}).$$

On note $\widetilde{\Sigma}$, $\widetilde{\Sigma}_{g,n}$ les ensembles des classes d'équivalence de Σ, $\Sigma_{g,n}$ respectivement.

1.2. Polynômes de Chebyshev et description de $\widetilde{\Sigma}_{0,n}$.

On note $T_n(z)$ le n-ième polynôme de Chebyshev,

$$T_n(z) = \cos(n \arccos z).$$

Pour la paire $\tau = (T_n, I_1)$, où[1] $I_1 = [-1, 1]$, le graphe G_τ est un graphe linéaire à n arêtes (voir fig. 1) ayant comme sommets les points de l'axe réel de coordonnée $\cos i\frac{\pi}{n}$, $i = 0, \ldots, n$, ainsi $\tau \in \Sigma_{0,n}$.

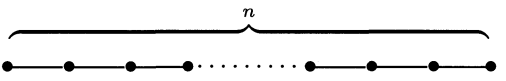

Figure 1

[1] Dans toute la suite on fixe la notation $T_n(z)$ pour le n-ième polynôme de Chebyshev et la notation I_1 pour le segment $[-1, 1]$.

THÉORÈME 1. — *Chaque paire* $(P, I) \in \Sigma_{0,n}$ *est équivalente à* (T_n, I_1).

Démonstration. — Il est clair que chaque paire $(P, I) \in \Sigma_{0,n}$ est équivalente à une paire $\hat{\tau} = (\widehat{P}, I_1)$ telle que les sommets de valence 1 du graphe $G_{\hat{\tau}}$ sont ± 1. En utilisant la proposition, on conclut que $\widehat{P}(z)$ satisfait l'équation

$$\widehat{P}^2(z) - \frac{\widehat{P}'^2(z)}{n^2}(z-1)(z+1) = 1. \tag{1.2.1}$$

On considère la courbe algébrique $L : z^2 + w^2 = 1$ et son adhérence projective $\bar{L} \cong \mathbb{P}^1$. En réécrivant l'équation (1.2.1) comme

$$\left(\widehat{P}(z) + i\frac{\widehat{P}'(z)}{n}w\right)\left(\widehat{P}(z) - i\frac{\widehat{P}'(z)}{n}w\right) = 1, \tag{1.2.2}$$

on voit que la fonction

$$\psi(z, w) = \widehat{P}(z) + i\frac{\widehat{P}'(z)}{n}w$$

n'a ni pôles ni zéros sur la partie affine de $\bar{L}$. Donc elle a un zéro en un des deux points de $\bar{L} \setminus L$ et un pôle en l'autre. De plus, l'ordre du pôle aussi bien que l'ordre du zéro est égal à $n = \deg \widehat{P}(z)$. Puisque pour les fonctions $(z \pm iw)^n$ ces conditions sont aussi satisfaites, il existe $c \in \mathbb{C}$ tel que $\psi(z, w) = c(z \pm iw)^n$ sur L. En utilisant l'égalité (1.2.2), on a

$$\psi(z, w)\psi(z, -w) = c^2(z + iw)^n(z - iw)^n = c^2 = 1,$$

d'où $c = \pm 1$. Donc

$$\widehat{P}(z) = \pm\frac{1}{2}\left((z + iw)^n + (z - iw)^n\right)$$

dans l'anneau $\mathbb{C}[z, w]/(w^2 + z^2 - 1)$. Comme la courbe L peut être paramétrisée par les fonctions $\cos\varphi$ et $\sin\varphi$, le dernière égalité implique que $\widehat{P}(z) = \pm T_n(z)$. □

1.3. Stratification abélienne et points de n-division.

On rappelle qu'une courbe hyperelliptique est une surface de Riemann compacte H qui est une normalisation d'une courbe dont l'équation affine est $w^2 = R(z)$, où le polynôme $R(z)$ n'a que des racines simples. Dans toute la suite on suppose que ∞ n'est pas un point de branchement de H, ce

qui est équivalent à la condition que le degré de $R(z)$ est pair. Il est bien connu (voir, par exemple, [GH]) que les courbes $w^2 = R_1(z)$ et $w^2 = R_2(z)$ sont isomorphes si et seulement s'il existe une homographie $\gamma : \mathbb{CP}^1 \to \mathbb{CP}^1$ qui transforme l'ensemble des racines de $R_1(z)$ en celui de $R_2(z)$. On note $\rho = (z, w)$ un point de H et soit $\rho \mapsto \rho' = (z, -w)$ l'involution canonique. On dit que le point ρ est de n-division, si ρ n'est pas un point de ramification de H et le diviseur $n(\rho - \rho')$ est principal. On note $\widetilde{H}_{g,n}$ l'ensemble des classes d'isomorphisme des paires (H, ρ) se composant d'une courbe hyperelliptique H de genre g et d'un point de n-division $\rho \in H$. On remarque que pour chaque paire (H, ρ), l'involution canonique donne l'isomorphisme de (H, ρ) avec la paire (H, ρ').

On définit l'application

$$\chi : \widetilde{\Sigma}_{g,n} \longrightarrow \widetilde{H}_{g,n}.$$

Pour cela on choisit dans la classe $\widetilde{\sigma} \in \widetilde{\Sigma}_{g,n}$ un représentant σ et on considère la courbe hyperelliptique H_σ définie par l'équation $w^2 = R_\sigma(z)$, où $R_\sigma(z)$ est le polynôme de l'équation (1.1.1), et un des deux points sur H_σ se trouvant au-dessus de l'infini. On associe maintenant à la classe $\widetilde{\sigma}$, la classe d'isomorphisme de la paire (H_σ, ρ_∞). Pour s'assurer que la définition ci-dessus est correcte, on remarque tout d'abord que si σ est équivalente à $\widehat{\sigma}$, alors $R_{\hat{\sigma}}(z) = R_\sigma(\gamma(z))$, où $\gamma(z)$ est une fonction linéaire, ce qui implique l'isomorphisme $(H_\sigma, \rho_\infty) \cong (H_{\hat{\sigma}}, \rho_\infty)$. Pour s'assurer que le point ρ_∞ sur la courbe H_σ est effectivement de n-division, on considère la fonction

$$(1.3.1)\quad \Psi_\sigma(z, w) = P(z) + Q(z)w - \frac{1}{2}(a+b) = P(z) + \frac{P'(z)}{nq_\sigma(z)}w - \frac{1}{2}(a+b).$$

En utilisant l'équation (1.1.2), on a :

$$\begin{aligned}
\mathrm{d}\Psi_\sigma &= \mathrm{d}P + w\,\mathrm{d}Q + Q\,\mathrm{d}w = \mathrm{d}P + w\,\mathrm{d}Q + Q\frac{\mathrm{d}R_\sigma}{2w} \\
&= \frac{1}{2w}(2w\,\mathrm{d}P + 2R_\sigma\,\mathrm{d}Q + Q\,\mathrm{d}R_\sigma) \\
&= \frac{1}{2wQ}\left(2wQ\,\mathrm{d}P + \mathrm{d}(Q^2R_\sigma)\right) \\
&= \frac{1}{2wQ}(2wQ\,\mathrm{d}P + 2P\,\mathrm{d}P - (a+b)\,\mathrm{d}P) \\
&= \frac{\mathrm{d}P}{Q}\frac{1}{w}\Psi_\sigma.
\end{aligned}$$

Il s'ensuit que

$$\frac{\mathrm{d}\Psi_\sigma}{\Psi_\sigma} = nq_\sigma \frac{\mathrm{d}z}{w}. \tag{1.3.2}$$

Comme la forme $\dfrac{\mathrm{d}z}{w}$ n'a pas de pôles sur H_σ et $\operatorname{div}_\infty q_\sigma(z) = g(\rho_\infty + \rho'_\infty)$, on conclut que la forme $\dfrac{\mathrm{d}\Psi_\sigma}{\Psi_\sigma}$ n'a que deux pôles au-dessus de l'infini avec les résidus $\pm n$, ce qui implique que le point ρ_∞ est de n-division. Enfin, il est bien connu que le genre de H_σ est égal à g.

THÉORÈME 2. — *L'application $\chi : \widetilde{\Sigma}_{g,n} \to \widetilde{H}_{g,n}$ est bijective. Pour la paire $\sigma = (P, I_1)$, l'ordre du diviseur $\rho_\infty - \rho'_\infty$ dans le groupe $\operatorname{Pic} H_\sigma$ est égal au minimum des degrés des polynômes $S(z)$ tels que $P(z)$ peut être mis sous la forme d'une composition $P(z) = \pm T_d(S(z))$.*

Démonstration. — Pour s'assurer de l'injectivité de χ, on note tout d'abord que, si pour les paires $\widehat{\sigma} = (\widehat{P}, I_1)$, $\sigma = (P, I_1)$ on a $R_{\widehat{\sigma}}(z) = R_\sigma(z)$ et $\deg \widehat{P}(z) = \deg P(z)$, alors $\widehat{P}(z) = \pm P(z)$. En effet, de la même façon que dans la démonstration du théorème 1, dans ce cas on obtient l'égalité $\Psi_{\widehat{\sigma}}(z, w) = \pm\Psi_\sigma(z, \pm w)$ sur H_σ et comme

$$P(z) = \frac{1}{2}\big(\Psi_\sigma(z, w) + \Psi_\sigma(z, -w)\big), \quad \widehat{P}(z) = \frac{1}{2}\big(\widehat{\Psi}_{\widehat{\sigma}}(z, w) + \widehat{\Psi}_{\widehat{\sigma}}(z, -w)\big),$$

on en conclut que $\widehat{P}(z) = \pm P(z)$. Supposons maintenant que pour les paires $\widehat{\sigma} = (\widehat{P}, \hat{I})$, $\sigma = (P, I) \in \Sigma_{g,n}$, on a $(H_{\hat{\sigma}}, \rho_\infty) \cong (H_\sigma, \rho_\infty)$. Il est clair que sans restreindre la généralité, on peut supposer que $\hat{I} = I = I_1$. L'isomorphisme $H_{\hat{\sigma}} \cong H_\sigma$ implique qu'il existe une homographie γ telle que les polynômes $R_{\widehat{\sigma}}(z)$ et $R_\sigma(\gamma(z))$ ont les mêmes racines. En outre, puisque les points des courbes $H_{\hat{\sigma}}$, H_σ se trouvant au-dessus de l'infini s'envoient les uns sur les autres, on a $\gamma(\infty) = \infty$, et, donc, γ est une fonction linéaire. Pour les paires $\widehat{\sigma} = (\widehat{P}, I_1)$ et $\sigma_\gamma = (P(\gamma), I_1)$ on a $R_{\hat{\sigma}}(z) = R_{\sigma_\gamma}(z)$. Ceci implique l'égalité $\widehat{P}(z) = \pm P(\gamma(z))$ et, par conséquent, l'injectivité de l'application χ.

Soit maintenant (H, ρ) la paire composée de la courbe H définie par l'équation $w^2 = R(z)$ et du point de n-division ρ qu'on peut supposer se trouvant au-dessus de l'infini. Soit $\Psi(z, w)$ une fonction sur H pour laquelle $\operatorname{div}\Psi(z, w) = n(\rho - \rho')$. On a

$$\Psi(z, w) = P(z) + Q(z)w,$$

où $P(z)$, $Q(z)$ sont des fonctions rationnelles. Puisque la fonction $\Psi(z,w)\Psi(z,-w)$ n'a ni zéros ni pôles sur H, c'est une constante que l'on peut estimer égale à 1. En outre, comme tous les pôles de la fonction $P(z) = \frac{1}{2}(\Psi(z,w) + \Psi(z,-w))$ sur H se trouvent au-dessus de ∞, $P(z)$ doit être un polynôme. L'équation

$$P^2(z) - Q^2(z)R(z) = 1$$

implique à présent que $Q(z)$ est aussi un polynôme, car $R(z)$ n'a que des racines simples. Puisque pour la paire $\sigma = (P, I_1)$ on a évidement $(H_\sigma, \rho_\infty) = (H, \rho)$, l'application χ est surjective.

Pour finir la démonstration du théorème on note que le diagramme

$$\begin{array}{ccccc} (S, I_1) & \in & \widetilde{\Sigma}_{g,n} & \xrightarrow{\chi} & \widetilde{H}_{g,n} \ni (H, \rho_\infty) \\ \downarrow & & \downarrow & & \downarrow \quad \downarrow \\ (T_d \circ S, I_1) & \in & \widetilde{\Sigma}_{g,dn} & \xrightarrow{\chi} & \widetilde{H}_{g,dn} \ni (H, \rho_\infty) \end{array}$$

est commutatif puisque pour la paire $(T_d \circ S, I_1)$, le graphe correspondant a même ensemble de sommets de valences impaires que celui de la paire (S, I_1). L'assertion sur l'ordre du diviseur $\rho_\infty - \rho'_\infty$ résulte alors de la bijectivité de χ et du fait que cet ordre divise n. □

Si $g = 1$, au lieu des paires composées d'une courbe elliptique définie par une équation du quatrième degré et d'un point de n-division, il est plus commode, parfois, de considérer des paires composées d'une courbe elliptique sous la forme de Weierstrass et d'un point d'ordre fini. Le passage nécessaire peut être réalisé par les formules

$$(z,y) = \Big(\frac{1}{2}\Big(\frac{B+w}{A-v}\Big), 2v + A - \frac{1}{4}\Big(\frac{B+w}{A-v}\Big)^2\Big) \tag{1.3.3}$$

qui donnent un isomorphisme birationnel entre la courbe elliptique X définie par l'équation

$$y^2 = R(z) = z^4 - 6Az^2 + 4Bz + C \tag{1.3.4}$$

et la courbe elliptique E définie par l'équation

$$w^2 = 4v^3 - g_2 v - g_3, \tag{1.3.5}$$

où

$$g_2 = 3A^2 + C, \quad g_3 = -AC + A^3 - B^2.$$

Il est facile de voir que l'un des deux points $\rho_\infty, \rho'_\infty$ sur la courbe X correspond au point (A, B) sur E, et l'autre à l'élément neutre de la loi de groupe. De plus, il est clair que l'ordre du diviseur $\rho_\infty - \rho'_\infty$ dans $\operatorname{Pic} X$ est égal à l'ordre du point (A, B) sur E.

Exemple. — On considère le cas $n = 2$, $g = 1$. Le théorème 1 implique que chaque paire (P, I) où $\deg P(z) = 2$ se trouve dans $\Sigma_{1,2}$ pourvu qu'elle ne soit pas équivalente à (T_2, I_1). De plus, chaque telle paire est équivalente à une paire (P_c, I_1) où $P_c = z^2 + (2c - 1)$, $c \in \mathbb{C}$, et, comme il est facile de vérifier, deux paires (P_c, I_1) et $(P_{c'}, I_1)$ sont équivalentes si et seulement si $c = c'$ ou $c = 1 - c'$. C'est pourquoi on peut identifier l'ensemble $\widetilde{H}_{1,2}$ et l'ensemble des orbites de l'action du groupe engendré par la transformation $\lambda \mapsto 1 - \lambda$ sur $\mathbb{C} \setminus \{0, 1\}$. D'autre part, l'ensemble des orbites de l'action du groupe Γ qui consiste en les substitutions

$$\lambda, \quad \frac{1}{\lambda}, \quad 1 - \lambda, \quad \frac{1}{1 - \lambda}, \quad \frac{\lambda}{\lambda - 1}, \quad \frac{\lambda - 1}{\lambda}$$

sur $\mathbb{C} \setminus \{0, 1\}$ peut être identifié à l'ensemble des classes d'isomorphisme des courbes elliptiques (sans structure supplémentaire). Le sous-groupe de Γ engendré par la transformation $\lambda \mapsto 1 - \lambda$ est d'indice 3, ce qui s'explique par le fait que chaque courbe elliptique a justement trois points d'ordre 2.

1.4. Remarques.

L'équation (1.1.2) est probablement apparue pour la première fois dans l'article d'Abel [Ab] consacré aux intégrales pseudo-elliptiques. En particulier, Abel a démontré que cette équation avec R_σ fixé, a une solution polynomiale P, Q, si et seulement si la fraction continue

$$\sqrt{R_\sigma} = r_0 + \frac{1|}{|r_1} + \frac{1|}{|r_2} + \cdots + \frac{1|}{|r_n} + \cdots$$

où $r_i \in \mathbb{C}[z]$ est périodique. Un autre problème classique qui se ramène à l'équation d'Abel est le suivant : pour une réunion des segments $K \subset \mathbb{R}$ retrouver un polynôme réel unitaire $P(x)$ *s'écartant le moins possible de zéro sur* K parmi tous les polynômes réels unitaires de degré n (voir, par exemple, [SoYu]). On remarque, en outre, que l'équation d'Abel avec $R(x) \in \mathbb{R}[x]$ (ou bien les courbes hyperelliptiques réelles ayant des points de n-division) apparaît aussi dans la théorie des systèmes intégrables [MM].

Le lien entre l'équation d'Abel et les points de n-division sur des courbes hyperelliptiques (surtout dans le cas où $\deg R_\sigma = 4$) est bien connu.

Ce lien dans des contextes différents a été étudié dans [AR], [Ber], [Jun], [Hal], [HL], [HBJ], [MM], [Pay], [P1], [Shin]. En particulier, dans [Jun], [HBJ], dans le cas où $\deg R_\sigma = 4$, un résultat similaire au théorème 2 a été obtenu[(2)].

Comme on l'a vu, la question sur la solubilité de l'équation (1.1.2) pour $\deg R_\sigma = 4$ est équivalente à la question suivante : *le point* (A, B) *sur la courbe elliptique* E *est-il d'ordre fini ?* Il est curieux de remarquer, que pour le cas où les coefficients de R_σ sont contenus dans le corps $\mathbb{Q}$, un critère *effectif* de résolubilité de l'équation (1.1.2) a été déjà donné en 1861 par Chebyshev [Ch] (voir aussi [Zol]).

2. ARBRES DE GENRE ABÉLIEN 1

2.1. Théorie des "dessins d'enfants" et stratification abélienne.

Dans [Gr], A. Grothendieck a établi une correspondance fondamentale entre les classes isotopiques de « dessins » sur les modèles topologiques des surfaces de Riemann compactes et les classes d'isomorphisme de « paires propres de Belyi ». On va donner une description très courte de certaines définitions et résultats qu'on utilisera par la suite et dont une discussion détaillée peut être retrouvée dans [Schn], [ShVo], [ShZv].

• *Une fonction propre de Belyi* sur une courbe C est une application rationnelle $\beta : C \to \mathbb{CP}^1$ ramifiée seulement au-dessus de $0, 1, \infty$ telle que l'indice de ramification en chacun des points au-dessus de 1 est exactement 2. D'après le théorème de Belyi [Be], une telle fonction existe si et seulement si C est définie sur $\overline{\mathbb{Q}}$.

• *Une paire propre de Belyi* est une paire (C, β) composée d'une courbe C et d'une fonction propre de Belyi β sur cette courbe.

Deux paires de Belyi (C, β) et $(\widehat{C}, \widehat{\beta})$ sont dites isomorphes s'il existe l'isomorphisme $\gamma : C \to \widehat{C}$ tel que $\beta = \widehat{\beta} \circ \gamma$. Si (C, β) est une paire propre de Belyi, alors l'image réciproque $\beta^{-1}[0, 1]$ du segment $[0, 1]$ est un graphe connexe dont les sommets correspondent aux zéros de β avec pour multiplicité la valence au sommet. De plus, la fonction β prend une et une seule fois la valeur 1 sur chaque arête. Enfin, sur chaque face de ce graphe se trouve un pôle de β dont la multiplicité est égale au nombre de segments

(2) L'auteur remercie A.P. Veselov qui lui fit observer cela.

qui bordent la face. Le graphe ci-dessus[3] est un représentant de la classe isotopique des «dessins» qui correspond à la classe d'isomorphisme de la paire (C, β).

Dans cet article, on travaille au fond dans le cas particulier de la correspondance entre les dessins et les paires de Belyi où la surface de Riemann est une sphère et les dessins sont des arbres. Dans ce cas, la correspondance ci-dessus admet une simplification décrite dans [ShVo]. À savoir, au lieu des fonctions de Belyi, il est plus commode de considérer des polynômes qui n'ont que deux valeurs critiques (finies) sans contraintes sur les indices de ramification aux points au-dessus de ces valeurs critiques. De tels polynômes sont dits *polynômes de Shabat.* On identifie l'ensemble des polynômes de Shabat avec l'ensemble des paires $(P, I) \in \Sigma$ composées d'un polynôme de Shabat $P(z)$ et du segment I qui joint ses valeurs critiques, et on note $S\Sigma, S\Sigma_{g,n}$ (resp. $S\widetilde{\Sigma}, S\widetilde{\Sigma}_{g,n}$) les sous-ensembles correspondants dans $\Sigma, \Sigma_{g,n}$ (resp. dans $\widetilde{\Sigma}, \widetilde{\Sigma}_{g,n}$). Le passage entre les fonctions de Belyi et les polynômes de Shabat se réalise de la façon suivante. Soit λ est un arbre. Alors puisqu'un arbre n'a qu'une face, chaque fonction de Belyi de la classe d'isomorphisme correspondante n'a qu'un pôle. Donc dans cette classe il existe une fonction β qui est un polynôme. Comme l'indice de ramification en chacun des points au-dessus de 1 de fonction β est exactement 2, on a $\beta(z) = 1 - P^2(z)$, où $P(z)$ est un polynôme de Shabat (dont toute valeur critique est dans $\{\pm 1\}$).

On désigne par Λ l'ensemble des classes d'équivalence isotopique des arbres planaires et par $\Lambda_{g,n}$ le sous-ensemble de Λ se composant des arbres à n arêtes dont le nombre de sommets de valence impaire[4] est $2g + 2$. La bijection entre les classes isotopiques des arbres et les classes d'isomorphisme des fonctions propres de Belyi correspondantes, induit la bijection $\alpha : \Lambda_{g,n} \to S\widetilde{\Sigma}_{g,n}$ qu'on peut visualiser de façon connue : si $\sigma = (P, I) \in S\Sigma$, alors G_σ est l'arbre correspondant (par abus de langage on appellera souvent arbre, un représentant de la classe d'équivalence isotopique des arbres planaires). Dans toute la suite on supposera que les valeurs critiques des polynômes de Shabat considérés sont $\{\pm 1\}$. L'exemple le plus simple de polynôme de Shabat est le polynôme de Chebyshev $T_n(z)$ dont l'arbre correspondant est un graphe linéaire à n arêtes représenté sur la figure 1[5].

---

(3) On remarque que la construction de ce graphe est un peu différente de celle du graphe G_σ de la première partie.

(4) On remarque que ce nombre est toujours pair.

(5) D'après l'existence de la bijection α, ce fait peut être utilisé pour une autre

La rationalité de $0, 1, \infty$ implique que dans la classe d'équivalence des fonctions de Belyi il existe des fonctions à coefficients algébriques. Donc on peut définir l'action du groupe $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ sur l'ensemble Λ. À savoir, pour $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ et $\lambda \in \Lambda$, on choisit dans la classe correspondante des fonctions de Belyi, une fonction β à coefficients algébriques et on définit $\sigma(\lambda)$ comme l'arbre qui correspond à la classe d'équivalence des fonctions de Belyi contenant la fonction $\sigma(\beta)$, qui est aussi évidemment une fonction de Belyi. Il est facile de vérifier que la définition ci-dessus ne dépend pas du choix de la fonction β. Puisque pour chaque arbre λ son orbite est finie, le stabilisateur $\mathrm{St}(\lambda)$ est d'indice fini dans $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Donc, d'après le théorème principal de la théorie de Galois, le corps k_λ des nombres algébriques qui sont invariants par l'action de $\mathrm{St}(\lambda)$, est une extension finie de $\mathbb{Q}$. Le corps k_λ s'appelle *corps des modules* de λ.

Soit λ un arbre à n arêtes. Alors on peut munir λ d'une *structure bicolore*, ce qui correspond à la peinture des images réciproques des extrémités du segment I de couleurs différentes, par exemple, blanc et noir. Si $u = u_1, u_2, \ldots, u_r$ (resp. $v = v_1, v_2, \ldots, v_q$) est la suite des valences des sommets blancs (resp. noirs) de l'arbre λ dans l'ordre décroissant, on dit que l'arbre est du *type* $(u; v)$. On note que $\sum_{\ell=1}^{r} u_\ell = \sum_{\ell=1}^{q} v_\ell = n$. Il est clair que si deux arbres bicolores qui sont de types $(u; v)$ et $(\hat{u}; \hat{v})$ respectivement, se trouvent dans la même orbite par l'action du groupe $\mathrm{Gal}(\widehat{\mathbb{Q}}/\mathbb{Q})$, alors soit $u = \hat{u}, v = \hat{v}$, soit $u = \hat{v}, v = \hat{u}$. Si deux arbres sont de même type on dit qu'ils se trouvent dans la même *orbite combinatoire*.

On définit maintenant l'application

$$\varphi : \Lambda_{g,n} \longrightarrow \widetilde{H}_{g,n}.$$

Pour $\lambda \in \Lambda_{g,n}$ on pose $\varphi(\lambda) = \chi(\alpha(\lambda))$, où χ est l'application du théorème 2. D'après le résultat de J.-M. Couveignes [Couv], pour chaque arbre λ dans la classe des fonctions de Belyi correspondante, il existe un polynôme β dont les coefficients sont contenus dans k_λ. Donc *dans la classe* $\varphi(\lambda)$ *il existe une courbe* $w^2 = R(z)$ *telle que* $R(z) \in k_\lambda$. En effet, si les coefficients du polynôme $\beta(z) = 1 - P^2(z)$ sont éléments du corps k_λ, alors les coefficients du polynôme $R(z)$ qui a comme racines (simples) toutes les racines de multiplicité impaire de β, sont aussi contenus dans k_λ. Pour un arbre λ on définit ses *genre abélien* et *ordre abélien* respectivement comme le genre de la courbe H et l'ordre du diviseur $\rho - \rho'$ dans le groupe $\mathrm{Pic}\, H$ pour un

---

démonstration du théorème 1.

représentant $(H, \rho) \in \varphi(\lambda)$. Il est clair que l'ordre abélien est invariant par l'action du groupe $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ sur Λ.

On note que si $\beta(z) = 1 - P^2(z)$ est une fonction de Belyi qui correspond à un arbre $\lambda \in \Lambda_{g,n}$ et H_σ est une courbe hyperelliptique qui correspond à la paire $\sigma = (P, I_1)$, alors la composition $\widehat{\beta} = \beta \circ \pi$, où $\pi : H_\sigma \to \mathbb{CP}^1$ est une projection canonique, est une fonction de Belyi sur H_σ. En effet, des valeurs critiques de π coïncident avec des racines du polynôme $R_\sigma(z)$ et l'équation (1.1.1) implique que la valeur de $\beta(z)$ en chacun de ces points est égale à 0. Le dessin qui correspond à $\widehat{\beta}$ a deux faces, $2n$ arêtes et $2n - 2g$ sommets.

2.2. Calcul d'ordre abélien.

Soit λ un arbre à n arêtes de genre abélien 1. Alors λ est de l'une des deux espèces suivantes :

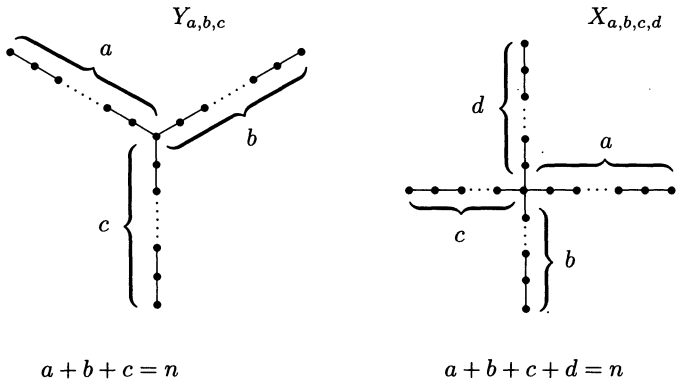

Figure 2

D'après l'isomorphisme (1.3.3), à partir d'un tel arbre on obtient une courbe elliptique sous la forme de Weierstrass E_λ définie sur k_λ avec un point de n-division $(A, B)_\lambda \in E(k_\lambda)$.

Exemple. — En utilisant le catalogue [BPZ] et les formules (1.3.3), il est facile de vérifier que les arbres qui sont représentés sur la figure 3 (ayant comme corps de modules $\mathbb{Q}$), donnent le point $(v, w) = (21, -243)$ sur la courbe elliptique $w^2 = 4v^3 + 540v + 10665$ qui est d'ordre 5, et le point $(v, w) = (3, -16)$ sur la courbe $w^2 = 4v^3 + 84v - 104$ qui est d'ordre 3 respectivement.

Figure 3

Le problème que l'on va traiter est le suivant : *à partir de la structure combinatoire de l'arbre λ définir son ordre abélien.* On rappelle que d'après le théorème 2, cet ordre est égal au minimum des degrés des polynômes $\widehat{P}(z)$ tels que $P(z) = \pm T_\ell(\widehat{P}(z))$, où $P(z)$ est un polynôme de Shabat qui correspond à l'arbre λ.

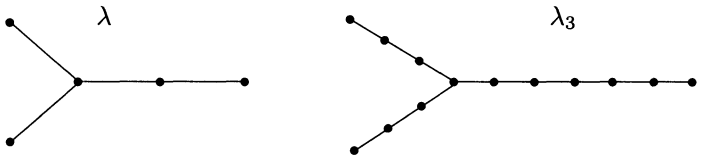

Figure 4

On remarque que pour chaque polynôme de Shabat $P(z)$, le polynôme $T_k(P(z))$ est aussi un polynôme de Shabat et si à $P(z)$ correspond l'arbre λ, alors à $T_k(P(z))$ correspond l'arbre λ_k obtenu à partir de λ par l'addition de $k-1$ nouveaux sommets de valence deux sur chaque arête de λ[6] (voir fig. 4). Cependant, le fait que $T_k(P(z))$ est un polynôme de Shabat n'implique pas en général que $P(z)$ est aussi un polynôme de Shabat mais implique seulement que l'ensemble des valeurs critiques de $P(z)$ est inclus dans l'ensemble $\cos \ell \frac{\pi}{k}$, $\ell = 0, \ldots, k$.

On note $(a_1, a_2, \ldots, a_\ell)$ le PGCD des nombres $a_1, a_2, \ldots, a_\ell$.

THÉORÈME 3. — *Soit λ un arbre à n arêtes de genre abélien 1. Alors l'ordre abélien de λ est égal à $n/(a,b,c)$ si $\lambda = Y_{a,b,c}$ et à $n/(a+b, b+c, c+d, d+a)$ si $\lambda = X_{a,b,c,d}$.*

Démonstration. — Soit $\lambda = Y_{a,b,c}$ avec $(a,b,c) = k$. On considère alors l'arbre $\hat{\lambda} = Y_{a/k,b/k,c/k}$ et le polynôme de Shabat correspondant $\widehat{P}(z)$.

---

(6) C'est un cas particulier de ce qu'on appelle *la composition des arbres* (voir [ShZv], [AdZv]).

Puisque le polynôme $T_k(\widehat{P}(z))$ représente l'arbre λ, on a $\operatorname{ord}\lambda \mid (n/k)$. D'autre part, si on a l'égalité $P(z) = \pm T_\ell(\widehat{P}(z))$ pour le polynôme $P(z)$ qui représente l'arbre $\lambda = Y_{a,b,c}$, alors le polynôme $\widehat{P}(z)$ est aussi un polynôme de Shabat. En effet, si $\widehat{P}(z)$ avait des valeurs critiques distinctes de ± 1 alors l'arbre λ aurait des sommets de valence paire distincte de 2. De plus, il est clair que le polynôme $\widehat{P}(z)$ correspond à un arbre $\hat{\lambda} = Y_{\hat{a},\hat{b},\hat{c}}$. Donc $\{a,b,c\} = \{\ell\hat{a}, \ell\hat{b}, \ell\hat{c}\}$, d'où il suit que $\ell \mid k$, et, par conséquent, $\operatorname{ord}\lambda = n/k$, ce qui prouve le théorème dans le cas où $\lambda = Y_{a,b,c}$.

Soient maintenant $\lambda = X_{a,b,c,d}$ et $P(z)$ le polynôme de Shabat correspondant. Si $(a,b,c,d) = \ell > 1$, alors on conclut comme ci-dessus que $P(z) = \pm T_\ell(\widehat{P}(z))$, où $\widehat{P}(z)$ est un polynôme de Shabat qui représente l'arbre $\hat{\lambda} = X_{a/\ell,b/\ell,c/\ell,d/\ell}$. Donc il suffit de prouver le théorème pour le cas où $(a,b,c,d) = 1$.

Supposons que $P(z) = \pm T_m(\widehat{P}(z))$. On prouve que cette hypothèse implique que $m \mid (a+b, b+c, c+d, d+a)$. Comme la condition $(a,b,c,d) = 1$ entraîne que $\widehat{P}(z)$ n'est pas un polynôme de Shabat, $\widehat{P}(z)$ a un point critique x tel que $\widehat{P}(x) \neq \pm 1$. Par ailleurs, comme $\deg q_{\tilde{\sigma}} = 1$, l'équation (1.1.1) implique que le polynôme $\widehat{P}(z)$ ne peut pas avoir plus d'un tel point et que la multiplicité du polynôme $\widehat{P}(z)$ en ce point est égale à deux. De plus, $P(x) \in L$, où $L = \{\cos i\frac{\pi}{m}, i = 0, \ldots, m\}$. Enfin, il est clair qu'en les points critiques du polynôme $\widehat{P}(z)$ de valeur ± 1, la multiplicité est aussi égale à 2.

L'égalité $P(z) = \pm T_m(\widehat{P}(z))$ signifie géométriquement que l'arbre λ se réalise comme l'image réciproque du graphe linéaire m-arêtes G_τ, $\tau = (T_m, I_1)$. On dessine G_τ et λ, en supposant, sans restreindre la généralité, que λ est inclus dans l'union des axes (voir fig. 5). On numérote les sommets de G_τ par les nombres de 1 à $m+1$ à partir de la droite. Cette numérotation induit une numérotation des sommets de λ. On considère le sommet de l'arbre λ de coordonnée maximale sur l'axe réel. Ce sommet est soit de numéro 1 soit de numéro $m+1$. On suppose qu'il est de numéro 1, le cas où il est de numéro $m+1$ peut être analyser de manière analogue. On avance le long de l'axe réel dans la direction $-\infty$. Il est clair que les numéros des sommets passés croissent de façon monotone jusqu'au moment où l'on retrouve un sommet qui est un point critique pour le polynôme $\widehat{P}(z)$. Soit y un tel premier sommet. Si $y \neq 0$ alors y est de numéro $m+1$. Dans ce cas on continue d'avancer dans la direction $-\infty$. Maintenant les numéros des sommets passés décroissent de façon monotone jusqu'au point critique suivant, car la multiplicité de $\widehat{P}(z)$ en y est égale à deux. En

continuant d'avancer de la même manière, à un certain moment on arrive au point zéro. On commence alors à avancer le long de l'axe imaginaire dans la direction $-i\infty$. Puisque zéro est un point critique de $\widehat{P}(z)$ d'ordre 2 et $\widehat{P}(0) \neq \pm 1$, les numéros des sommets passés continueront soit à croître de façon monotone soit à décroître de façon monotone selon leur conduite avant le passage par zéro. À un moment, on arrive au sommet de λ de coordonnée minimale sur l'axe imaginaire. Puisque le numéro de ce point est égal soit à 1 soit à $m+1$ notre construction implique que $m \mid (a+b)$ (en notation de fig. 2). Les faits que $m \mid (b+c)$, $m \mid (c+d)$, $m \mid (d+a)$ se démontrent de manière analogue.

Par contre, on prouve que si $m|(a+b, b+c, c+d, d+a)$ alors l'arbre λ peut être représenté par un polynôme de Shabat d'espèce $T_m(\widehat{P}(z))$. Pour cela on dessine λ et G_τ comme avant et on numérote leurs sommets par les nombres de 1 à $m+1$ à partir des sommets de coordonnée maximale (sur l'axe réel) comme si l'arbre λ était déjà l'image réciproque du graphe G_τ (la règle formelle de numérotation des sommets de λ est claire d'après l'étude précédente). On construit la triangulation Δ_1 (resp. Δ_2) de la sphère de Riemann en joignant chaque sommet de λ (resp. de G_τ) de valence i, $i = 1, 2, 4$, avec le point ∞ par i segments (voir fig. 5). On prouve par récurrence sur le nombre $t = n/m$ qu'il existe une application *continue* $\widehat{P} : \mathbb{P}^1 \to \mathbb{P}^1$ telle que les triangles de Δ_1 de sommets de numéros j et $j+1$, $(1 \leq j \leq m)$ ont pour images les triangles de Δ_2 de sommets de mêmes numéros en préservant les numéros des sommets de telle façon que la restriction de l'application $\widehat{P} : \mathbb{P}^1 \setminus \widehat{P}^{-1}(L) \to \mathbb{P}^1 \setminus L$ soit un revêtement à t feuillets. En effet, si $t = 2$, alors $a = c$, $b = d$, et on peut poser $\widehat{P}(z) = z^2$.

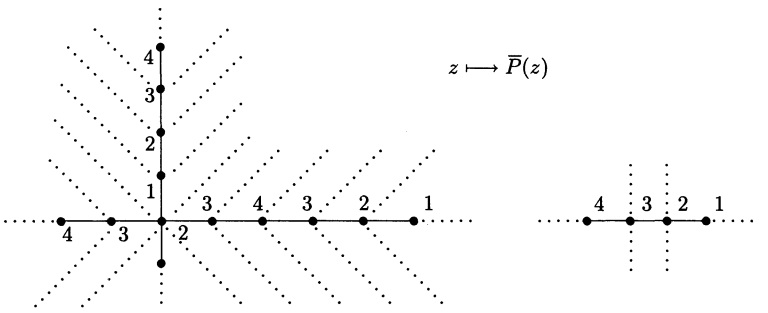

Figure 5

On suppose que notre affirmation soit prouvée pour $t < k$ et on

considère le cas $t = k$. Puisque $k > 2$ et $(a, b, c, d) = 1$, parmi les nombres a, b, c, d il en existe un qui est strictement supérieur à m. On suppose que ce nombre est a. On considère l'arbre $\hat{\lambda} = X_{a-m,b,c,d}$. D'après l'hypothèse de récurrence pour cet arbre il existe une application ayant les propriétés nécessaires et on voit clairement comment on peut la modifier pour obtenir l'application cherchée pour l'arbre λ. Donc une telle application $\widehat{P}(z)$ existe pour chaque arbre qui satisfait la condition $m \mid (a+b, b+c, c+d, d+a)$. Maintenant, d'après le résultat classique de la théorie des fonctions d'une variable complexe, il existe une structure complexe sur $\mathbb{P}^1$ telle que $\widehat{P}$ est holomorphe. Puisque $\widehat{P}^{-1}\{\infty\} = \{\infty\}$, $\widehat{P}$ dans cette structure est un polynôme. Il est clair que le polynôme $T_m(\widehat{P}(z))$ représente l'arbre λ. □

Exemple. — On considère les arbres $\lambda_1 = X_{1,2,4,5}$ et $\lambda_2 = X_{2,2,3,5}$ représentés sur la figure 6. Ces arbres sont dans la même orbite combinatoire qui correspond au type $(4, 2, 2, 2, 1, 1\,;\ 2, 2, 2, 2, 2, 1, 1)$. Pourtant ils ne peuvent pas se trouver dans la même orbite par l'action du groupe $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ puisque l'ordre abélien de λ_1 est égal à 4 et l'ordre de λ_2 est égal à 12.

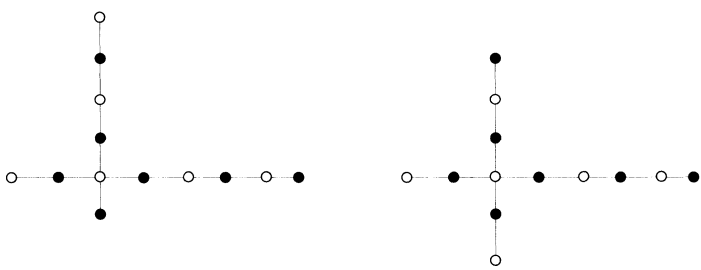

Figure 6

2.3. Arbres de genre abélien 1 et points d'ordre fini sur les courbes elliptiques.

On donne maintenant quelques applications concernant des corps des modules des arbres. Soit λ un arbre de genre abélien 1 et d'ordre abélien n ayant comme corps des modules k_λ. D'après l'isomorphisme (1.3.3), à partir de cet arbre on obtient une courbe elliptique E définie sur k_λ avec un point (A, B) d'ordre n telle que $(A, B) \in E(k_\lambda)$. D'autre part, d'après le résultat de L. Merel [Mer], pour tout corps de nombres k, il existe une borne qui ne dépend que du degré de k sur $\mathbb{Q}$, pour l'ordre d'un point de torsion sur une courbe elliptique définie sur k si les coordonnées de ce point sont aussi contenues dans k. Dans le cas où $k = \mathbb{Q}$, il y a une description complète des

groupes possibles de torsion obtenue par B. Mazur [Maz]. En particulier, d'après le résultat de B. Mazur l'ordre d'un tel point est égal à $2, 3, ..., 10$ ou 12. Ceci implique immédiatement le résultat suivant :

THÉORÈME 4. — *Pour chaque $t \in \mathbb{N}$ il existe $\ell = \ell(t) \in \mathbb{N}$ tel que si λ est un arbre de genre abélien 1 et $\operatorname{ord}\lambda > \ell$ alors $[k_\lambda : \mathbb{Q}] > t$. En particulier, si $\operatorname{ord}\lambda > 12$ alors $[k_\lambda : \mathbb{Q}] > 1$.* □

Dans certains cas à partir d'un arbre λ de genre abélien 1 et d'ordre abélien n on peut obtenir une courbe elliptique E définie sur k_λ avec un point dans $E(k_\lambda)$ d'ordre $2n$. En effet, si ζ_i, $1 \leq i \leq 4$, sont des racines du polynôme $R(z)$ de l'équation (1.3.4) alors comme il est possible de vérifier que les points

$$(A_i, B_i) = \Big(\frac{1}{2}(\zeta_i^2 - A),\ 3A\zeta_i - B - \zeta_i^3\Big), \quad 1 \leq i \leq 4,$$

sont des solutions de l'équation $2x = (A, B)$ dans le groupe E. En particulier, si n est un nombre pair alors l'ordre de (A_i, B_i), $1 \leq i \leq 4$, est égal à $2n$. D'autre part, pour l'arbre $\lambda = Y_{a,b,c}$ le polynôme correspondant $R(z) \in k_\lambda[z]$ admet toujours une racine $\zeta \in k_\lambda$ (celle qui correspond au sommet de valence 3).

Comme on l'a vu, l'égalité $P(z) = \pm T_\ell(\widehat{P}(z))$ pour le polynôme $P(z)$ qui correspond à un arbre d'espèce $Y_{a,b,c}$, implique que $\widehat{P}(z)$ est aussi un polynôme de Shabat et que $\widehat{P}(z)$ correspond à un arbre de même espèce. C'est pourquoi le résultat de B. Mazur et les observations faites plus haut impliquent, que pour obtenir la liste complète des arbres d'espèce $Y_{a,b,c}$ dont le corps de modules est $\mathbb{Q}$, il suffit d'obtenir celui pour des arbres dont le nombre des arêtes est égale à $3, 4, 5, 6, 7$ ou 9. Les calculs fait par N. Magot [Mag] montrent qu'entre des arbres d'espèce $Y_{a,b,c}$ d'ordre abélien 9, il n'y a pas d'arbres dont le corps de modules est $\mathbb{Q}$. D'autre part les arbres dont le nombre des arêtes est moins ou égal à 8 et dont le corps de modules est $\mathbb{Q}$, peuvent être retrouvés dans le catalogue [BPZ]. En utilisant ce catalogue on obtient :

THÉORÈME 5. — *Soit $\lambda = Y_{a,b,c}$ un arbre dont le corps de modules est $\mathbb{Q}$. Alors $\{a, b, c\} = \{d\hat{a}, d\hat{b}, d\hat{c}\}$ où $d \in \mathbb{N}$ et le triplet $\{\hat{a}, \hat{b}, \hat{c}\}$ est de l'un des quatre triplets suivants : $\{1, 1, 1\}$, $\{1, 1, 2\}$, $\{1, 2, 2\}$, $\{1, 1, 3\}$.* □

2.4. Description analytique de $\varphi(Y_{a,b,c})$.

Notre prochain but est de donner un critère pour une classe d'isomorphisme $\tilde{h} \in \widetilde{H}_{1,n}$ de se trouver dans l'image $\varphi(Y_{a,b,c})$.

Soient $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ un réseau planaire, $\rho(u)$, $\zeta(u)$, $\sigma(u)$ les fonctions de Weierstrass qui correspondent à L (voir, par exemple, [Ak]),

$$\omega_3 = \omega_1 + \omega_2 \quad \text{et} \quad \eta_i = \zeta(u + \omega_i) - \zeta(u), \quad i = 1, 2, 3.$$

Pour un point $u \in \mathbb{C} \setminus L$, $u = u_1\omega_1 + u_2\omega_2$ on définit, en suivant [La], *une forme de Hecke*

$$G(L, u) = (u_1\eta_1 + u_2\eta_2) - \zeta(u_1\omega_1 + u_2\omega_2).$$

THÉORÈME 6. — *Soient $h = (L, v)$ une paire composée d'un réseau L et d'un point de n-division par rapport à ce réseau $v \in \mathbb{C}$, $\tilde{h} \in \widetilde{H}_{1,n}$ la classe d'isomorphisme correspondante. Les conditions suivantes sont équivalentes :*

1) *$\tilde{h} = \varphi(\lambda)$ pour un arbre $\lambda = Y_{a,b,c}$.*

2) *$G(L, v)$ est une racine du polynôme*

$$z^4 - 6\rho(v)z^2 + 4\rho'(v)z + g_2 - 3\rho^2(v) = 0.$$

3) *$G(L, \theta) = 0$ pour un nombre complexe θ tel que $2\theta \equiv v \pmod{L}$.*

Démonstration. — On note tout d'abord que la classe $\tilde{\tau} \in \widetilde{\Sigma}_{1,n}$ appartient à $\alpha(Y_{a,b,c})$ si et seulement si pour un représentant $\tau = (P, I)$ de $\tilde{\tau}$ le polynôme $q_\tau = (z - x_\tau)$ divise le polynôme $R_\tau(z)$. En effet, dans ce cas l'équation (1.1.1) implique que le polynôme $P(z)$ n'a que deux valeurs critiques donc $\tilde{\tau} = \alpha(\lambda)$ pour un arbre λ. De plus, l'arbre λ a quatre sommets de valence impaire, un desquels est de valence trois d'où $\lambda = Y_{a,b,c}$. Donc pour prouver l'équivalence des conditions 1) et 2), en tenant compte de l'isomorphisme (1.3.3), il suffit de prouver que si la paire τ correspond à la paire h alors $x_\tau = G(L, v)$. Il est connu (voir, par exemple, [TM], p. 94) que la courbe (1.3.4) peut être paramétrisée par les fonctions $\phi(u), \phi'(u)$ où

$$\phi(u) = \frac{1}{2}\frac{\rho'(u) - \rho'(v)}{\rho(u) - \rho(v)} = \zeta(u + v) - \zeta(u) - \zeta(v) \tag{2.2.2}$$

et v est le point dans le parallélogramme des périodes, tel que $\rho(v) = A$, $\rho'(v) = B$. On pose $\widetilde{\Psi}_\tau(u) = \Psi_\tau(\phi(u), \phi'(u))$ où $\Psi_\tau(z, w)$ est une

fonction (1.3.1) sur la courbe (1.3.4) qui correspond à la paire τ. En utilisant l'équation (1.3.2) on obtient :

$$\frac{\widetilde{\Psi}'_\tau(u)}{\widetilde{\Psi}_\tau(u)} = n\big(\phi(u) - x_\tau\big) = n\big(\zeta(u+v) - \zeta(u) - (\zeta(v) + x_\tau)\big).$$

En résolvant cette équation on trouve que

$$\widetilde{\Psi}_\tau(u) = c\Big(\frac{\sigma(u+v)}{\sigma(u)\,\mathrm{e}^{(\zeta(v)+x_\tau)u}}\Big)^n,$$

pour une constante c. Comme $\widetilde{\Psi}_\tau(u)$ est une fonction double-périodique on a $\widetilde{\Psi}_\tau(u+\omega_i) = \widetilde{\Psi}_\tau(u)$, $i = 1, 2$, et, en utilisant le fait que

$$\sigma(u+\omega_i) = -\,\mathrm{e}^{\eta_i(u+\omega_i/2)}\sigma(u),$$

on en conclut que

$$n\big(\eta_1 v - \omega_1(\zeta(v) + x_\tau)\big) = 2\pi i b,$$

$$n\big(\eta_2 v - \omega_2(\zeta(v) + x_\tau)\big) = -2\pi i a,$$

où $a, b \in \mathbb{Z}$. Maintenant la relation de Legendre $\eta_1\omega_2 - \eta_2\omega_1 = 2\pi i$, entraîne que

$$nv = a\omega_1 + b\omega_2,$$
$$n\big(\zeta(v) + x_\tau\big) = a\eta_1 + b\eta_2,$$

d'où il suit que $x_\tau = G(L, v)$.

Pour prouver l'équivalence des conditions 2) et 3), on note que la représentation paramétrique (2.2.2) implique que les racines du polynôme (2.2.1) sont les valeurs de la fonction $\phi(u)$ aux points où la fonction $\phi'(u)$ s'annule. D'autre part, les zéros de fonction $\phi'(u) = \rho(u) - \rho(u+v)$ sont les points $-\frac{1}{2}v$ et $-\frac{1}{2}v + \frac{1}{2}\omega_i$, $i = 1, 2, 3$. On a

$$\begin{aligned} G(L,v) - \phi\Big(-\frac{1}{2}v\Big) &= 2G\Big(L, \frac{1}{2}v\Big) \\ G(L,v) - \phi\Big(-\frac{1}{2}v + \frac{1}{2}\omega_i\Big) &= \frac{a\eta_1 + b\eta_2}{n} - \zeta\Big(\frac{1}{2}v + \frac{1}{2}\omega_i\Big) - \zeta\Big(\frac{1}{2}v - \frac{1}{2}\omega_i\Big) \\ &= \frac{a\eta_1 + b\eta_2}{n} - 2\zeta\Big(\frac{1}{2}v + \frac{1}{2}\omega_i\Big) + \eta_i \\ &= 2G\Big(L, \frac{1}{2}v + \frac{1}{2}\omega_i\Big) \end{aligned}$$

$i = 1, 2, 3$, ce qui entraîne l'équivalence les conditions 2) et 3). □

2.5. Interprétation modulaire de $Y(N)$.

Soient $H = \{\tau \in \mathbb{C} \mid \operatorname{Im}\tau > 0\}$ le demi-plan supérieur et

$$\Gamma_1(N) = \left\{A \subset \mathrm{SL}_2(\mathbb{Z}) \mid A \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \bmod N \right\}.$$

On rappelle que le groupe $\Gamma_1(N)$ admet une action naturelle sur H et les orbites $H \setminus \Gamma_1(N)$ de cette action peuvent être identifiées avec l'ensemble des classes d'isomorphisme des paires composées d'une courbe elliptique avec un point d'ordre exact N. À savoir, à un représentant τ d'une orbite, correspond la classe d'isomorphisme de la paire composée d'une courbe elliptique $L = \mathbb{Z} + \mathbb{Z}\tau$ avec le point $1/N$ (voir, par exemple, [HBJ], app. 1). L'ensemble des orbites $H \setminus \Gamma_1(N)$ admet une structure complexe unique telle que la projection naturelle

$$p : H \longrightarrow H \setminus \Gamma_1(N)$$

est holomorphe. On note $X_1(N)^0$ la surface de Riemann obtenue et $X_1(N)$ sa compactification. Le but de ce paragraphe est de donner une description géométrique de l'ensemble $Y(N)$ des points de $X_1(N)^0$ qui correspondent aux arbres $Y_{a,b,c}$ d'ordre abélien N.

On rappelle qu'une forme modulaire de poids k par rapport au groupe $\Gamma_1(N)$ est une fonction holomorphe sur H telle que

$$\pi(A\tau) = (c\tau + d)^k \pi(\tau) \quad \text{pour chaque} \quad A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(N),$$

qui possède, de plus, certaines conditions de régularité (voir [La]).

La définition implique que si une forme modulaire s'annule en un point $\tau \in H$ alors elle s'annule en chaque point de l'orbite par l'action $\Gamma_1(N)$ sur H qui contient τ. Donc à partir d'un ensemble de zéros $Z(f) \subset H$ d'une forme modulaire $f(\tau)$ on obtient un ensemble $\widehat{Z}(f) \subset X_1(N)^0$.

On pose, avec $q = \mathrm{e}^{\pi i \tau}$,

$$\theta_1(\tau, u) = \frac{1}{i} \sum_n (-1)^n q^{(n+\frac{1}{2})^2} \mathrm{e}^{(2n+1)u\pi i},$$

$$\theta_2(\tau, u) = \sum_n q^{(n+\frac{1}{2})^2} \mathrm{e}^{(2n+1)u\pi i},$$

$$\theta_3(\tau, u) = \sum_n (-1)^n q^{n^2} \mathrm{e}^{2nu\pi i},$$

$$\theta_4(\tau, u) = \sum_n q^{n^2} \mathrm{e}^{2nu\pi i}.$$

THÉORÈME 7. — *$Y(N)$ coïncide avec $\widehat{Z}(\mu)$ où*

$$\mu(\tau) = \frac{\theta_1'(\tau, \frac{1}{2}N)\,\theta_2'(\tau, \frac{1}{2}N)\,\theta_3'(\tau, \frac{1}{2}N)\,\theta_4'(\tau, \frac{1}{2}N)}{\theta_1(\tau, \frac{1}{2}N)\,\theta_2(\tau, \frac{1}{2}N)\,\theta_3(\tau, \frac{1}{2}N)\,\theta_4(\tau, \frac{1}{2}N)}$$

est une forme modulaire de poids 4 par rapport au groupe $\Gamma_1(N)$.

Démonstration. — En effet, on pose

$$G_N(\tau) = G(L, 1/N), \quad \rho_N(\tau) = \rho(L, 1/N), \quad \rho_N'(\tau) = \rho'(L, 1/N),$$

où $L = \mathbb{Z} + \mathbb{Z}\tau$. Il est connu (voir [L], [He], [Scho]) que $G_N(\tau)$, $\rho_N(\tau)$ et $\rho_N'(\tau)$ sont des formes modulaires par rapport au groupe $\Gamma_1(N)$, de poids 1,2,3 respectivement. De plus, g_2 est aussi une forme modulaire de poids 4 par rapport au groupe $\Gamma_1(N)$ puisque elle l'est pour le groupe $\mathrm{SL}_2(\mathbb{Z})$. Donc la fonction

$$\widetilde{\pi}(\tau) = G_N^4(\tau) - 6\rho_N(\tau)G_N^2(\tau) + 4\rho_N'(\tau)G_N(\tau) + g_2(\tau) - 3\rho_N^2(\tau)$$

est une forme modulaire de poids 4 par rapport au groupe $\Gamma_1(N)$. De plus, le théorème 6 implique que $\widehat{Z}(\widetilde{\pi}(\tau))$ coïncide avec $Y(N)$. D'autre part, comme on l'a vu au cours de la démonstration du théorème 6

$$\widetilde{\pi}(\tau) = 8G(L, v)G\big(L, v + \tfrac{1}{2}\big)G\big(L, v + \tfrac{1}{2}\tau\big)G\big(L, v + \tfrac{1}{2} + \tfrac{1}{2}\tau\big),$$

où $L = \mathbb{Z} + \mathbb{Z}\tau$ et $v = \frac{1}{2}N$. Maintenant les formules (voir [TM])

$$\zeta(\tau, u) - \frac{\eta_1 u}{\omega_1} = \frac{1}{\omega_1}\frac{\theta_1'(\tau, \nu)}{\theta_1(\tau, \nu)}, \quad \zeta\Big(\tau, u + \frac{\omega_i}{2}\Big) - \frac{\eta_i}{2} - \frac{\eta_1 u}{\omega_1} = \frac{1}{\omega_1}\frac{\theta_i'(\tau, \nu)}{\theta_i(\tau, \nu)},$$

où

$$\tau = \frac{\omega_2}{\omega_1}, \quad \nu = \frac{u}{\omega_1}, \quad i = 2, 3, 4,$$

impliquent que $\widetilde{\pi}(\tau) = 8\pi(\tau)$. □

Remarque. — Soient $\lambda = Y_{a,b,c}$ un arbre et β une fonction de Belyi qui représente λ. On considère la fonction de Belyi $\widehat{\beta} = \beta \circ \pi$ sur la courbe elliptique associée à λ (voir le fin du paragraphe 2.1). Le dessin torique $\widehat{Y}_{a',b',c'}$ qui correspond à $\widehat{\beta}$ consiste en trois boucles se croisant en un point (voir fig. 7) et les nombres des arêtes sur ces boucles sont égaux à $a' = 2a$, $b' = 2b$, et $c' = 2c$. Les dessins toriques consistant en de

telles boucles (sans contraintes sur la parité du nombres des arêtes sur ces boucles) ont été étudiés dans l'article de L. Zapponi [Zap] où en utilisant des méthodes différentes des résultats similaires (non équivalents) aux nôtres ont été obtenus.

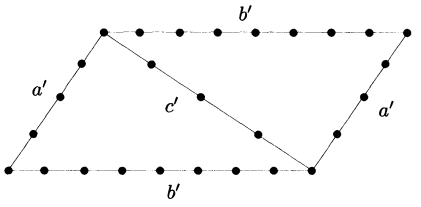

Figure 7

3. ARBRES DE GENRE ABÉLIEN ARBITRAIRE

3.1. Critère d'existence d'un morphisme.

Soient λ, μ deux arbres et $P(z)$, $R(z)$ les polynômes de Shabat correspondants. On dira que l'arbre λ admet un *morphisme* sur l'arbre μ s'il existe un polynôme $Q(z)$ tel que $P(z) = R(Q(z))$. Il est clair que la propriété d'admettre un morphisme sur un arbre à d-arêtes est invariante par l'action de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ sur Λ. Le cas particulier important où $Q(z)$ est aussi un polynôme de Shabat et l'opération de *composition* des arbres reliée à ce cas ont été étudiés dans [ShZv], [AdZv]. Ici on va aborder le cas général. On note que l'ordre abélien d'un arbre à n arêtes est égal à n/d où d est le nombre maximal tel que λ admet un morphisme sur un graphe linéaire à d-arêtes.

On rappelle qu'un groupe de permutations G agissant sur l'ensemble E s'appelle *imprimitif* s'il existe des sous-ensembles disjoints $E_i \subset E$, $1 \leq i \leq \ell$, tels que $E = \bigcup_{i=1}^{\ell} E_i$ et que le groupe G permute les ensembles E_i, $1 \leq i \leq \ell$. D'après le résultat classique de Ritt (voir [R]), un polynôme complexe $P(z)$ peut être mis sous la forme d'une composition $P(z) = R(Q(z))$ où $R(z), Q(z)$ sont des polynômes complexes de degrés supérieurs à 1 si et seulement si le groupe de monodromie de $P(z)$ est imprimitif. D'autre part si $P(z)$ est un polynôme de Shabat alors son groupe de monodromie peut être visualisé facilement. À savoir, en suivant [AKSS], on définit pour un arbre bicolore à n arêtes λ, son *groupe de rotations des arêtes* Γ_λ comme un groupe de permutations agissant sur l'ensemble des arêtes de λ et engendré par deux permutations a, b, où a (resp. b)

transforme chaque arête incidente à un sommet blanc (resp. noir) en l'arête suivante par la rotation directe autour de ce sommet. Il est clair que pour un arbre λ, le groupe Γ_λ coïncide avec le groupe de monodromie du polynôme de Shabat $P(z)$ correspondant.

En utilisant le théorème de monodromie, il est facile de vérifier que le groupe Γ engendré par une paire de permutations a, b, est le groupe des rotations des arêtes pour un arbre λ si et seulement si ab est un cycle de longueur n, et $c(a) + c(b) = n + 1$, où $c(u)$ est le nombre de cycles de permutation u. De plus, deux tels groupes $\Gamma = \langle a, b\rangle$ et $\Gamma' = \langle a', b'\rangle$ correspondent au même arbre à n arêtes, si et seulement s'il existe $u \in \mathrm{S}_n$ tel que $a' = ua, b' = ub$. On remarque que l'isomorphisme entre Γ_λ et Γ'_λ comme groupes abstraits n'implique pas en général que $\lambda = \lambda'$.

THÉORÈME 8. — *Soient λ un arbre à n arêtes, $\Gamma_\lambda = \langle a, b\rangle$ son groupe de rotations des arêtes et d un diviseur de n. Les conditions suivantes sont équivalentes :*

1) *L'arbre λ admet un morphisme sur un arbre à d arêtes μ.*

2) *Les orbites du groupe $\Gamma^+_{\lambda,d} \subset \Gamma_\lambda$ engendré par l'élément $(ab)^d$ forment un système d'imprimitivité pour le groupe Γ_λ.*

3) *Les orbites du groupe $\Gamma^+_{\lambda,d}$ coïncident avec ceux du groupe $\Gamma^-_{\lambda,d} \subset \Gamma_\lambda$ engendré par l'élément $(ba)^d$.*

Supposons que ces conditions soient satisfaites. Alors μ est un graphe linéaire si et seulement si chaque orbite du groupe $\Gamma^+_{\lambda,d}$ reste invariante par l'action des éléments a^2, b^2.

Démonstration. — Si l'arbre λ admet un morphisme sur un arbre μ à d-arêtes alors, d'après le théorème de Ritt, le groupe Γ_λ admet un système d'imprimitivité $A = \{A_1^+, A_2^+, \ldots, A_d^+\}$, où chaque A_i, $1 \leq i \leq d$, est l'image réciproque d'une arête de l'arbre μ. L'action du groupe Γ_λ sur l'ensemble des blocs A induit un homomorphisme ψ du groupe Γ_λ sur le groupe Γ_μ qui transforme les générateurs de Γ_λ en ceux de Γ_μ. Comme l'arbre μ est à d-arêtes, l'élément $(ab)^d$ se trouve dans le noyau de cet homomorphisme; d'où il suit que chaque orbite du groupe $\Gamma^+_{\lambda,d}$ est à l'intérieur d'un bloc de A. Puisque $(ab)^d$ est un cycle de longueur n/d et le cardinal de chaque bloc est aussi égal à n/d, on conclut que l'ensemble des orbites de $\Gamma^+_{\lambda,d}$ coïncide avec l'ensemble des blocs de A. Par contre, si les ensembles A_i^+, $1 \leq i \leq d$, forment un système d'imprimitivité pour le groupe Γ_λ, alors le théorème de Ritt implique que l'arbre λ admet un

morphisme sur un arbre à d-arêtes μ. En effet, l'égalité $P(z) = R(Q(z))$ pour un polynôme de Shabat $P(z)$ implique que $R(z)$ est aussi un polynôme de Shabat.

Pour prouver l'équivalence des conditions 2) et 3), on remarque que les ensembles $b\{A_i^+\}$, $1 \leq i \leq d$, sont des orbites du groupe $b\Gamma_{\lambda,d}^+ b^{-1} = \Gamma_{\lambda,d}^-$. Donc si les orbites A_i^+ forment un système d'imprimitivité alors les orbites de $\Gamma_{\lambda,d}^+$ coïncident avec ceux de $\Gamma_{\lambda,d}^-$. Par contre la condition que les orbites A_i^+, $1 \leq i \leq d$, du groupe $\Gamma_{\lambda,d}^+$ coïncident avec les orbites A_i^-, $1 \leq i \leq d$, du groupe $\Gamma_{\lambda,d}^-$ implique que b permute les ensembles A_i^+. De plus a permute aussi les ensembles A_i^+, $1 \leq i \leq d$, puisque $A_i^+ = A_k^-$ pour un certain k, $1 \leq k \leq d$, et $a\{A_k^-\}$ est une orbite du groupe $a\Gamma_{\lambda,d}^- a^{-1} = \Gamma_{\lambda,d}^+$. Donc chaque élément du groupe Γ_λ permute les ensembles A_i^+ et, par conséquent, les ensembles A_i^+, $1 \leq i \leq d$, forment un système d'imprimitivité pour le groupe Γ_λ.

Pour finir la démonstration du théorème, on remarque que si chaque orbite du groupe $\Gamma_{\lambda,d}^+$ reste invariante par l'action des éléments a^2, b^2 alors Γ_μ est un groupe engendré par deux éléments a', b' pour lesquels $a'^2 = b'^2 = 1$. Donc la valence maximale des sommets d'arbre μ est égale à 2; ce qui implique que μ est un graphe linéaire. Par contre si μ est un graphe linéaire alors $a'^2 = b'^2 = 1$ et donc a^2, b^2 se trouvent dans le noyau de l'homomorphisme ψ; d'où il suit que chaque orbite de groupe $\Gamma_{\lambda,d}^+$ reste invariante par l'action des éléments a^2, b^2. □

Exemple. — On considère les deux arbres représentés sur la figure 8 qui sont tous les deux du type $(3,3,3,3,2,1,1;\ 4,2,2,2,1,1,1,1,1,1)$ et dont les groupes de rotations des arêtes sont $\Gamma_{\lambda_1} = \langle a_1, b_1\rangle$, $\Gamma_{\lambda_2} = \langle a_2, b_2\rangle$. Des arêtes de l'arbre λ_1 (resp. λ_2) qui sont dans la même orbite du groupe engendré par l'élément $(a_1 b_1)^4$ (resp. $(a_2 b_2)^4$) sont marquées sur la figure par le même signe. Il est facile de voir que ces orbites forment un système d'imprimitivité pour le groupe Γ_{λ_1} et ne forment pas de tel système pour le groupe Γ_{λ_2}. Donc, d'après le théorème 8, λ_1 admet un morphisme sur un arbre λ à 4 arêtes et λ_2 n'en admet pas; ce qui implique, en particulier que λ_1 et λ_2 ne peuvent pas se trouver dans la même orbite par l'action du groupe $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. On remarque que le groupe Γ_λ est engendré par les éléments $a = (123)(4)$ et $b = (1)(3)(24)$ ce qui entraîne que $\lambda = Y_{1,1,2}$.

3.2. Exemples de torsion sur $\mathbb{Q}$.

Le problème général de la description des arbres dont le corps de modules est $\mathbb{Q}$ paraît être compliqué. Pour le cas où le genre abélien est

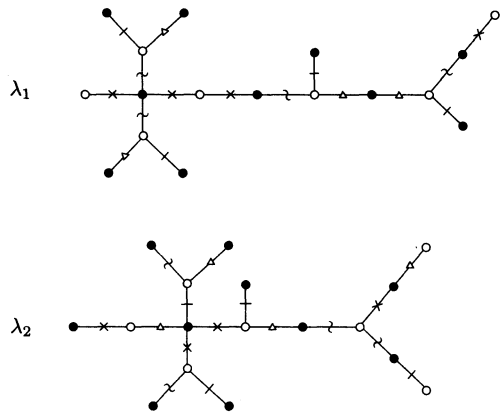

Figure 8

égal à 1, on a obtenu dans 2.2.2 quelques informations sur de tels arbres en utilisant le résultat de B. Mazur [Maz]. Cependant, pour les genres supérieurs à 1, des résultats analogues au résultat de B. Mazur n'existent pas. D'autre part, l'absence de tels résultats rend intéressants tous les exemples de diviseurs rationnels de torsion sur des courbes définies sur $\mathbb{Q}$ (ou plus généralement sur des corps de nombres). En particulier, la vitesse de croissance de cet ordre par rapport au genre est intéressante. Dans les articles [Fl1], [Fl2], [Le1], [Le2] (voir aussi [HL]) ont été construites des séries d'exemples de croissance linéaire et quadratique.

Dans ce paragraphe, en utilisant la technique développée ici, on construit des séries d'exemples de croissance linéaire dans le cadre de la théorie des « dessins d'enfants ».

On considère l'arbre $\mu_{k,t}$ du type $\langle 2k-1, 1, 1, \ldots, 1;\ t, 2, 2, \ldots, 2\rangle$, $t, k \in \mathbb{N}$, à $t+4k-4$ arêtes (voir fig. 9). En utilisant la formule du nombre de classes isotopiques des arbres de type donné (voir [ShZv]), on conclut qu'il n'existe qu'un *seul* arbre de ce type [7], d'où il suit que le corps de modules de $\mu_{k,t}$ est $\mathbb{Q}$. Si t est un nombre impair alors l'ordre abélien de $\mu_{k,t}$ est égal à $t+4k-4$. En effet, $\mu_{k,t}$ contient deux sommets adjoints de valence impaire et donc il ne peut pas être image réciproque d'un graphe linéaire à $d > 1$ arêtes. Si pour g fixé et $1 \leq k \leq g+1$ on pose $t = 2g - 2k + 3$,

[7] La liste complète des arbres dont l'orbite combinatoire contient un seul arbre et des polynômes de Shabat correspondants a été obtenue par N. Adrianov (voir [AdSh], [ShZv]).

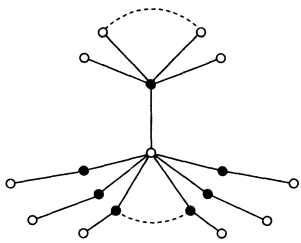

Figure 9

alors le genre abélien de $\mu_{k,t}$ est égal à g et l'ordre abélien de $\mu_{k,t}$ est égal à $t+4k-4=2g+2k-1$, et on obtient le résultat suivant :

THÉORÈME 9. — *Pour chaque genre g et chaque N impair tel que $2g+1 \leq N \leq 4g+1$, il existe une courbe hyperelliptique définie sur $\mathbb{Q}$ avec un diviseur rationnel d'ordre N.*

On prouve que si t est un nombre pair alors l'ordre abélien de $\mu_{k,t}$ est égal à $\frac{1}{2}(t+4k-4)$. En effet, si $t=2$ alors le polynôme de Shabat qui correspond à $\mu_{k,t}$ est égal (à changement de variable linéaire près) à $T_2(z^{2k-1})$. Comme $2k-1$ est un nombre impair, ceci implique que l'ordre abélien de $\mu_{k,t}$ est égal à $\frac{1}{2}(t+4k-4)$. On remarque maintenant que si $t>2$ est un nombre pair et si $\mu_{k,t}$ admet un morphisme sur un graphe linéaire à d arêtes, alors $d=2$. En effet, on considère le sommet de valence t et deux arêtes différentes x_1, x_2 adjacentes vers ce sommet, telles que $b^2(x_1)=x_2$. D'après le théorème 7, x_1 et x_2 sont dans la même orbite du groupe engendré par l'élément $(ab)^d$, ce qui est évidemment possible seulement si $d=2$. D'autre part, il est facile de vérifier que si t est un nombre pair alors les orbites du groupe $\widetilde{\Gamma}$ engendré par l'élément $(ab)^2$ forment un système d'imprimitivité pour le groupe $\Gamma_{\mu_{k,t}}$ et chaque orbite de groupe $\widetilde{\Gamma}$ reste invariante par l'action des éléments a^2, b^2, ce qui d'après le théorème 7 implique que l'ordre abélien de $\mu_{k,t}$ est égal à $\frac{1}{2}(t+4k-4)$. On fixe maintenant $g \in \mathbb{N}$. Si on pose pour $1 \leq k \leq g+1$, $t=2g-2k+4$ alors le genre abélien de $\mu_{k,t}$ est égal à g et l'ordre abélien de $\mu_{k,t}$ est égal à $\frac{1}{2}(t+4k-4)=g+k$. On a ainsi obtenu le résultat suivant :

THÉORÈME 10. — *Pour chaque genre g et chaque entier N, avec $g+1 \leq N \leq 2g+1$, il existe une courbe hyperelliptique définie sur $\mathbb{Q}$ avec un diviseur rationnel d'ordre N.*

BIBLIOGRAPHIE

[Ab] N.H. ABEL, Uber die Integration der Differential-Formel $\rho\,\mathrm{d}x/\sqrt{R}$ wenn ρ und R ganze Functionen sind, J. Reine Angew. Math., 1 (1826), 185–221.

[Ak] N.I. AKHIEZER, Elements of the Theory of Elliptic Functions, AMS Translations of mathematical monographs, 79 (1990).

[AdSh] N.M. ADRIANOV, G.B. SHABAT, Planar dessins with one face and polynomials with two critical values, Preprint, 1990 (en russe).

[AKSS] N.M. ADRIANOV, Yu.Yu. KOCHETKOV, A.D. SUVOROV and G.B. SHABAT, Mathieu groupes and plane trees, Fundamentalnaiya i prikladnaya matematika, 1 (1995), 377–384 (en russe).

[AdZv] N. ADRIANOV, A. ZVONKIN, Composition of plane trees, soumis à Acta Applicandae Mathematicae.

[AR] W. W. Adams, M.J. RAZAR, Multiples of points on elliptic curves and continued fractions, Proc. London Math. Soc., 41 (1980), 481–498.

[Be] G.V. BELYI, On Galois extension of a maximal cylotomic field, Math. USSR Izvestija, 14, 2 (1980), 247–256.

[Ber] T.G. BERRY, On periodicity of continued fractions in hyperelliptic function fields, Arch. Math., 55 (1990), 259–266.

[BPZ] J. BÉTRÉMA, D. PÉRÉ, A. ZVONKIN, Plane trees and their Shabat polynomials (Catalog), Rapport interne de LaBRI, n° 92–75, Bordeaux, 1992.

[Ch] P. CHEBYSHEV, Sur l'intégration de la différentielle $(x+A)/\sqrt{x^4+\alpha x^3+\beta x^2+\gamma}\,\mathrm{d}x$, Bull. Acad. Impériale de Saint–Pétersbourg, 3 (1861), 1–12. (Réédité dans Journal des Math. Pures et Appl., 2, 9 (1864), 225–246).

[Couv] J.–M. COUVEIGNES, Calcul et rationalité des fonctions de Belyi en genre 0, Ann. Inst. Fourier, 44–1 (1994), 1–38.

[Gr] A. GROTHENDIECK, Esquisse d'un programme, non publié, 1984.

[Fl1] E.F. FLYNN, Sequences of rational torsion on abelian varieties, Inventiones Math., 106 (1991), 433–442.

[Fl2] E.F. FLYNN, The arithmetic of hyperelliptic curves, in Algorithms in Algebraic Geometry and applications, Birkhauser, Progress in Mathematics, 143 (1996), 165–175.

[GH] P. GRIFFITHS, J. HARRIS, Principles of Algebraic Geometry, New York, John Wiley and Sons, 1978.

[Hal] G.H. HALPHEN, Traité des fonctions elliptiques et leurs applications, Paris, 1886–1891.

[HL] Y. HELLEGOUARCH, M. LOZACH, Équation de Pell et points d'ordre fini, in Analitic and Elementary Number Theory, Marseille, Publ. Math. Orsay, 86–1, 1983.

[HBJ] F. HIRZEBRUCH, T. BERGER, R. JUNG, Manifolds and modular forms, Bonn, Vieweg, 1992.

[Jun] R. JUNG, Zolotarev-Polynome und die Modulkurve $X_1(N)$, Diplomarbeit, Bonn, 1989.

[La] S. LANG, Introduction to modular forms, Springer-Verlag, 1976.

[Le1] F. LEPRÉVOST, Famille de courbes hyperelliptique de genre g munies d'une classe de diviseurs rationnels d'ordre $2g^2+4g+1$, in Séminaire de théorie des

nombres, Paris, France, 1991–1992, Birkhauser, Progress in Mathematics, 116 (1994), 107–119.

[Le2] F. LEPRÉVOST, Torsion sur des familles de courbes de genre g, Manuscripta Math., 75 (1992), 303–326.

[Mag] N. MAGOT, Communication personnelle.

[Maz] B. MAZUR, Rational points of modular curves, in Modular Functions of One Variable V, Lecture Notes in Math., Springer, 601 (1977), 107–148.

[Mer] L. MEREL, Bornes pour la torsion des courbes elliptiques sur les corps de nombres, Invent. Math., 124 (1996), 437–449.

[MM] H. P. McKean, P. van MOERBEKE, Hill and Toda Curves, Communication on Pure and Applied Mathematics, XXXIII (1980), 23–42.

[P1] F.B. PAKOVITCH, Les polynômes elliptiques, Uspechi Mat. Nauk, 58, 8 (1995), 312–314 (en russe).

[Pay] R. PAYSANT–LE ROUX, Périodicité des fractions continues dans un corps de fonctions hyperelliptiques, Arch. Math., 61 (1993), 45–58.

[R] J.F. RITT, Prime and composite polynomials, Trans. Amer. Math. Soc., 23 (1922), 51–66.

[Schn] L. SCHNEPS, Dessins d'Enfants on the Riemann Sphere, in The Grothendieck Theory of Dessins d'Enfants, L. Shneps eds., Cambridge University Press London Mathematical Society Lecture Notes series, 200 (1994), 47–77.

[ShZv] G. SHABAT, A. ZVONKIN, Plane trees and algebraic numbers, in Jerusalem Combinatorics 93, H. Barcelo, G. Kalai eds., AMS Contemporary Mathematics series, 178 (1994), 233–275.

[ShVo] G. SHABAT, V. VOEVODSKII, Drawing curves over number fields, in The Grothendieck FestShrift, Birkhäuser, 3 (1990), 199–227.

[Shin] A. SHINZEL, On some problems in the arithmetical theory of continued fraction II, Acta Arith., 7 (1962), 287–298.

[TaMo] J. TANNERY, J. MOLK, Eléments de la théorie des fonctions elliptiques, 3, Paris, 1898.

[Zap] L. ZAPPONI, Dessins d'enfants en genre 1, à paraître.

[Zol] G. ZOLOTAREFF, Sur la méthode d'intégration de M. Tchebicheff, J. Math. Pures et Appl., 2, 19 (1874), 161–188.

Manuscrit reçu le 11 avril 1997,
accepté le 4 novembre 1997.

Fedor PAKOVITCH,
Weizmann Institute of Sciences
Department of Mathematics
Rehovot (Israël).
pakovitc@wisdom.weizmann.ac.il