Dessins d'enfants sur les courbes elliptiques

Salim Alloun, ENS de Lyon,
Stage de M1 auprès de Leila Schneps
à l'Institut de Mathématiques de Jussieu

Résumé

En 1979, Belyi établit une caractérisation des courbes algébriques définies sur $\overline{\mathbf{Q}}$, résultat que Grothendieck trouva si « profond et déroutant » qu'il eut sur lui un « impact psychologique » conséquent. Cette caractérisation permet d'aborder le groupe de Galois absolu de $\mathbf{Q}$ de manière géométrique et topologique en en exhibant une action fidèle sur l'ensemble des dessins d'enfants. Il s'agit ici d'étudier des cas particuliers de dessins en genre 1 et de voir comment l'action s'y manifeste. En effet, si l'action galoisienne sur les dessins est comprise au niveau algébrique, aucune description purement topologique n'existe. Nous considérons la famille de les courbes elliptiques d'équation $y^2 = x(x-1)(x-\lambda)$, où λ est une racine, munies d'une fonction de Belyi canonique et donc d'un dessin canonique, et nous cherchons à expliciter la nature topologique de l'action galoisienne sur ces dessins.

Table des matières

1 Introduction

« Je ne crois pas qu'un fait mathématique m'ait jamais autant frappé que celui-là, et ait eu un impact psychologique comparable. Cela tient sûrement à la nature familière, non technique, des objets considérés, dont tout dessin d'enfant griffoné sur un bout de papier donne un exemple parfaitement explicite. À un tel dessin se trouvent associés des invariants arithmétiques subtils [...] il y a une identité profonde entre la combinatoire des cartes finies d'une part, et la gémotrie des courbes algébriques définies sur un corps de nombres, de l'autre. »

C'est ainsi que dans son *Esquisse d'un programme* , Grothendieck s'émerveille du lien entre les symétries arithmétiques des corps de nombres et la combinatoire des dessins d'enfants. À tout dessin on associe une courbe algébrique X définie sur un corps de nombres, c'est-à-dire sur $\overline{\mathbf{Q}}$. L'on peut désormais faire agir $\mathrm{G}_{\mathbf{Q}} := \mathrm{Gal}(\overline{\mathbf{Q}} \,|\, \mathbf{Q})$ sur les coefficients définissant cette courbe pour obtenir un nouveau dessin.

2 Dessins d'enfants

Définition 1.. Un *dessin d'enfant* est un triplet $D = (X_2, X_1, X_0)$, où $X_0 \subset X_1 \subset X_2$,

- X_2 est une surface de Riemann compacte,
- X_0 un ensemble fini de **sommets**,
- $X_1 \backslash X_0$ une réunion finie d'**arêtes** (ensembles homéomorphes à des segments ouverts),
- $X_2 \backslash X_1$ une réunion finie de **faces** (ensembles homéomorphes à des disques ouverts).
- Le graphe défini à partir de X_0 et X_1 est bipartite. [1]

Deux dessins D, D' sont *isomorphes* s'il existe un homéomorphisme $\phi : X_2 \to X_2'$ tel que $\phi(X_0) = X_0'$ et $\phi(X_1) = X_1'$. On note $\mathcal{D}$ l'ensemble des classes d'isomorphisme de dessins d'enfants ou *dessins abstraits*.

En fait, et c'est précisément ici que se joue la correspondance entre topologie et algèbre, chaque dessin abstrait est associé à une classe d'isomorphisme de revêtements finis de $\widehat{\mathbf{C}}$ non-ramifiés en dehors de $\{0, 1, \infty\}$.

Définition 2.. Une *fonction de Belyi* sur une surface de Riemann X est une fonction méromorphe $X \longrightarrow \widehat{\mathbf{C}}$ dont les valeurs critiques appartiennent à $\{0, 1, \infty\}$, on appelle (X, β) un *couple de Belyi*. Deux couples de Belyi (X, β), (X', β') sont isomorphes s'il existe un biholomorphisme $\phi : X \longrightarrow X'$ tel que $\beta' \circ \phi = \beta$.

1. Deux sommets sont connectés s'ils sont dans l'adhérence d'une arête et on dira rouge et bleu pour les couleurs des sommets de X_0

Théorème 3.. Si (X, β) est un couple de Belyi alors $(X, \beta^{-1}[0,1], \beta^{-1}\{0,1\})$ est un dessin d'enfant noté $D(X, \beta)$.

PREUVE. β n'est pas ramifié dans $]0,1[$ donc $\beta^{-1}[0,1]\backslash\beta^{-1}\{0,1\}$ est la réunion finie (car X compact) de ses composantes connexes qui sont des arêtes puisque $]0,1[$ est une arête.

Soit $\gamma :]0,1[\longrightarrow X$ paramétrant une arête, qu'on définit comme un inverse de β sur une arête et qu'on peut étendre par continuité avec $\beta(\gamma(0))$ et $\beta(\gamma(1))$ dans $\{0,1\}$. Si $\beta_{\gamma(0)} = \beta(\gamma(1))$ alors le théorème de Rolle assure que $\beta'(\gamma(c))\gamma'(c) = 0$ pour $c \in]0,1[$, ce qui est absurde car β n'est pas ramifié en $\gamma(c)$. Les arêtes ne relient donc pas des préimages de 0 entre elles ou de préimages de 1 entre elles □

Corollaire 4.. Notons e_0, e_1, e_∞ le nombre de préimages respectivement de $0, 1, \infty$. $D(X, \beta)$ a e_0 sommets bleus, e_1 sommets rouges, $\deg(\beta)$ arêtes et e_∞ faces. De plus le nombre d'arêtes sortantes correspond à la multiplicté de β en ce point

PREUVE. Il y a par définition e_0 sommets bleus et e_1 sommets rouges.

Chaque arête correspond à la préimage d'un point non-ramifié de $]0,1[$, par exemple $1/2$, qui a exactement $\deg(\beta)$ préimages.

Ainsi en notant F le nombre de faces on a $e_0 + e_1| - \deg(\beta) + F = \chi(X)$. Or en notant M_p la multiplicité de β en p la formule de Riemman-Hurwitz donne que

$$\chi(X) = \deg(\beta)\chi(\widehat{\mathbf{C}}) - \sum_{p\in X}(M_p - 1)$$

Or β n'est ramifié qu'au-dessus de $0, 1, \infty$ donc

$$\begin{aligned}\sum_{p\in X}(M_p - 1) &= \sum_{\beta(p)=0}(M_p - 1) + \sum_{\beta(p)=1}(M_p - 1) + \sum_{\beta(p)=\infty}(M_p - 1)\\ &= \deg(\beta) - e_0 + \deg(\beta) - e_1 + \deg(\beta) - e_\infty\end{aligned}$$

En combinant les équations on arrive à $F = e_\infty$.

Le dernier point du théorème découle directement de la forme locale $z \mapsto z^k$ d'une fonction méromorphe autour d'un point de multiplicité k □

Ici, une courbe algébrique projective est toujours considérée de la sorte : c'est le compactifié d'une courbe algébrique affine lisse du type $\{f(x,y) = 0\} \subset \mathbf{C}^2$, où $f \in \mathbf{C}[x,y]$. Le théorème suivant est le théorème central qui a montré l'intêret du sujet à Grothendieck.

Théorème de Belyi. Une courbe algébrique projective X admet un modèle sur $\overline{\mathbf{Q}}$ si et seulement si X possède une fonction de Belyi.

PREUVE. [2] Supposons que X soit définie sur $\overline{\mathbf{Q}}$. Alors on dispose d'une fonction g

2. Je reprends ici la preuve écrite dans [4] en changeant juste un peu l'algorithme donnant la fonction de Belyi.

méromorphe sur X dont les valeurs critiques sont dans $\overline{\mathbf{Q}}$, on prend par exemple $(x, y) \mapsto x$ (les valeurs critiques vérifient des équations polynomiales à coefficient dans $\overline{\mathbf{Q}}$, et $\overline{\mathbf{Q}}$ est algébriquement clos).

Ensuite on définit des polynômes $f_0, f_1, \ldots, f_n \in \mathbf{Q}[z]$ de telle sorte à ce que les valeurs critiques de $h := f_n \circ f_{n-1} \circ \cdots \circ f_0 \circ g$ soient dans $\mathbf{Q}$. Soit S l'ensemble des valeurs critiques irrationnelles de g, et S' l'ensemble des conjugués galoisiens des éléments de S. On pose $f_0(z) = \prod_{s \in S'}(z - s)$. f_0 est à coefficients rationnels car il est produit de polynômes minimaux sur $\mathbf{Q}$.

Pour tout $i \geqslant 0$,

$$f_{i+1}(z) = \mathrm{Res}(f_i', f_i - z) \in \mathbf{Q}[z]$$

Ainsi, chaque point critique de f_i est envoyé sur 0 par $f_{i+1} \circ f_i$. De plus, $(\deg(f_i))$ est strictement décroissante car $\deg(f_{i+1}) \leqslant \deg(f_i') < \deg(f_i)$. On pose n tel que $\deg(f_{n+2}) = 0$.

Les valeurs critiques de la composée $a \circ b$ sont les images par a des valeurs critiques de b ou parmi les valeurs critiques de a. Par conséquent, les valeurs critiques de h sont des deux types suivants :

— Les images par h des valeurs critiques rationnelles de g. Ce sont bien des nombres rationnels car $h \in \mathbf{Q}[z]$.

— Définissons E_i par $E_1 = 0$ et $E_{i+1} = f_{i-1}(E_i) \cup \{0\}$. Alors E_{n+1} (ensemble de nombres rationnels) contient toutes les autres valeurs critiques puisque initialement S est envoyé sur 0 par f_0, et par définition des f_i chaque point critique de f_i est envoyé sur 0 par f_{i+1}.

Finalement, il reste à envoyer ces valeurs rationnelles sur $0, 1, \infty$. À l'aide du lemme 1.4 dans [2] on peut composer h avec une fraction rationnelle pour avoir une fonction de Belyi sur X.

La réciproque dans le cas général est bien plus difficile à démontrer et peut être trouvée dans [5]. Dans la section suivante on la démontre dans le cas où X est une courbe elliptique.

Ainsi quels que soient $\sigma \in \mathrm{G}_{\mathbf{Q}}$ et (X, β) couple de Belyi on peut définir (X^σ, β^σ) tel que le diagramme suivant est commutatif :

$$\begin{array}{ccc} X & \xrightarrow{\sigma} & X^\sigma \\ \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \beta^\sigma} \\ \widehat{\mathbf{C}} & \xrightarrow{\sigma} & \widehat{\mathbf{C}} \end{array}$$

Ainsi $\mathrm{G}_{\mathbf{Q}}$ agit sur {classes d'isomorphismes de couples de Belyi}.

Un deuxième point de vue consiste à utiliser la correspondance de Galois qui implique qu'il y a une bijection entre les sous-groupes d'indice fini de $\pi_1(\widehat{\mathbf{C}} \setminus \{0, 1, \infty\})$ et les revêtements finis de $\widehat{\mathbf{C}}$ dont les points de ramification sont dans $\{0, 1, \infty\}$.

3 Cas des courbes elliptiques

Dans [4] on étudie les dessins d'enfants sur la sphère de Riemann et on démontre en particulier que l'action de $\mathrm{G}_{\mathbf{Q}}$ sur les arbres est fidèle.

Ici on s'intéresse au cas des courbes elliptiques. Rapellons qu'il s'agit des courbes de genre 1, on peut les représenter de deux manières, sous la forme $\mathbf{C}/\Lambda$ (où Λ est un réseau) ou sous la forme $y^2 = 4x^3 - g_2x + g_3$, biholomorphes via la fonction de Weierstrass — via une transformation affine on peut se ramener à la forme de Legendre $y^2 = x(x-1)(x-\lambda)$ avec $\lambda \neq 1, \lambda \neq 0$. Dans la suite on va noter $E(\lambda)$ la courbe projective d'équation $y^2 = x(x-1)(x-\lambda)$.

Réciproque du [Théorème de Belyi] : Il s'agit de montrer qu'une courbe elliptique X admettant une fonction de Belyi admet un modèle sur $\mathbf{Q}$.

Dans [5] on montre que (X, β) est un couple de Belyi si et seulement si $X \simeq \Gamma\backslash\mathcal{H}$ et Γ est un groupe d'indice fini d'un groupe triangulaire Δ dont la signature correspond aux ramifications de β en $0, 1, \infty$ et β correspond à la projection canonique $\Gamma\backslash\mathcal{H} \longrightarrow \Delta\backslash\mathcal{H}$.

Lemme 5. Notons $\mathrm{G}_{\mathbf{C}}$ le groupe $\mathrm{Aut}(\mathbf{C} \mid \mathbf{Q})$ des automorphismes de $\mathbf{C}$ qui présèrvent $\mathbf{Q}$. Soit Y une courbe admettant une fonction de Belyi. Alors il existe un sous-groupe U de $\mathrm{G}_{\mathbf{C}}$ d'indice fini tel que pour tout $\sigma \in U$, $X \simeq X^{\sigma}$. Notons $M(X)$ le corps fixé par U. Alors $M(X) \subset \overline{\mathbf{Q}}$.

Preuve. X^{σ} est de la forme $\Gamma^{\sigma}\backslash\mathcal{H}$ où Γ^{σ} est un sous-groupe d'un certain Δ^{σ}, et $\beta^{\sigma} = \Gamma^{\sigma}\backslash\mathcal{H} \to \Delta^{\sigma}\backslash\mathcal{H}$. Or σ est un automorphisme de corps donc β^{σ} et β ont mêmes degrés de ramification et même degré. Par conséquent, $\Delta = \Delta^{\sigma}$ et $[\Gamma : \Delta] = [\Gamma^{\sigma} : \Delta]$. Finalement, il n'y a — à conjugaison près — qu'un nombre fini de sous-groupes de Δ ayant le même indice, car Δ est finiment engendré. D'où l'existence de U.

Soit $x \in M(X)$. Alors U étant d'indice fini, il existe $x = x_1, x_2, \ldots, x_n \in \mathbf{C}$ tels que $\{x_i\}$ est stable par $\mathrm{G}_{\mathbf{C}}$. Par conséquent, le polynôme $(z - x_1)\cdots(z - x_n)$ est stable par $\mathrm{G}_{\mathbf{C}}$, donc appartient à $\mathbf{Q}[z]$ et est annulé par x ; x est donc algébrique. □

Théorème 6. Il existe une courbe C définie sur $\overline{\mathbf{Q}}$ telle que pour tout $\sigma \in U$, $C \simeq X^{\sigma}$. Preuve. La classe d'isomorphisme d'une courbe elliptique est déterminée par son $j-$invariant. Or $j(X)$ est une fraction rationnelle des coefficients de X, donc $j(X^{\sigma}) = \sigma(j(X))$. Ainsi, $\sigma(j(X)) = j(X)$ pour tout $\sigma \in U$ et donc $j(X) \in M(X) \subset \overline{\mathbf{Q}}$ d'après le lemme 5 . Or la courbe $E = \{y^2 = 4x^3 - \frac{27j}{j-1}(x-1)\}$ vérifie $j(E) = j$. (voir [2]) Par conséquent, dans la classe d'isomorphismes de courbes de X il y a une courbe définie sur $\mathbf{Q}(j(X)) \subset \overline{\mathbf{Q}}$. □

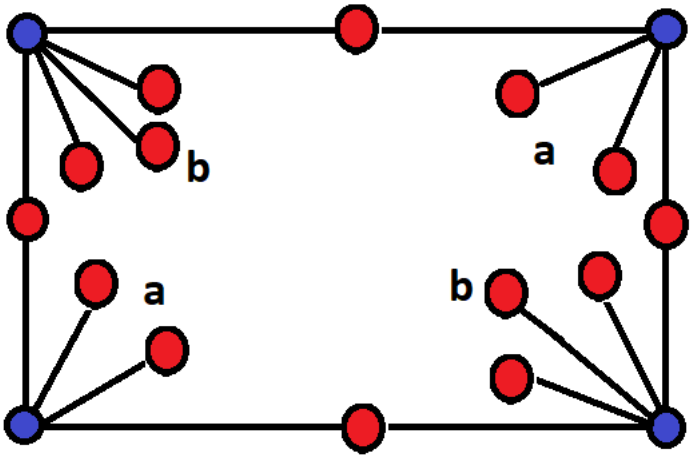
On a donc démontré qu'une courbe elliptique admettant une fonction de Belyi admet un modèle sur $\overline{\mathbf{Q}}$.

4 Exemple

L'algorithme qui apparaît dans la sens facile du rmet d'associer à chaque courbe un dessin canonique. Cependant le degré de la fonction de Belyi associé augmente très rapidement. On peut considérer une famille plus simple de dessins dont l'action de $\mathrm{G}_{\mathbf{Q}}$ est abélienne. En notant $\zeta_n = \exp 2i\pi/n$ il s'agit des dessins $D_{n,k}$ définis par

$$D_{n,k} = D(E(\zeta_n^k), x^n)$$

Théorème 7. Pour $k \neq 0(n)$, $D_{n,k}$ définit bien un dessin d'enfant et est de la forme suivante :



$a = 3$ et $b = 2$

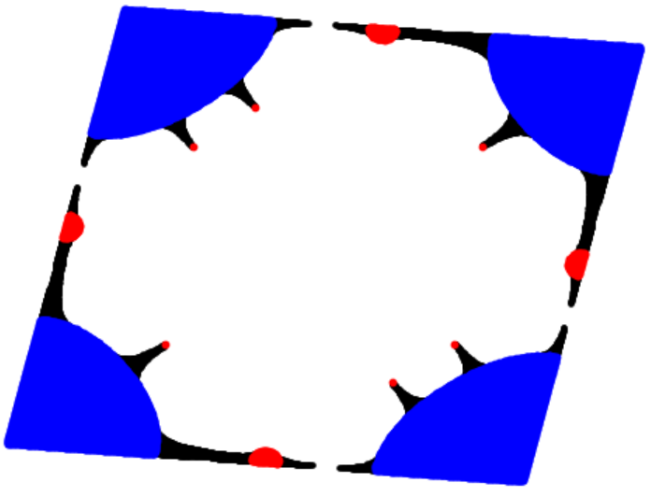
(où l'on a donc recollé les côtés opposés pour avoir un tore)

et $\boxed{a + b = n - 2}$, notons ce dessin abstrait $C(a, b)$.

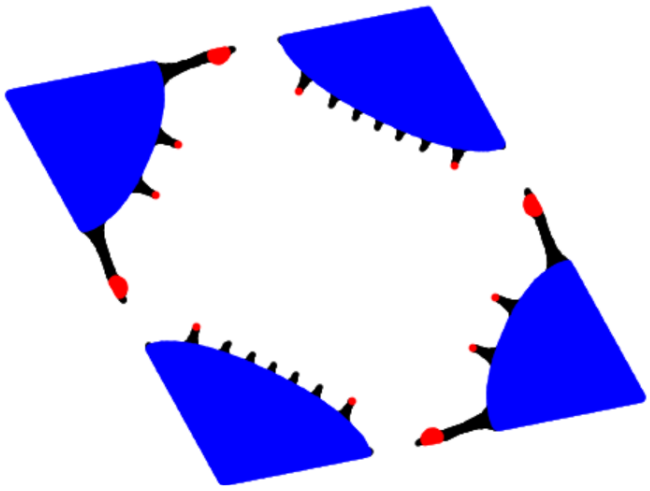
Preuve. $x \mapsto x^n$ n'a qu'un point critique qui est 0, et les valeurs critiques de $(x, y) \mapsto x$ sont $(0, 0), (1, 0), (\zeta_n^k, 0) et le point à l'infini$. Ainsi par composition $(x, y) \mapsto x^n$ est bien une fonction de Belyi de degré $2n$. Il y a un seul sommet bleu qui est $(0, 0)$ d'ordre $2n$. Les préimages de 1 sont les $(\zeta_n^p, \pm y_p)$, il y en a $2n-2$ car $(x, y) \mapsto x$ a comme valeur critique 1 et ζ_n^k donc $y_1 = 0$ et $y_k = 0$. Ce qui donne deux sommets rouges de degré 2 et $2n - 2$ sommets de degré 1. Si on prend la représentation de la courbe sous la forme $\mathbf{C}/\Lambda$ alors on remarque que le dessin doit être symétrique par rapport à 0 puisque β ne dépend pas de y et $z \mapsto -z$ équivaut à $(x, y) \mapsto (x, -y)$ (voir [3]). Enfin $2a+2b = 2n-2$, donc $a + b = n - 2$. □

À l'aide de Python j'ai calculé numériquement pour entrevoir la formule en tant que dessins abstraits

$$\boxed{D_{n,k} = C(k - 1, n - 1 - k)}$$



$D_{5,2}$



$D_{11,3}$

(Le calcul se faisant par approximation il faut voir la zone bleue comme un sommet...)

Remarquons qu'en tant que dessins abstraits $C(a,b) = C(b,a)$, comment le voit-on sur ces dessins ? Dans [2] on remarque que l'écriture sous-forme d'équation de Legendre $y^2 = x(x-1)(x-\lambda)$ d'une classe d'isomorhpie de courbes algébriques est possible en remplaçant λ par $1/\lambda$, ce qui dans les cas des racines de l'unité consiste à remplaçer ζ_n^k par $\zeta_n^{-k} = \zeta_n^{n-k}$ ce qui est compatible avec le fait que en tant que dessins abstraits $D_{n,k} = D_{n,n-k}$

Finalement, dans ce cas l'action de $\mathrm{G}_{\mathbf{Q}}$ sur l'orbite de $D_{n,k}$ se résume à l'action de $\mathrm{Gal}(\mathbf{Q}(\zeta_n), \mathbf{Q}) \simeq (\mathbf{Z}/n\mathbf{Z})^\times$. Plus précisément on peut quotienter $(\mathbf{Z}/n\mathbf{Z})^\times$ par $\{1, -1\}$ pour avoir une action libre sur l'orbite des dessins abstraits à partir de $D_{n,k}$.

Bibliographie

[1] A. Grothendieck, *Esquisse d'un programme*, Lond. Math. Soc., Lecture Notes 242 (1997).

[2] G. A. Jones and J. Wolfart, *Dessins d'Enfants on Riemann Surfaces*, Springer, 2016.

[3] A. W. Knapp, *Elliptic Curves*, no. 40 in Princeton Mathematical Notes, Princeton University Press, 1992.

[4] L. Schneps, *Dessins d'enfants on the riemann sphere*, London Math. Soc., Lecture Notes 242 (1997).

[5] J. Wolfart, *Geometric galois actions : The 'obvious' part of belyi's theorem and riemann surfaces with many automorphisms*, vol. Lecture Notes 242, Cambridge University Press, 1997.