Journal de Théorie des Nombres
de Bordeaux **8** *(1996), 93–99*

À propos du théorème de Belyi

par Jean-Marc COUVEIGNES

Résumé – Le théorème de Belyi affirme que sur toute courbe algébrique $\mathcal{C}$ lisse projective et géométriquement connexe, définie sur $\bar{\mathbb{Q}}$, il existe une fonction f non ramifiée en dehors de $\{0, 1, \infty\}$. Nous montrons que cette fonction peut être choisie sans automorphismes, c'est-à-dire telle que pour tout automorphisme non trivial $\mathfrak{a}$ de $\mathcal{C}$, on ait $f \circ \mathfrak{a} \neq f$. Nous en déduisons que si $\mathbb{K} \subset \mathbb{C}$ est une extension finie de $\mathbb{Q}$, toute $\mathbb{K}$-classe d'isomorphisme de courbes algébriques lisses projectives géométriquement connexes peut être caractérisée par un *dessin d'enfant* de Grothendieck, c'est à dire par une classe d'isomorphisme topologique de revêtements de la sphère privée de trois points. Nous en donnons quelques exemples.

Abstract – A famous theorem of Belyi asserts that on any smooth projective geometrically connected algebraic curve $\mathcal{C}$ defined over $\bar{\mathbb{Q}}$ there exists a function f unramified outside $\{0, 1, \infty\}$. We show that this function can be choosen without non trivial automorphism. As a consequence, for $\mathbb{K} \in \mathbb{C}$ a finite extension of $\mathbb{Q}$, any $\mathbb{K}$-isomorphism class of smooth projective geometrically connected algebraic curves can be characterized by a *dessin d'enfant de Grothendieck*, i.e. an isomorphism class of finite connected topological coverings of the sphere minus three points. We give a few examples of this situation.

1. Introduction et définitions

Dans tout cet article le mot courbe désignera une courbe lisse projective et géométriquement connexe. On appelle *fonction de Belyi* une fonction algébrique f d'une courbe $\mathcal{C}$ définie sur $\mathbb{C}$, à valeurs dans $\mathbb{P}^1$, non ramifiée en dehors de $\{0, 1, \infty\}$. La paire $(\mathcal{C}, f)$ est appelée *paire de Belyi.*

Deux paires de Belyi $(\mathcal{C}_i, f_i)$ pour $i \in \{1, 2\}$ sont dites isomorphes s'il existe un isomorphisme $i : \mathcal{C}_1 \to \mathcal{C}_2$ tel que $f_1 = f_2 \circ i$. Une classe d'isomorphisme de paires de Belyi est appelée un *dessin d'enfant* selon la terminologie de Grothendieck dans [GR].

1991 *Mathematics Subject Classification.* 11R32-11Y40.
Mots-clés : Corps globaux, revêtements.
Manuscrit reçu le 11 juillet 1995

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

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

Nous appelons groupe d'automorphismes $\mathrm{Aut}(\mathcal{D})$ d'un dessin $\mathcal{D}$ le groupe des automorphismes d'une paire de Belyi de ce dessin.

Si une paire de Belyi est définie sur un corps de nombres $\mathbb{K} \subset \mathbb{C}$ on dit que $\mathbb{K}$ est *un corps de définition* du dessin $\mathcal{D}$ associé. Tout corps de définition de $\mathcal{D}$ contient le corps des modules $\Gamma_{\mathcal{D}}$.

Si $\mathrm{Aut}(\mathcal{D})$ est trivial, alors le corps des modules est un corps de définition. Plus précisément, il existe une unique $\mathbb{K}_{\mathcal{D}}$-classe d'équivalence de paires de Belyi associées à $\mathcal{D}$. C'est la descente de Weil, [WE]. Plus généralement, on définit le *dessin réduit* $\mathcal{D}_0$ d'un dessin $\mathcal{D}$ comme le quotient de $\mathcal{D}$ par $\mathrm{Aut}(\mathcal{D})$ et on montre ([C1]) que le corps des modules de $\mathcal{D}$ est un corps de définition de son dessin réduit et qu'il existe une $\mathbb{K}_{\mathcal{D}}$-classe d'équivalence canonique de paires de Belyi associée à $\mathcal{D}_0$ vu comme dessin réduit de $\mathcal{D}$.

On peut ainsi associer à tout dessin $\mathcal{D}$ une $\mathbb{K}_{\mathcal{D}}$-classe d'isomorphisme de courbes lisses projectives, que l'on note $\mathcal{C}(\mathcal{D})$. En particulier, si $\mathcal{D}$ est sans automorphismes, c'est simplement la classe associée à un modèle défini sur $\mathbb{K}_{\mathcal{D}}$ du dessin $\mathcal{D}$.

Réciproquement, étant donné une extension finie $\mathbb{K}$ de $\mathbb{Q}$, on se demande si toute $\mathbb{K}$-classe d'isomorphisme de courbes est obtenue ainsi (rappelons que dans tout cet article on entend par courbe une courbe algébrique lisse projective et géométriquement connexe). On sait bien que toute courbe définie sur $\mathbb{K}$ admet une fonction de Belyi, c'est le théorème de Belyi, mais il reste à voir si cette fonction peut être choisie sans automorphismes.

C'est ce qu'on se propose de démontrer ici. Nous remercions J. Oesterlé d'avoir attiré notre attention sur ce problème.

Théorème. *Pour toute courbe lisse projective définie sur une extension finie $\mathbb{K}$ de $\mathbb{Q}$ dans $\mathbb{C}$, il existe une fonction de Belyi* **sans automorphismes** *de $\mathcal{C}$ dans $\mathbb{P}_1$, définie sur $\mathbb{K}$.*

2. Preuve du théorème

Dans toute cette section $\mathbb{K}$ est une extension finie de $\mathbb{Q}$ dans $\mathbb{C}$. Nous procéderons en trois lemmes.

LEMME 1 (BELYI). *Soit $\mathcal{C}$ une courbe définie sur $\mathbb{K}$ et ϕ une fonction de $\mathcal{C}$ dans $\mathbb{P}_1$ définie sur $\mathbb{K}$, alors il existe un* **polynôme** *$P(x)$ à coefficients dans $\mathbb{Q}$ tel que les valeurs singulières de $P \circ \phi$ soient dans $\{0, 1, \infty\}$.*

Preuve: On compose successivement à gauche par des polynômes annulateurs des valeurs singulières irrationnelles ainsi que dans la preuve de Belyi. On obtient alors une fonction ϕ_0 dont toutes les valeurs singulières sont rationnelles. Soient S et s la plus grande et la plus petite des valeurs singulières finies de ϕ_0. Si $s = S$ on compose ϕ_0 par le polynôme $x \mapsto x - s$ et c'est fini. Sinon on compose ϕ_0 par le polynôme

$$x \mapsto \frac{x - s}{S - s}.$$

On obtient alors une fonction dont toutes les valeurs singulières finies sont entre 0 et 1. S'il n'y a pas d'autre valeur singulière que $\{0, 1, \infty\}$ alors c'est fini. Sinon soit $0 < \alpha < 1$ l'une d'elles. On peut écrire

$$\alpha = \frac{m}{m + n}$$

avec $m, n \in \mathbb{Z}_{>0}$. On compose alors par le polynôme

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

On vérifie que $A_{m,n}(\alpha) = 1$ et que les valeurs singulières de $A_{m,n}$ sont dans $\{0, 1, \infty\}$. De plus, et c'est le seul point nouveau par rapport à Belyi, on remarque que

$$A_{m,n}([0, 1]) = [0, 1].$$

Ainsi, en composant par $A_{m,n}$ on diminue le nombre de valeurs singulières hors de $\{0, 1, \infty\}$ et les valeurs singulières finies de la fonction obtenue sont toujours dans $[0, 1]$.

On arrive à une fonction de Belyi en itérant ce processus.

Conséquence: La fonction de Belyi $\psi = P \circ \phi$ obtenue a les mêmes pôles que ϕ. Plus précisément, pour toute fonction f sur $\mathcal{C}$ notons $(f)_0$ la partie positive du diviseur de f et $(f)_\infty$ sa partie négative si bien que $(f) = (f)_0 - (f)_\infty$. Alors si p est le degré du polynôme P, on a

$$p.(\phi)_\infty = (\psi)_\infty\,.$$

Soit alors $\bar{\mathcal{C}}$ la courbe obtenue à partir de $\mathcal{C}$ par extension des scalaires de $\mathbb{K}$ à $\bar{\mathbb{Q}}$ et notons $\mathrm{Aut}(\bar{\mathcal{C}})$ son groupe d'automorphismes. Tout diviseur D de $\mathcal{C}$ peut se voir comme diviseur de $\bar{\mathcal{C}}$. On appelle alors groupe des automorphismes de D l'ensemble des automorphismes de $\bar{\mathcal{C}}$ qui stabilisent D. De même pour toute fonction f sur $\mathcal{C}$, un automorphisme de f est un élément $\mathfrak{a}$ de $\mathrm{Aut}(\bar{\mathcal{C}})$ tel que $f = f \circ \mathfrak{a}$. On note $\mathrm{Aut}(D)$ et $\mathrm{Aut}(f)$ les ensembles ainsi définis. On a

$$\mathrm{Aut}(f) \subset \mathrm{Aut}((f)_0) \subset \mathrm{Aut}(\bar{\mathcal{C}}).$$

Dans la situation qui nous intéresse, supposons que le diviseur $(\phi)_\infty$ n'a pas d'automorphismes. Alors $(\psi)_\infty = p.(\phi)_\infty$ n'en a pas non plus et donc ψ n'a pas d'automorphismes.

On en déduit le

Lemme 2. *Soit $\mathcal{C}$ une courbe définie sur $\mathbb{K}$. Supposons qu'il existe sur $\mathcal{C}$ un diviseur positif D sans automorphismes et défini sur $\mathbb{K}$, alors il existe une fonction de Belyi définie sur $\mathbb{K}$ et sans automorphismes, de $\mathcal{C}$ dans $\mathbb{P}_1$.*

Preuve: Soit g le genre de $\mathcal{C}$. D'après le théorème de Riemann-Roch on sait que pour tout diviseur E sur $\mathcal{C}$ de degré $\deg(E)$ supérieur à $2g-2$, la dimension $\ell(E)$ de l'espace linéaire associé $\mathcal{L}(E)$ est $\deg(E)+1-g$. On en déduit que si $\deg(E)$ est supérieur à $2g-1$ il existe une fonction f dans $\mathcal{L}(E)$ dont le diviseur des pôles $(f)_\infty$ est exactement la partie positive de E. Soit maintenant un entier m tel que $\deg(mD) > 2g-1$. Il existe une fonction f telle que $(f)_\infty = mD$ n'a pas d'automorphismes. On obtient alors une fonction de Belyi sans automorphismes en appliquant la construction du lemme 1 à la fonction f.

Lemme 3. *Soit $\mathcal{C}$ une courbe définie sur $\mathbb{K}$. Il existe sur $\mathcal{C}$ un diviseur positif défini sur $\mathbb{K}$ et sans automorphisme non trivial.*

Preuve: Nous montrons d'abord qu'il existe un diviseur positif défini sur $\mathbb{K}$ dont le groupe d'automorphismes est fini. Ensuite nous décrivons un procédé pour faire diminuer ce groupe d'automorphismes jusqu'à le rendre trivial.

Soit g le genre de la courbe. Si $g = 0$, tout ensemble contenant au moins trois points distincts a un groupe d'automorphismes fini. En effet, tout automorphisme stabilisant n points induit une permutation de ces n points. Mais la connaissance de l'image de n points distincts avec $n \geq 3$ suffit à déterminer une homographie. Il y a donc au plus $n!$ automorphismes. Si $g = 1$ on choisit un point O sur $\bar{\mathcal{C}}$ ce qui fait de $\bar{\mathcal{C}}$ une courbe elliptique, et on note que tout automorphisme de $\bar{\mathcal{C}}$ s'écrit

$$P \mapsto [\epsilon]P \oplus C,$$

où $\oplus$ désigne la loi d'addition sur la courbe elliptique, C est un point de $\bar{\mathcal{C}}$ et $[\epsilon]$ est un automorphisme de la courbe elliptique $(\bar{\mathcal{C}}, O)$. Un point fixe vérifie alors l'équation $([\epsilon] \ominus \mathrm{Id})P = -C$ et comme le degré de l'endomorphisme $[\epsilon] \ominus \mathrm{Id}$ est borné par quatre on en déduit qu'un automorphisme d'une courbe de genre 1 a au plus quatre points fixes (cf [SI, page 103] pour tout ceci). Ainsi, tout automorphisme fixant 5 points est trivial et donc un ensemble de n points distincts avec $n \geq 5$ a au plus $n!$ automorphismes. Si $g > 1$, la courbe elle même n'a qu'un nombre fini d'automorphismes. N'importe quel ensemble défini sur $\mathbb{Q}$ et non vide fera l'affaire. Nous obtenons dans tous les cas un diviseur positif de groupe d'automorphismes $\mathrm{Aut}(D)$ fini.

Soit maintenant une courbe $\mathcal{C}$ définie sur $\mathbb{K}$ et un diviseur positif D défini sur $\mathbb{K}$ dont le groupe d'automorphismes $\mathrm{Aut}(D)$ est fini et non trivial. Nous allons montrer qu'il existe un diviseur D_2 plus grand que D tel que le groupe d'automorphismes de D_2 soit strictement plus petit que $\mathrm{Aut}(D)$.

Soit $\mathbb{L}$ le corps des fonctions de $\mathcal{C}$ et $\mathbb{M} = \bar{\mathbb{Q}}\mathbb{L}$ le corps des fonctions de $\bar{\mathcal{C}}$. Le groupe $\mathrm{Aut}(D) \subset \mathrm{Aut}(\bar{\mathcal{C}})$ agit sur $\mathbb{M}$. Notons $\mathbb{M}^D$ le sous-corps de $\mathbb{M}$ fixé par $\mathrm{Aut}(D)$ et soit $\mathbb{L}^D = \mathbb{M}^D \cap \mathbb{L}$. Alors $\mathbb{M}^D \neq \mathbb{M}$ car $\mathrm{Aut}(D)$ est non trivial. Comme $\mathrm{Aut}(D)$ n'agit pas sur $\bar{\mathbb{Q}}$ on en déduit que $\mathbb{L}^D \neq \mathbb{L}$.

Soit alors f une fonction de $\mathbb{L}$ non fixée par $\mathrm{Aut}(D)$. Si a est un rationnel, la fibre $f^{-1}(a)$ n'est pas stabilisée par $\mathrm{Aut}(D)$ sauf pour un nombre fini de valeurs de a. Il existe donc une fibre non singulière $f^{-1}(a_0)$ non stabilisée par $\mathrm{Aut}(D)$ et disjointe du support de D. Soit D_1 le diviseur positif associé et posons $D_2 = D + (\deg(D) + 1)D_1$. Alors, tout automorphisme de D_2 respecte la distribution des multiplicités et donc induit un automorphisme de D (tous les points du support de D ont multiplicité au plus $\deg(D)$) et un automorphisme de D_1. Ainsi $\mathrm{Aut}(D_2) \subset \mathrm{Aut}(D)$ et de plus $\mathrm{Aut}(D_2) \neq$

Aut(D) car Aut(D) ne stabilise pas D_1.

3. Conclusion

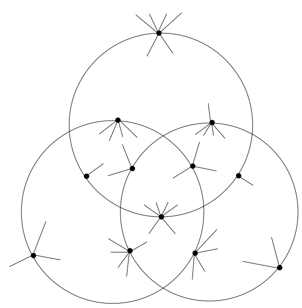
Bien que la preuve donnée plus haut soit "constructive" il ne faut pas trop compter calculer des revêtements explicites de cette manière. Dans le cas particulier des courbes de genre 0, une construction plus contournée nous a permis d'exhiber un dessin pour toute conique définie sur $\mathbb{Q}$. Nous en montrons simplement un exemple sans preuve, laissant au lecteur le soin de deviner une généralisation adéquate. Pour plus de détails, et des preuves, voir [C1], [C2].

Considérons dans $\mathbb{P}^3$ la conique d'équations

$$
\begin{aligned}
a + 2b + 3c + 5d &= 0 \\
a^2 + 2b^2 + 3c^2 + 5d^2 &= 0
\end{aligned}
$$

que nous appelons $\mathcal{C}_{1,2,3,5}$.

Alors, il existe une fonction de Belyi $\phi : \mathcal{C}_{1,2,3,5} \rightarrow \mathbb{P}_1$ sans automorphismes correspondant au dessin suivant



Nous rappelons que ce dessin est obtenu comme préimage du segment $[0,1]$ par ϕ tracée sur la surface de Riemann associée à $\mathcal{C}_{1,2,3,5}$. Les points au dessus de 0 sont représentés par des ronds noirs. Il y a 6 points au dessus de 1 ramifiés d'ordre 4. Les autres points au dessus de 1 sont non ramifiés et ils correspondent aux extrémités libres du dessin.

Notons enfin que $\mathcal{C}_{1,2,3,5}$ est isomorphe à la conique de Legendre $\mathcal{L}_{1,1,5.11}$ d'équation $x^2 + y^2 + 5.11.z^2 = 0$. Elle a donc des points rationnels sur tous les complétés de $\mathbb{Q}$ exceptés $\mathbb{R}$ et $\mathbb{Q}_{11}$.

La fonction de Belyi ϕ est définie de la façon suivante. On pose $\delta = (10a^{-1} + 9b^{-1} + 8c^{-1} + 6d^{-1})/11$ et pour tout point $P = (a, b, c, d)$ sur $\mathcal{C}_{1,2,3,5}$ on définit ϕ par

$$\phi(P) = (1 - a\delta)^m (1 - b\delta)^n (1 - c\delta)^p (1 - d\delta)^q.$$

Bibliographie

[GR] Alexandre Grothendieck, *esquisse d'un programme*, non publié (1974).

[C1] Jean-Marc Couveignes, *Calcul et rationalité de fonctions de Belyi en genre 0*, Annales de l'Institut Fourier **44** (1994), 1–38.

[C2] ______, *Quelques revêtements définis sur* $\mathbb{Q}$, à paraître dans Manuscripta Mathematica (1996).

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

[SI] Joseph Silverman, *The arithmetic of elliptic curves*, vol. 106, Springer Lecture Notes in Math., 1986.

[SC] Leila Schneps, *The Grothendieck theory of dessins d'enfant*, vol. 200, Cambridge University Press, London Mathematical Society Lecture Notes Series, 1994.

Jean-Marc COUVEIGNES
Universiteit Utrecht
Membre de l'Option Recherche du Corps des Ingénieurs de l'Armement
e-mail : couveign@math.ruu.nl