Arbres planaires et points d'ordre fini sur les jacobiennes des courbes hyperelliptiques.

Fedor Pakovitch

Introduction

Soient $P(z) \in \mathbb{C}$[z] un polynôme de degré n et $I \subset \mathbb{C}$ un segment. L'ensemble $P^{-1}(I)$, image réciproque de I par l'application $P(z) : \mathbb{C} \to \mathbb{C}$, est habituellement homéomorphe à une union de n segments disjoints. Cependant, cette image réciproque peut être homéomorphe à un *seul* segment, comme on le voit avec l'exemple du polynôme de Chebyshev $T_n(z) = \cos(n \arccos z)$ et du segment $[-1, 1]$. On note Σ l'ensemble de *toutes* les paires (P, I) composées d'un polynôme $P(z)$ et d'un segment I. Les propriétés topologiques de l'ensemble $P^{-1}(I)$ peuvent être prises comme base d'une stratification de Σ. Par abus de langage on pourra dire que la paire se trouve dans g-ième strate Σ_g de cette stratification si le nombre minimal des segments qui est nécessaire pour "composer" l'ensemble $P^{-1}(I)$ est égal à $g + 1$.

Dans la première partie de cet article on donne la définition précise de la stratification ci-dessus et on étudie ses propriétés. On construit une correspondance bijective entre les classes d'équivalence affine des paires $(P, I) \in \Sigma_g$, $(g \geq 1)$ pour lesquelles $\deg P(z) = n$, et les classes d'isomorphisme des paires se composant d'une courbe hyperelliptique de genre g et d'un point de n-division sur cette courbe. On montre, de plus, que chaque paire $(P, I) \in \Sigma_0$ est équivalente à la paire composée d'un polynôme de Chebyshev et du segment $[-1, 1]$, ce qui donne une caractérisation topologique curieuse des polynômes de Chebyshev.

Dans la deuxième partie on réunit ces résultats et un cas particulier de la théorie des "dessins d'enfants". On définit l'application qui associe à chaque arbre planaire 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. Dans le cas où $g = 1$, cette construction est un pont entre la théorie de la torsion des courbes elliptiques et celle des "dessins d'enfants". Ce cas est étudié en détail dans cet article. En particulier, à partir de la structure *combinatoire* d'un arbre n-arêtes, on calcule l'ordre *exact* du point de n-division associé. Ceci permet, en utilisant les résultats correspondants

sur la torsion des courbes elliptiques, d'obtenir des estimations effectives *inférieures* sur les degrés des corps des modules des arbres de certaines classes. D'autre part, la construction ci-dessus donne une suite interessante d'exemples de points d'ordre aussi grand que l'on veut sur des courbes elliptiques definies sur des corps de nombres dont les coordonnées sont incluses dans le corps de définition.

Une partie des résultats de cet article a été anoncée dans [P].

1. Soient $P(z)$ un polynôme complexe et $I = [a, b]$ le segment qui joint les points distincts $a, b \in \mathbb{C}$. Désignons par $u_1, u_2, ..., u_k$ toutes les valeurs critiques du polynôme $P(z)$ qui sont à l'intérieur de I, et posons $u_0 = a$, $u_{k+1} = b$. 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, $i = 0, ..., k+1$, et d'arêtes les images réciproques des intervalles ouverts $]u_i, u_{i+1}[$, $i = 0, ..., k$. 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 $P(x) \in \{u_1, ..., u_k\}$. 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 zéro à l'intérieur des domaines que les circuits bordent, ce qui est impossible.

Exemple. Pour la paire $\tau = (T_n, I_1)$ composée du n-ième polynôme de Chebyshev $T_n(z) = \cos(n \arccos z)$ et du segment[1] $I_1 = [-1, 1]$, le graphe G_τ est un graphe *linéaire* n-arêtes ayant comme sommets les points de l'axe réel de coordonnée $\cos \frac{\pi i}{n}$, $i = 0, ..., n$ (voir fig. 1).

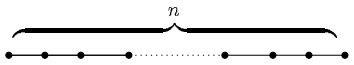

fig. 1

On note Σ l'ensemble des toutes paires (P, I) composées d'un polynôme $P(z)$ et d'un segment $I = [a, b]$, $a \neq b$.

Définition 1. On dira que $\sigma \in \Sigma$ est dans la g-ième *strate d'Abel*, si le graphe G_σ est une union de $g+1$ sous-graphes linéaires sans arêtes communes, mais n'est pas une union de g tels sous-graphes.

Désignons par Σ_g le sous-ensemble de Σ se composant des paires $\sigma = (P, I)$ qui sont dans g-ième strate d'Abel et par $\Sigma_{g,n}$ le sous-ensemble de Σ_g se composant des paires pour lesquelles deg $P(z) = n$.

[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 $[-1, 1]$.

Proposition 1. *Pour une paire $\sigma = (P, I)$, où $I = [a, b]$ les conditions suivantes sont équivalentes:*

1) $\sigma \in \Sigma_{g,n}$.

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

3) $P(z)$ satisfait l'équation d'Abel

$$(P(z) - a)(P(z) - b) = \left(\frac{P'(z)}{nq_\sigma(z)}\right)^2 R_\sigma(z), \tag{1}$$

où $q_\sigma(z), R_\sigma(z)$ sont des polynômes unitaires, $\deg R_\sigma(z) = 2g + 2, \deg q_\sigma(z) = g$, *et $R_\sigma(z)$ n'a que des racines simples.*

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. Cette dernière affirmation se démontre par récurrence sur g. Dans le cas où $g = 0$ elle est évidente. Supposons maintenant que notre affirmation soit prouvée pour $g < n$. Soit G un graphe ayant $2n + 2$ sommets de valence impaire qui est réunion de $k + 1$ sous-graphes linéaires sans arêtes communes, mais n'est pas réunion de k tels sous-graphes. Soit G_1 un sous-graphe linéaire de G qui contient deux sommets de valence 1 du graphe G (il est clair qu'un tel graphe existe toujours). Considérons le graphe $\bar{G}$ obtenu de G par suppression des sommets de valence 1 ou 2 ainsi que de toutes les arêtes du graphe G_1 (voir fig. 2).

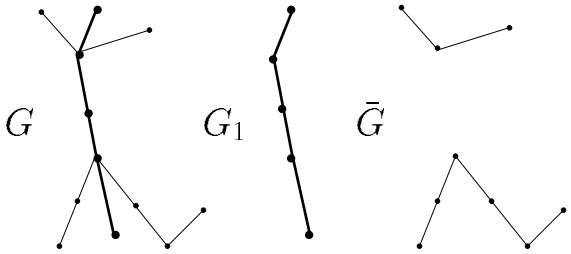

fig. 2

Le passage de G à $\bar{G}$ ne change pas la parité de la multiplicité des sommets restants. Par conséquent, $\bar{G}$ a justement $2n$ sommets de valence impaire. En utilisant l'hypothèse de récurrence, on conclut que $k \leq n$. Admettons que k soit strictement inférieur à n. Soit $G = \cup_{i=1}^{k} G_i$, où G_i sont des sous-graphes linéaires de G. On suppose sans restreindre la généralité qu'au moins une des deux extrémités du graphe linéaire G_1 consideré comme un sommet du graphe G est de valence 1. Désignons cette extrémité

par x et l'autre par y. Définissons $\bar{G}$ comme avant. Le nombre des sommets de valence impaire du graphe $\bar{G}$, est égal soit à $2n$, soit à $2n+2$, selon la parité de la multiplicité de l'extrémité y de G_1. Dans le premier cas, on obtient une contradiction avec l'hypothèse de récurrence, puisque le graphe $\bar{G}$ est réunion de moins de n sous-graphes linéaires. Dans le deuxième cas répétons notre construction pour le graphe $\bar{G}$ qui est déjà réunion de k sous-graphes linéaires sans arêtes communes. Il est clair qu'à un certain moment nous obtiendrons un graphe ayant $2n$ sommets de valence impaire, qui est réunion de moins de n sous-graphes linéaires, ce qui contredit l'hypothèse de récurrence. Donc $k = n$, ce qui prouve l'équivalence $1 \Leftrightarrow 2$.

$2 \Rightarrow 3$. Désignons par $R_\sigma(z)$ un polynôme qui a comme racines tous les points de l'ensemble $P^{-1}\{a, b\}$ pour les valeurs desquels $P(z)$ 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

$$(1') \qquad (P(z)-a)(P(z)-b) = Q^2(z)R_\sigma(z).$$

En dérivant (1'), on obtient

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

Puisque chaque diviseur $Q(z)$ est soit diviseur de $P(z)-a$, soit diviseur de $P(z)-b$, $Q(z)$ est premier avec $2P(z)-(a+b) = (P(z)-a)+(P(z)-b)$. Donc, l'équation (2) implique que $Q(z)|P'(z)$. En désignant $P'(z)/(nQ(z))$ par $q_\sigma(z)$, on retrouve l'équation (1).

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

Définition 2. Les paires $\sigma = (P, I), \bar{\sigma} = (\bar{P}, \bar{I}) \in \Sigma$ seront dites équivalentes s'il existe des fonctions linéaires γ_1, γ_2 telles que $P(z) = \gamma_1(\bar{P}(\gamma_2(z))$ et $I = \gamma_1(\bar{I})$.

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

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 $(\tilde{P}, I_1)$ telle que les coordonnées de valence 1 du graphe $G_{\tilde{P},I_1}$ sont ± 1. En utilisant la proposition, on conclut que $\tilde{P}(z)$ satisfait l'équation

$$(3) \qquad \tilde{P}^2(z) - \frac{\tilde{P}'^2(z)}{n^2}(z-1)(z+1) = 1.$$

Considérons la courbe algèbrique $L:\ w^2 + z^2 = 1$ et sa clôture projective $\bar{L} = \mathbb{P}^1$. En réécrivant l'équation (3) comme

$$(4) \qquad \left(\tilde{P}(z) + i\frac{\tilde{P}'(z)}{n}w\right)\left(\tilde{P}(z) - i\frac{\tilde{P}'(z)}{n}w\right) = 1,$$

on voit que la fonction $\psi(z,w) = \tilde{P}(z) + i\frac{\tilde{P}'(z)}{n}w$ n'a ni zéros ni pôles 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. En plus, comme on le vérifie aisément, l'ordre du zéro aussi bien que l'ordre du pôle est égal à $n = \deg \tilde{P}(z)$. Puisque pour les fonctions $(z \pm iw)^n$ ces conditions sont aussi satisfaites, il existe $c \in \mathbb{C}$ tel que $\psi(z,w) = c(z \pm iw)^n$. En utilisant l'égalité (4), 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 $\tilde{P}(z) = \pm \mathrm{Re}(z \pm iw)^n$ dans l'anneau $\mathbb{C}$[z, w], ce qui implique l'égalité $\tilde{P}(z) = \pm T_n(z)$. □

On rappelle qu'une courbe hyperelliptique est une surface de Riemann compacte H qui est une normalisation d'une courbe affine définie par l'équation $w^2 = R(z)$, 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 fonction fractionnaire-linéaire γ 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 $\rho \to \rho' = (z,-w)$ l'involution canonique. Le point ρ est dit de n-division, si ρ n'est pas un point de branchement de H et le diviseur $n(\rho - \rho')$ est principal. On note $\tilde{\mathrm{H}}_{g,n}$, l'ensemble des classes d'isomorphisme des paires (H, ρ) se composant d'une courbe hyperelliptique H de genre g avec 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 $\chi : \tilde{\Sigma}_{g,n} \to \tilde{\mathrm{H}}_{g,n}$. Pour cela on choisit dans la classe $\tilde{\sigma} \in \tilde{\Sigma}_{g,n}$ 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), et du point ρ_∞ sur H_σ se trouvant au-dessus de l'infini. On associe maintenant à la classe $\tilde{\sigma}$, 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 $\bar{\sigma}$, alors $R_{\bar{\sigma}}(z) = R_\sigma(\gamma(z))$, où $\gamma(z)$ est une fonction linéaire, ce qui implique l'isomorphisme $(\mathrm{H}_\sigma, \rho_\infty) \cong (\mathrm{H}_{\bar{\sigma}}, \rho_\infty)$. Pour s'assurer que le point ρ_∞ sur la courbe H_σ est effectivement de n-division, on considère la fonction

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

En utilisant l'équation (1′), on a:

$$d\Psi_\sigma = dP + wdQ + Qdw = dP + wdQ + Q\frac{dR_\sigma}{2w} = \frac{1}{2w}(2wdP + 2R_\sigma dQ + QdR_\sigma) =$$

$$= \frac{1}{2wQ}(2wQdP + d(Q^2R_\sigma)) = \frac{1}{2wQ}(2wQdP + 2PdP - (a+b)dP) = \frac{dP}{Q}\frac{1}{w}\Psi_\sigma.$$

Il s'ensuit que

$$\frac{d\Psi_\sigma}{\Psi_\sigma} = n q_\sigma \frac{dz}{w}. \tag{5}$$

Puisque $\mathrm{div}_\infty\ q_\sigma(z) = g(\rho_\infty + \rho'_\infty)$, $\mathrm{div}_0\ \frac{dz}{w} = (g-1)(\rho_\infty + \rho'_\infty)$, et $\frac{dz}{w}$ n'a pas des pôles sur H_σ, on conclut que la forme $\frac{d\Psi_\sigma}{\Psi_\sigma}$ n'a que deux pôles simples aux points qui se trouvent au-dessus de l'infini avec les résidus $\pm n$, ce qui implique que le point ρ_∞ est de n-division. Enfin, il est clair que le genre de H_σ est égal à g.

Théorème 2. *L'application $\chi : \tilde{\Sigma}_{g,n} \to \tilde{\mathrm{H}}_{g,n}$ est bijective. De plus, pour la paire $\sigma = (P, I_1)$ l'ordre exact du diviseur $\rho_\infty - \rho'_\infty$ dans le groupe $\mathrm{Pic}\,\mathrm{H}_\sigma$ est égal au minimum des degrés des polynômes $\bar{P}(z)$ tels que $P(z) = \pm T_d(\bar{P}(z))$.*

Démonstration. On prouve d'abord l'injectivité de χ. Pour cela notons que si pour les paires $\bar{\sigma} = (\bar{P}, I_1), \sigma = (P, I_1)$ on a $R_{\bar{\sigma}}(z) = R_\sigma(z)$ et $\deg \bar{P}(z) = \deg P(z)$, alors $\bar{P}(z) = \pm P(z)$, puisque pour les fonctions correspondantes $\Psi_{\bar{\sigma}}(z,w)$ et $\Psi_\sigma(z,w)$ on a l'égalité $\Psi_{\bar{\sigma}}(z,w) = \pm\Psi_\sigma(z, \pm w)$. Cette dernière égalité se démontre de la même façon que dans la démonstration du théorème 1. Supposons maintenant que pour les paires $\bar{\sigma} = (\bar{P}, \bar{I})$, $\sigma = (P, I) \in \Sigma_{g,n}$ on a $(\mathrm{H}_{\bar{\sigma}}, \rho_\infty) \cong (\mathrm{H}_\sigma, \rho_\infty)$. Il est clair que sans restreindre la généralité on peut supposer que $\bar{I} = I = I_1$. L'isomorphisme $\mathrm{H}_{\bar{\sigma}} \cong \mathrm{H}_\sigma$ implique qu'il existe une fonction fractionnaire-linéaire γ telle que les polynômes $R_{\bar{\sigma}}(z)$ et $R_\sigma(\gamma(z))$ ont les mêmes racines. En outre, puisque les points des courbes $\mathrm{H}_{\bar{\sigma}}, \mathrm{H}_\sigma$ 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 $\bar{\sigma} = (\bar{P}, I_1)$ et $\sigma_\gamma = (P(\gamma), I_1)$ on a $R_{\bar{\sigma}}(z) = R_{\sigma_\gamma}(z)$. Ceci implique l'égalité $\bar{P}(z) = \pm P(\gamma(z))$ 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 $\Psi(z,w) = P(z) + Q(z)w$, où $P(z), Q(z) \in \mathbb{C}(z)$, la fonction sur H pour laquelle $\mathrm{div}\,\Psi(z,w) = n(\rho - \rho')$. 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 $2P(z) = \Psi(z,w) + \Psi(z,-w)$ sur H se trouvent au-dessus de ∞, $P(z)$ doit être un pôlynome. L'équation $P^2(z) - Q^2(z)R(z) = 1$ implique à présent que $Q(z)$ est aussi un pôlynome, car $R(z)$ n'a que des racines simples. Puisque pour la paire $\sigma = (P, I_1)$ on a évidement $(\mathrm{H}_\sigma, \rho_\infty) = (\mathrm{H}, \rho)$, l'application χ est surjective.

Pour finir la démonstration du théorème, supposons que pour la paire $\sigma = (P, I_1)$ le minimum des degrés des polynômes $\bar{P}(z)$ pour lesquels $P(z) = \pm T_d(\bar{P}(z))$ est égal à k. Comme il est facile à vérifier, l'égalité $P(z) = \pm T_{n/k}(\bar{P}(z))$ implique l'égalité $R_{\bar{\sigma}} = R_\sigma$, où $\bar{\sigma} = (\bar{P}, I_1)$. Ainsi, l'ordre l du point ρ sur la courbe H divise k. Admettons que l soit strictement inférieur à k. Soit $\hat{\psi}(z,w) = \hat{P}(z) + \hat{Q}(z)w$ une fonction sur H telle que $\mathrm{div}\ \hat{\psi}(z,w) = l(\rho - \rho')$ et $\hat{\psi}(z,w)\hat{\psi}(z,-w) = 1$. Pour les

paires $\hat{\sigma} = (T_{n/l}(\hat{P}), I_1), \sigma = (P, I_1)$ on a $R_{\hat{\sigma}}(z) = R_\sigma(z)$ et $\deg T_{n/l}(\hat{P}) = \deg P(z)$. Donc $P(z) = \pm T_{n/l}(\hat{P}(z))$ avec $\deg \hat{P}(z) < k$, ce qui contredit l'hypothèse préalable. □

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

$$(z, y) = \left(\frac{1}{2}\left(\frac{B+w}{A-v}\right), 2v + A - \frac{1}{4}\left(\frac{B+w}{A-v}\right)^2\right) \tag{6}$$

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

$$y^2 = R(z) = z^4 - 6Az^2 + 4Bz + C$$

et la courbe elliptique L définie par l'équation

$$w^2 = 4v^3 - g_2 v - g_3,$$

où

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

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 L, 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 L.

Dans le cas où $n = 2$ le théorème 2 admet une interprétation géométrique facile. A savoir, le théorème 1 implique que chaque paire (P, I) avec $\deg P(z) = 2$ qui n'est pas équivalente à (T_2, I_1) se trouve dans la première strate d'Abel. 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 $\tilde{\mathrm{H}}_{1,2}$ et l'ensemble des orbites de l'action du groupe engendré par la transformation $\lambda \to 1 - \lambda$ sur $\mathbb{C} \setminus \{0, 1\}$. D'autre part, l'ensemble des orbites de l'action du groupe Γ qui consiste en les substitutions λ, $\frac{1}{\lambda}$, $1 - \lambda$, $\frac{1}{1-\lambda}$, $\frac{\lambda}{\lambda-1}$, $\frac{\lambda-1}{\lambda}$ 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 $\lambda \to 1 - \lambda$ est d'indice 3, ce qui s'explique par le fait que chaque courbe elliptique a justement trois points d'ordre 2.

Remarque. L'équation (1′) 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 (1′) avec R_σ fixé, a une solution polynômiale P, Q, si et seulement si la fraction continue de $\sqrt{R_\sigma}$ est périodique. D'autre part, la question sur la solubilité de l'équation (1′) pour $\deg R_\sigma = 4$ est équivalente à la question suivante: *le point* (A, B) *sur la courbe elliptique* L *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 solubilité de l'équation (1′) a été déjà donné en 1864 par Chebyshev [Ch] (voir aussi [Zol]). Le lien entre les équations (1), (1′) pour $\deg R_\sigma = 4$ et les points d'ordre fini sur des courbes elliptiques a aussi été étudié dans [Hal], [Shin], [AR], [Jun], [HBJ]. En particulier, dans [Jun], [HBJ], un résultat, au fond équivalent au théorème 2 a été obtenu.[2] On remarque, en outre, que l'équation (1′) avec $R_\sigma(z) \in \mathbb{R}[z]$ (ou bien les courbes hyperelliptiques réelles ayant des points de n-division) apparaît aussi dans la théorie d'approximation [SoYu] et dans la théorie des systèmes intégrables [MM].

2. Dans [Gr] A. Grotendieck a établi la 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], [ShZv]. *Une fonction propre de Belyi* sur une courbe C est une application rationnelle $\beta : \mathrm{C} \to \mathbb{CP}^1$ 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. *Une paire propre de Belyi* est une paire (C, β) composée d'une courbe et d'une fonction propre de Belyi sur cette courbe. L'image réciproque 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 seul 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 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 dans le cas particulier de la correspondance entre les dessins et les paires de Belyi où la surface de Riemann est une sphère[4] et les dessins sont des arbres. Dans ce cas, la correspondance ci-dessus admet une simplification décrite par G. Shabat. A savoir, au lieu des fonctions de Belyi, il est plus commode de considérer des polynômes qui n'ont que deux valeurs critiques[5] (finies).

[2] L'auteur remercie A. P. Veselov qui lui a signalé cela.

[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 deux paires de Belyi $(\mathbb{CP}^1, \beta_1)$ et $(\mathbb{CP}^1, \beta_2)$ sont isomorphes si et seulement si il existe une fonction fractionnaire-linéaire γ telle que $\beta_1(z) = \beta_2(\gamma(z))$.

[5] Sans contraintes sur les indices de ramification aux points au-dessus de ces valeurs critiques.

De tels polynômes sont dits *polynômes de Shabat*. Dans toute la suite on identifiera 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 notera $S\Sigma, S\Sigma_{\mathrm{g}}, S\Sigma_{\mathrm{g,n}}$ (resp. $S\tilde{\Sigma}, S\tilde{\Sigma}_{\mathrm{g}}, S\tilde{\Sigma}_{\mathrm{g,n}}$) les sous-ensembles correspondants dans $\Sigma, \Sigma_g, \Sigma_{g,n}$ (resp. dans $\tilde{\Sigma}, \tilde{\Sigma}_g, \tilde{\Sigma}_{g,n}$). 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, et 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 (ayant ± 1 pour valeurs critiques). Désignons 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 n-arêtes dont le nombre de sommets de valence impaire[6] 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 $\alpha : \Lambda_{g,n} \to S\tilde{\Sigma}_{\mathrm{g,n}}$ 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). L'exemple le plus simple de polynôme de Shabat est le polynôme de Chebyshev $T_n(z)$. L'arbre correspondant est représenté sur la figure 1.[7]

La rationalité de $0, 1, \infty$ implique que dans la classe d'équivalence des fonctions de Belyi il existe des fonctions à coefficients algèbriques. Donc on peut définir l'action du groupe $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ sur l'ensemble Λ. A savoir, pour $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ et $\lambda \in \Lambda$, on choisit dans la classe correspondante des fonctions de Belyi, une fonction β à coefficients algèbriques et on définit $\sigma(\lambda)$ comme l'arbre qui correspond à la classe d'équivalence des fonctions de Belyi contenant la fonction $\sigma(\beta)$. Il est facile de vérifier que la définition ci-dessus ne dépend pas du choix de la fonction β. Puisque des raisons combinatoires simples impliquent que pour chaque arbre λ son orbite est finie, le stabilisateur $\mathrm{St}(\lambda)$ est d'indice fini dans $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. 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.

On définit maintenant l'application $\varphi : \Lambda_{g,n} \to \tilde{\mathrm{H}}_{g,n}$ en posant pour $\lambda \in \Lambda_{g,n}$, $\varphi(\lambda) = \chi(\alpha(\lambda))$. D'après [Couv], pour chaque arbre λ dans la classe des fonctions de Belyi correspondante, il existe une polynôme β dont les coefficients sont contenus dans k_λ. Donc *dans la classe $\varphi(\lambda)$ il existe une courbe dont les coefficients sont contenus*

[6] On remarque que ce nombre est toujours pair.

[7] D'après l'existence de la bijection α, ce fait peut être utilisé pour une autre démonstration du théorème 1.

dans k_λ. En effet, si les coefficients du polynôme $\beta(z) = 1 - P^2(z)$ sont éléments du corps k_λ, alors les coefficients du polynôme qui a comme racines (simples) toutes les racines de multiplicité impaire de β, sont aussi contenus dans k_λ.

Définition 3. On définit pour un arbre λ ses *genre* et *ordre* respectivement comme le genre de la courbe H et l'ordre du diviseur $\rho - \rho'$ dans le groupe Pic H pour un représentant $(H, \rho) \in \phi(\lambda)$.

Rappellons que d'après le théorème 2, l'ordre de λ est égal au minimum des degrés des polynômes $\bar{P}(z)$ tels que $P(z) = \pm T_l(\bar{P}(z))$, où $\sigma = (P, I_1)$ est un représentant de $\alpha(\lambda)$. Puisque les coefficients de $T_n(z)$ sont rationnels, on conclut que *l'ordre est invariant par l'action de* $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ sur Λ.

Le problème qui apparaît alors naturellement est le suivant: *à partir de la structure combinatoire de l'arbre* λ *définir son ordre.* On va résoudre ce problème dans le cas où le genre de λ est égal à 1. Ce cas est spécialement intéressant. En effet, d'après les formules (6), à partir d'un arbre d'ordre n de genre 1 ayant comme corps des modules k_λ, 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 [Mer], pour tout corps de nombres k, il existe une borne effective 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. Ceci implique immédiatement le résultat suivant: *pour chaque* $t \in \mathbb{N}$ *il existe* $l = l(t) \in \mathbb{N}$, *tel que pour chaque arbre* λ *de genre* 1 *l'inégalité* $\mathrm{ord}\,\lambda > l$ *implique que le degré de* k_λ *sur* $\mathbb{Q}$ *est strictement supérieur à* t. En particulier, d'après [Maz] on a: *si l'ordre d'un arbre de genre 1 est strictement supérieur à* 12, *alors le corps* $\mathbb{Q}$ *ne peut pas être son corps de définition.*

On remarque que pour chaque paire $\sigma = (P, I_1)$, le fait $\sigma \in \mathrm{S}\Sigma$, implique que la paire $\sigma_k = (T_k(P), I_1)$ est aussi dans $\mathrm{S}\Sigma$, et si à σ correspond l'arbre λ, alors à σ_k 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 (voir fig. 3).[8]

fig. 3

Cependant, l'inclusion $\sigma_k \in \mathrm{S}\Sigma$, pour $\sigma_k = (T_k(P), I_1)$ n'implique pas $\sigma = (P, I_1) \in \mathrm{S}\Sigma$ mais implique seulement que l'ensemble des valeurs critiques de $P(z)$ est inclus

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

dans l'ensemble $\cos\frac{\pi l}{k},\ l=0,...,k$.

On considère maintenant les arbres de genre 1. Un tel arbre est de l'une des deux espèces suivantes:

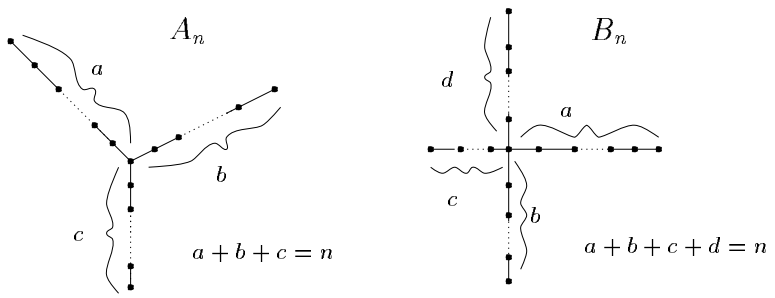

fig. 4

Chaque arbre d'espèce $\mathrm{A_n}$ (resp. $\mathrm{B_n}$) est défini par le triplet $<a,b,c>$ (resp. quadruplet $<a,b,c,d>$.) Posons $\mathrm{A}=\bigcup_{\mathrm{n=1}}^{\infty}\mathrm{A_n}$, $\mathrm{B}=\bigcup_{\mathrm{n=1}}^{\infty}\mathrm{B_n}$.

Théorème 3. *Soit λ un arbre n-arêtes de genre un. Alors l'ordre de λ est égal à $n/(a,b,c)$ si $\lambda\in A_n$ et à $n/(a+b,b+c,c+d,d+a)$ si $\lambda\in B_n$.*

Démonstration. Pour s'assurer de la véracité du théorème dans le cas où $\lambda\in A_n$, on prouve tout d'abord le critère simple suivant: la classe $\tilde{\sigma}$ de $\tilde{\Sigma}_1$ appartient à $\alpha(\mathrm{A})$ si et seulement si pour un représentant $\sigma=(P,I)$ de $\tilde{\sigma}$ on a $q_\sigma|R_\sigma$. En effet, dans ce cas l'équation 1 implique que le polynôme $P(z)$ n'a que deux valeurs critiques donc $\tilde{\sigma}=\alpha(\lambda)$ pour un arbre λ. De plus, comme il est facile de vérifier, l'arbre λ a quatre sommets de valence impaire, un desquels est de valence trois d'où il suit que $\lambda\in\mathrm{A}$. On prouve maintenant que l'égalité $P(z)=\pm T_l(\bar{P}(z))$ pour la paire $\sigma=(P,I_1)$ qui représente l'arbre $\lambda\in A_n$, implique que la paire $\bar{\sigma}=(\bar{P},I_1)$ appartient aussi à $\mathrm{S}\Sigma$ et représente un arbre $\bar{\lambda}\in A_{n/l}$. Pour cela on remarque que l'égalité ci-dessus implique que $\Psi_\sigma(z,w)=\pm(\Psi_{\bar{\sigma}}(z,\pm w))^l$. D'après la formule (5) on obtient l'égalité $q_\sigma=q_{\bar{\sigma}}$. Notre affirmation découle à présent du critère prouvé.

Soit $\lambda\in A_n$, $\lambda=<a,b,c>$ et $(a,b,c)=k$. Soient l'arbre $\tilde{\lambda}=<a/k,b/k,c/k>$ et un représentant $\tilde{\sigma}=(\tilde{P},I_1)$ de $\alpha(\tilde{\lambda})$. Puisque la paire $\tilde{\sigma}_k=(T_k(\tilde{P}),I_1)$ est un représentant de la classe $\alpha(\lambda)$, on a $\operatorname{ord}\lambda|(n/k)$.

Par contre, l'égalité $P(z)=\pm T_l(\bar{P}(z))$ pour la paire $\sigma=(P,I_1)$ qui représente l'arbre $\lambda\in A_n$, comme on a prouvé, implique que $\bar{\sigma}=(\bar{P}(z),I_1)$ est un représentant de $\alpha(\bar{\lambda})$ où $\bar{\lambda}\in\mathrm{A_{n/l}}$. Si $\bar{\lambda}=<\bar{a},\bar{b},\bar{c}>$, alors $\lambda=<l\bar{a},l\bar{b},l\bar{c}>$, d'où $l|k$, et, par conséquent, $\operatorname{ord}\lambda=n/k$, ce qui prouve le théorème dans le cas où $\lambda\in A_n$.

Soit maintenant $\lambda\in\mathrm{B_n}$, $\lambda=<a,b,c,d>$. Si $(a,b,c,d)=l>1$ alors, en utilisant les mêmes raisonnements que plus haut, on conclut qu'il existe un représentant $(\tilde{P},I_1)$ de la classe $\alpha(\tilde{\lambda})$, où $\tilde{\lambda}=<a/l,b/l,c/l,d/l>\in\mathrm{B_{n/l}}$, tel que la paire $(T_l(\tilde{P}),I_1)$

représente l'arbre λ. Donc, en tenant compte de l'égalité $T_{uv}(z) = T_u(T_v(z))$,[9] il suffit de prouver le théorème en supposant que $(a, b, c, d) = 1$.

Supposons que $P(z) = \pm T_m(\bar{P}(z))$. Puisque la condition $(a, b, c, d) = 1$ implique que $\bar{\sigma} = (\bar{P}(z), I_1) \notin \mathrm{S}\Sigma$, le polynôme $P(z)$ a un point critique x tel que $\bar{P}(x) \neq \pm 1$. Par ailleurs, comme $\deg q_{\bar{\sigma}} = 1$, l'équation (1) implique que le polynôme $\bar{P}(z)$ ne peut pas avoir plus d'un tel point et que la multiplicité du polynôme $\bar{P}(z)$ en ce point est égale à deux. De plus, $P(x) \in L$, où $L = \{\cos \frac{\pi i}{m}, i = 0, ..., m\}$. Enfin, il est clair qu'en les points critiques du pôlynome $\bar{P}(z)$ en lesquels sa valeur est égale à ± 1, sa multiplicité est aussi égale à deux.

L'égalité $P(z) = \pm T_m(\bar{P}(z))$ signifie géométriquement que l'arbre λ se réalise comme l'image réciproque du graphe lineaire 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 les axes (voir fig. 5).

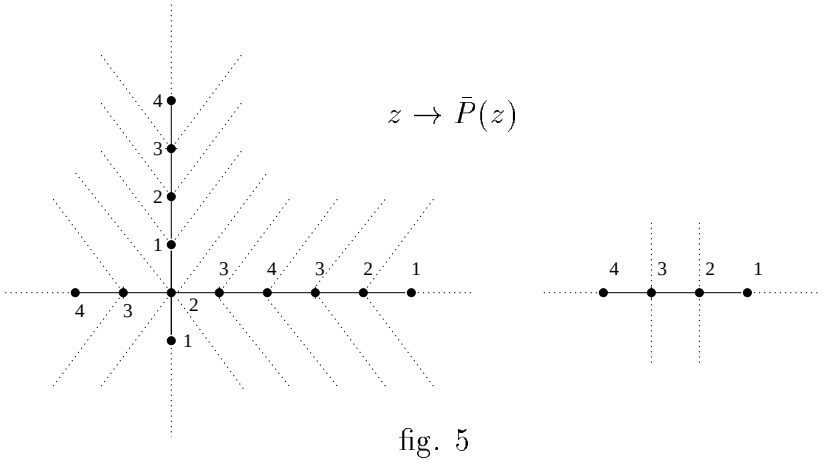

fig. 5

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 en longueur de l'axe réel dans direction la $-\infty$. 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 $\bar{P}(z)$. 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 $\bar{P}(z)$ en y est égale à deux. En continuant d'avancer de la même manière, à un certain moment on arrive au point

[9] Ce fait bien connu découle facilement, par exemple, du théorème 1.

zéro. On commence alors à avancer le long de l'axe imaginaire dans la direction $-i\infty$. Puisque zéro est un point critique de $\bar{P}(z)$ d'ordre 2 et $\bar{P}(0) \neq \pm 1$, 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. A un moment, on arrive au sommet de λ de coordonnée minimale sur l'axe imagine. Puisque le numéro de ce point est égal soit à 1 soit à $m+1$ notre construction implique que $m|(a+b)$ (en notation de fig. 4). Les faits que $m|(b+c)$, $m|(c+d)$, $m|(d+a)$ 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 la paire $(T_m(\bar{P}), I_1)$. 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 deux triangulations de la sphère de Riemann en joignant chaque sommet de λ et de G_τ de valence i, $(1 \leq i \leq 4)$ 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* $\bar{P} : \mathbb{P}^1 \to \mathbb{P}^1$ telle que les triangles à gauche des sommets de numéros j et $j+1$, $(1 \leq j \leq m)$ ont pour images les triangles à droite des sommets de mêmes numéros en préservant les numéros des sommets de telle façon que la restriction de l'application $\bar{P} : \mathbb{P}^1 \setminus \bar{\mathrm{P}}^{-1}(\mathrm{L}) \to \mathbb{P}^1 \setminus \mathrm{L}$ soit un revêtement à t feuillets. En effet, si $t = 2$, alors $a = c$, $b = d$, et on peut poser $\bar{P}(z) = z^2$. Supposons que notre affirmation soit prouvée pour $t < k$ et considèrons le cas $t = k$. Puisque $k > 2$ parmi les nombres a, b, c, d il en existe au moins un qui est strictement supérieur à m (on rappelle que $(a, b, c, d) = 1$). On suppose que ce nombre est a. On considère l'arbre $\tilde{\lambda} \in \lambda$, $\tilde{\lambda} =< a - m, b, c, d >$. D'après l'hypothèse de récurrence pour l'arbre $\tilde{\lambda}$ il existe une application ayant les propriétés nécessaires et on voit clairement comment la modifier pour obtenir l'application cherchée pour l'arbre λ. Maintenant, d 'après les théorèmes généraux de la théorie des fonctions de la variable complexe, il existe une structure complexe telle que $\bar{P}$ est holomorphe. Puisque $\bar{P}^{-1}\{\infty\} = \{\infty\}$, $\bar{P}$ dans cette structure est un pôlynome. Il est clair que le polynôme $T_m(\bar{P}(z))$ représente l'arbre λ (cf. [ShZv]). □

Exemple. En utilisant le catalogue [BPZ], il est facile de vérifier que les arbres qui sont représentés sur la figure 6 (ayant comme corps de modules $\mathbb{Q}$),

fig. 6

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.

Comme les arbres de genre 1 offrent une curieuse suite d'exemples de torsion sur les courbes elliptiques définies sur les corps de nombres, il est interessant d'estimer pour ces arbres les degrés de leur corps de définition, ou, ce qui est équivalent, les longueurs de leur orbite par l'action du groupe $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. On se borne ici au cas des arbres d'espèce $\mathrm{A_p}$, où p est un nombre premier. Le cas général peut être analyser de manière analogue. Pour trouver les estimation nécessaires on note que pour chaque arbre planaire λ représenté par une paire $(P,I)\in \mathrm{S}\Sigma$ peut être fournie 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 $\alpha=\alpha_1,\alpha_2,...,\alpha_p$ (resp. $\beta=\beta_1,\beta_2,...,\beta_q$) 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 $(\alpha;\beta)$. Il est clair que si deux arbres bicolores qui sont de types $(\alpha;\beta)$ et $(\bar\alpha;\bar\beta)$ respectivement, se trouvent dans la même orbite par l'action du groupe $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, alors soit $\alpha=\bar\alpha,\beta=\bar\beta$, soit $\alpha=\bar\beta,\beta=\bar\alpha$. En comptant que le sommet de valence trois est blanc, on obtient que chaque arbre $\lambda\in A$ est d'un de quatre types suivants:

$$(3,\overbrace{2,2,...2}^{k};\overbrace{2,2,...,2}^{k},1,1,1),\qquad (3,\overbrace{2,2,...2}^{k},1;\overbrace{2,2,...,2}^{k+1},1,1),$$

$$(3,\overbrace{2,2,...2}^{k},1,1;\overbrace{2,2,...,2}^{k+2},1),\qquad (3,\overbrace{2,2,...2}^{k},1,1,1;\overbrace{2,2,...,2}^{k+3}).$$

Puisque le nombre d'arêtes dans chacun de ces types est égal à $2k+3$, $2k+4$, $2k+5$, $2k+6$ respectivement, les deuxième et quatrième types ne se réalisent pas car le nombre p est premier. Maintenant, en utilisant la formule pour le nombre de classes isotopiques des arbres de type donné (voir. [ShZv]), on conclut qu'il y a $(p^2-1)/24$ classes isotopiques d'arbres de premier type et $(p-3)(p-1)/8$ de troisième. On remarque que ceci implique le résultat suivant: *pour chaque nombre premier $p\geq 5$ il existe une courbe elliptique E definie sur un corps de nombres K telle que $E(K)$ possède un point d'ordre p et que le degré du corps K sur $\mathbb{Q}$ est inférieur ou égal $(p^2-1)/24$.*

Remerciements: L'auteur remercie G. Shabat, M. Zaidenberg et A. Zvonkin pour de nombreuses discussions.

Bibliographie

[Ab] **N. H. Abel,** Uber die Integration der Differential-Formel $\frac{\rho dx}{\sqrt{R}}$ wenn ρ und R ganze Functionen sind, *J. Reine Angew. Math.*, **1,** 1826, 185-221.

[AR] **W. W. Adams, M. J. Razar,** Multiples of points on elliptic curves and continued fractions, *Proc. London Math. Soc.*, **41**, 1980, 481-498.

[AdZv] **N. Adrianov, A. Zvonkin,** Composition of plane trees, Soumis à *Acta Applicandae Mathematicae.*

[BPZ] **J. Bétréma, D. Péré, A. Zvonkin,** Plane trees and their Shabat polynomials (Catalog), Rapport interne de LaBRI, no. 92-75, Bordeaux, 1992.

[Ch] **P. Chebyshev,** Sur l'intégration de la différentielle $\frac{x+A}{\sqrt{x^4+\alpha x^3+\beta x^2+\gamma}}dx$, *Journal des math. pures et appl.*, **2**, 9, 1864, 225-246.

[Couv] **J.-M. Couveignes,** Calcul et rationalité de fonctions de Belyi en genre 0, *Ann. Inst. Fouriere,* vol. **44**, no 1, 1994, 1-38.

[Gr] **A. Grothendieck**, Esquisse d'un programme, non publié.

[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.

[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.

[Maz] **B. Mazur**, Rational points of modular curves, dans: "Modular Functions of One Variable V", (Lect. Notes Math. Vol. **601**), Springer, 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*, vol. **XXXIII**, 1980, 23-42.

[P] **F. B. Pakovitch,** Les polynômes elliptiques, Uspechi Mat. Nauk, vol. **58,** no. 8, 1995, 312-314 (en russe).

[Schn] **L. Schneps**, Dessins d'enfants on the Riemann sphere, dans "The Grothendieck Theory of Dessins D'enfants" (L. Shneps eds.), Cambridge University Press ("London mathematical society lecture notes series", vol. **200**), 1994, 47-77.

[ShZv] **G. Shabat, A. Zvonkin,** Plane trees and algebraic numbers, dans "Jerusalem Combinatorics 93" (H. Barcelo, G. Kalai eds.), AMS ("Contemporary Mathematics" series, vol. **178**), 1994, 233-275.

[Shin] **A. Shinzel**, On some problems in the arithmetical theory of continued fraction II, *Acta Arith.*, **7**, 1962, 287-298.

[SoYu] **M. L. Sodin, P. M. Yuditskii,** Functions deviating least from zero on closed subset of the real axis, *St. Petesburg Math. J.,* vol. **4**, 1993, no. 2, 241-249.

[Zol] **G. Zolotareff,** Sur la méthode d'intégration de M. Tchebicheff, *Journal des math. pures et appl.*, **2**, 19, 1874, 161-188.

Fedor Pakovitch, Université Grenoble I, Institut Fourier et Laboratoire de Mathématiques associé au CNRS, BP 74, 38402 St. Martin d'Hères–cédex, France. e-mail: FEDOR.PAKOVITCH@PUCCINI.UJF–GRENOBLE.FR