LE THEOREME DE BELYI

(Exposé de première année de magistère)

Sujet proposé par Y. Laszlo

David Madore (`david.madore@ens.fr`)
et Jean Marot (`jean.marot@ens.fr`)

Résumé : Un théorème dû à Riemann affirme que toute surface de Riemann compacte X est en fait une courbe algébrique (projective lisse) — c'est-à-dire peut être définie par des équations algébriques. La question se pose de savoir quand ces équations peuvent être choisies à coefficients dans $\bar{\mathbb{Q}}$, la clôture algébrique de $\mathbb{Q}$. Le théorème de Belyĭ donne une condition nécessaire et suffisante portant uniquement sur la géométrie de la surface : il faut et il suffit que celle-ci se réalise comme un revêtement holomorphe de la sphère de Riemann Σ ramifié en au plus trois points de Σ.

Cette caractérisation étant obtenue, on en déduit une action fidèle du groupe de Galois "absolu" de $\bar{\mathbb{Q}}/\mathbb{Q}$ sur le groupe profini libre à deux générateurs.

Abstract: A theorem due to Riemann asserts that every compact Riemann surface X is in fact a (smooth projective) algebraic curve — that is, can be defined by algebraic equations. The question arises of when these equations can be chosen with coefficients in $\bar{\mathbb{Q}}$, the algebraic closure of $\mathbb{Q}$. Belyĭ's theorem gives a necessary and sufficient condition involving only the geometry of the surface: namely, that it can be realized as a branched covering of the Riemann sphere Σ having at most three ramification points in Σ.

From this characterization one deduces a faithful action of the "absolute" Galois group of $\bar{\mathbb{Q}}/\mathbb{Q}$ on the free profinite group with two generators.

Préliminaires sur les surfaces de Riemann.

Une <u>surface de Riemann</u> est une variété différentiable de dimension 1 complexe (2 réelle) munie d'un atlas dont les changements de cartes sont holomorphes. Une application entre surfaces de Riemann qui, dans les systèmes de coordonnées donnés par un tel atlas, se représente par des fonctions holomorphes, est dite holomorphe. Les morphismes entre surfaces de Riemann sont les applications holomorphes. Les isomorphismes entre surfaces de Riemann sont les applications holomorphes bijectives (la réciproque en est alors nécessairement holomorphe).

Exemples : Le plan complexe $\mathbb{C}$, la sphère de Riemann notée $\bar{\mathbb{C}}$, $\mathbb{P}^1(\mathbb{C})$ ou Σ, et le <u>demi-plan de Poincaré</u>

$$\mathcal{H} := \{z \in \mathbb{C}\colon \operatorname{Im} z > 0\}$$

sont des surfaces de Riemann — ce sont d'ailleurs les seules simplement connexes.

On rappelle qu'un <u>point critique</u> d'une fonction différentiable f (entre variétés différentiables) est un point où f n'est pas submersive. Une <u>valeur critique</u> est l'image d'un point critique. Un point de la variété d'arrivée qui n'est pas une valeur critique (y compris s'il n'est pas atteint du tout) est appelé <u>valeur régulière</u>.

Une application continue surjective $p\colon X \to Y$ entre espaces topologiques non vides est appelée un <u>revêtement [topologique]</u> ssi pour tout point $y \in Y$ il existe un voisinage ouvert V de y dans Y tel que $p^{-1}(V)$ soit une union disjointe d'ouverts U_i avec $p|_{U_i}\colon U_i \to V$ un homéomorphisme pour tout i. Le nombre de préimages d'un point $y \in Y$ est alors localement constant, donc constant si Y est connexe. Dans ce dernier cas, et s'il est fini, on l'appelle le <u>degré</u> du revêtement. Il est clair que le degré d'une composée est le produit des degrés.

On appellera <u>revêtement [holomorphe] ramifié</u> une application $f\colon X \to Y$ holomorphe non constante *propre* entre surfaces de Riemann. Si de plus f est sans valeur critique, alors f

est un revêtement au sens topologique ([Dol]). Quitte à restreindre le domaine, on peut toujours se ramener à ce cas, et ainsi définir le degré $\deg f$ de f même dans le cas ramifié. On utilise ici implicitement le fait que l'ensemble des valeurs régulières est non vide — en fait l'ensemble des valeurs critiques d'une application C^∞ entre variétés différentielles est de mesure nulle, c'est le théorème de Morse-Sard, cf. [Hir] — mais puisqu'ici on ne se servira du degré que pour des revêtements entre surfaces de Riemann compactes, ce résultat n'est pas nécessaire. On a encore la propriété de multiplicativité des degrés $\deg(fg) = (\deg f)(\deg g)$. On remarquera que toute application holomorphe non constante entre surfaces de Riemann *compactes* est un revêtement ramifié (en effet, elle est trivialement propre).

Il est bien connu que toute application holomorphe non constante est localement, et à changement de variable près, l'application $z \mapsto z^n$ avec $n > 0$; n est alors appelé l'indice de ramification au point considéré. On montre ([Dol], [Gun], [Far]) que le degré d'un revêtement ramifié est égal à la somme des indices de ramification des préimages d'un point quelconque.

Soient $f_1, \ldots, f_m$ des polynômes à coefficients complexes homogènes en les $n+1$ variables $z_0, \ldots, z_n$, et supposons de plus que la matrice jacobienne $(\frac{\partial f_i}{\partial z_j})$ soit de rang $n-1$ en tout point de $\mathbb{C}^{n+1} \setminus \{0\}$ où tous les f_i s'annulent. Alors l'ensemble

$$X = \{(z_0 \colon z_1 \colon \cdots \colon z_n) \colon f_1(z_0, \ldots, z_n) = \cdots = f_m(z_0, \ldots, z_n)\}$$

des zéros communs aux f_i dans l'espace projectif $\mathbb{P}^n(\mathbb{C})$ est une sous-variété différentiable de celui-ci, de dimension 2 réelle. On le munit d'une structure de surface de Riemann en décrétant que les projections $(z_0 \colon \cdots \colon z_n) \mapsto z_i/z_j$ sont toutes holomorphes (là où elles sont définies). Une telle surface de Riemann est appelée une <u>courbe algébrique</u> projective lisse, définie par les équations $f_1 = \cdots = f_m = 0$.

Lorsque X est une courbe algébrique projective lisse, définie par les équations $f_1 = \cdots = f_m = 0$, on appelle <u>fonction rationnelle</u> sur X un élément *de degré zéro* du corps des fractions du quotient de $\mathbb{C}[X_0, \ldots, X_n]$ par l'idéal engendré par $f_1, \ldots, f_m$, c'est-à-dire le rapport de deux classes de polynômes homogènes de même degré. Les fonctions rationnelles définissent des fonctions holomorphes de X privé d'un nombre fini de points (les zéros communs au numérateur et au dénominateur) vers la sphère de Riemann Σ. En regardant dans des cartes, on voit aisément que ces points manquants ne sont pas des singularités essentielles, et qu'il est donc possible d'étendre les fonctions rationnelles en des fonctions holomorphes sur X tout entier.

On a le théorème fondamental suivant :

Théorème de Riemann. *Toute surface de Riemann compacte est (isomorphe à) une courbe algébrique projective lisse. De plus, toute fonction méromorphe dessus est rationnelle.*

:-([Dol], [Far] ou [Gun]. :-)

Classification des surfaces de Riemann compactes : On rappelle ([Hir]) qu'une surface différentiable compacte orientable est classifiée par un unique invariant : son genre. Par conséquent, le genre constitue également un invariant des surfaces de Riemann compactes. Ainsi, la sphère de Riemann est la seule surface de Riemann compacte de genre 0. En revanche, pour tout genre $g \geq 1$, l'ensemble des classes d'isomorphismes de surfaces de Riemann compactes de genre g est indénombrable — dans un sens que nous ne préciserons pas, elles sont classifiées par $3g-3$ paramètres complexes pour $g \geq 2$, et par un seul paramètre pour $g = 1$ (voir plus loin).

Théorème de Belyĭ.

On appelle fonction de Belyĭ sur une surface de Riemann X un revêtement ramifié $\beta: X \to \Sigma$ (où Σ est la sphère de Riemann) dont l'ensemble des valeurs critiques est contenu dans $\{0, 1, \infty\}$.

Exemple fondamental : Pour $m, n \in \mathbb{Z}$, avec $m, n, m+n \neq 0$, posons

$$\begin{aligned} \beta_{m,n}: \Sigma &\to \Sigma \\ z &\mapsto \frac{(m+n)^{m+n}}{m^m n^n} z^m (1-z)^n \end{aligned}.$$

On a alors, en dehors de ∞ et des pôles éventuels,

$$\beta'_{m,n}(z) = \frac{(m+n)^{m+n}}{m^m n^n} z^{m-1}(1-z)^{n-1}(m-(m+n)z),$$

et par conséquent $\beta'_{m,n}(z)$ ne s'annule pas en-dehors de 0, 1 et $\frac{m}{m+n}$. L'ensemble des points critiques est donc inclus dans $\{0, 1, \frac{m}{m+n}, \infty\}$, et l'ensemble des valeurs critiques, dans $\{0, 1, \infty\}$. Il s'ensuit que $\beta_{m,n}$ est une fonction de Belyĭ.

Théorème de Belyĭ. *Soit X une courbe algébrique projective lisse définie par des équations à coefficients dans $\bar{\mathbb{Q}}$. Alors il existe une fonction de Belyĭ $\beta: X \to \Sigma$.*

On aura pour cela besoin du résultat suivant, qui découle immédiatement de la formule de composition des différentielles :

Lemme. *Soit $f_i: X_i \to X_{i+1}$ une application C^∞ pour tout $1 \leq i \leq r-1$ avec X_i des variétés différentiables. Alors les valeurs critiques de $f_{r-1} \circ \cdots \circ f_1$ sont exactement les $y \in X_r$ qui sont image par $f_{r-1} \circ \cdots \circ f_{i+1}$ d'une valeur critique de f_i, pour un certain i.*

:-((du théorème) Supposons X définie par des équations polynômiales dans $\mathbb{P}^n(\mathbb{C})$. On peut clairement supposer que X n'est pas entièrement contenue dans un hyperplan. Alors la fonction rationnelle $(z_0: \cdots : z_n) \mapsto z_1/z_0$ restreinte à X définit une fonction méromorphe non constante sur X, c'est-à-dire un revêtement ramifié $\pi: X \to \Sigma$. Les équations définissant X étant à coefficients algébriques, les valeurs critiques de π sont clairement dans $\bar{\mathbb{Q}} \cup \{\infty\}$.

Soit f_1 le polynôme minimal sur $\mathbb{Q}$ de l'ensemble des valeurs critiques finies de π, c'est-à-dire le polynôme (unitaire) à coefficients rationnels de plus petit degré s'annulant sur toutes les valeurs critiques finies de π — un tel polynôme existe puisque les valeurs critiques en question sont algébriques. Par récurrence, soit f_{i+1} le polynôme minimal sur $\mathbb{Q}$ de l'ensemble des valeurs critiques finies de f_i. Or tout conjugué algébrique d'un zéro de f'_i est un zéro de f'_i (car $f'_i \in \mathbb{Q}[X]$), donc tout conjugué algébrique d'une valeur critique de f_i est une valeur critique de f_i. Comme celles-ci sont en nombre au plus $\deg f_i - 1$, il s'ensuit que $\deg f_{i+1} \leq \deg f_i - 1$, et les f_i forment une suite de polynômes dont les degrés décroissent strictement. Ainsi, il existe k tel que les valeurs critiques finies de f_k soient rationnelles. Considérons l'application composée

$$\rho = f_k \circ \cdots \circ f_1 \circ \pi: X \to \Sigma :$$

les valeurs critiques finies de π sont envoyées dans $\mathbb{Q}$ par f_1 et y restent par l'action de $f_k \circ \cdots \circ f_2$; de même, les valeurs critiques finies de f_i sont envoyées dans $\mathbb{Q}$ par f_{i+1} et y restent par l'action de $f_k \circ \cdots \circ f_{i+2}$. En appliquant le lemme, on dispose maintenant d'une application $\rho: X \to \Sigma$ dont toutes les valeurs critiques finies sont rationnelles.

Soit A_1 l'ensemble des valeurs critiques finies de ρ autres que 0 et 1. Cet ensemble est bien entendu fini. S'il est vide, le théorème est démontré. Sinon, il contient un rationnel, qui peut s'écrire sous la forme $\frac{m}{m+n}$ avec $m, n, m+n \neq 0$. Posons $g_1 = \beta_{m,n}$. Par récurrence, on définit A_{i+1} comme l'ensemble des valeurs critiques finies de $g_i \circ \cdots \circ g_1 \circ \rho$ autres que 0 et 1, et, s'il contient un rationnel $\frac{m}{m+n}$, on pose $g_{i+1} = \beta_{m,n}$. D'après le lemme, et puisque les valeurs critiques de chaque g_i sont contenues dans $\{0, 1, \infty\}$, chaque A_{i+1} est contenu dans $g_i(A_{i+1})$. Comme de plus $\beta_{m,n}$ envoie $\frac{m}{m+n}$ sur 1, on a card $A_{i+1} <$ card A_i pour tout i, et par conséquent il existe i tel que $A_i = \emptyset$. Alors la fonction

$$\beta = g_{i-1} \circ \cdots \circ g_1 \circ \rho$$

est la fonction de Belyĭ recherchée. :-)

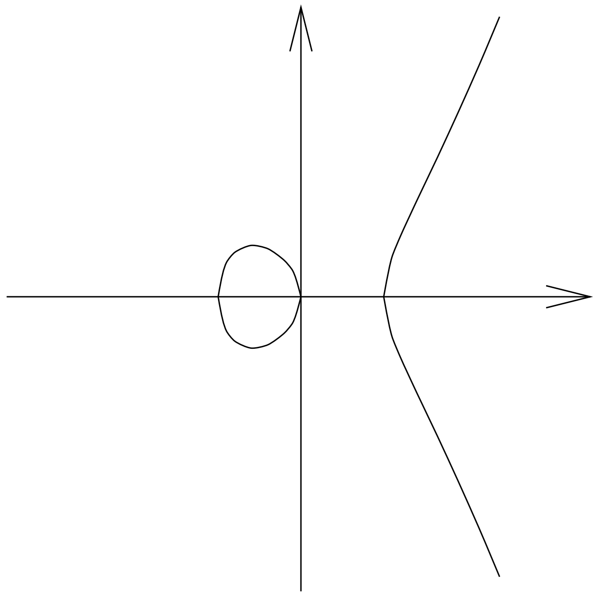
Remarque : La réciproque de ce théorème est vraie en toute généralité — une surface de Riemann compacte sur laquelle il existe une fonction de Belyĭ peut être définie par des équations à coefficients algébriques. Ce résultat sera démontré plus bas dans le cas particulier des courbes elliptiques.

Courbes elliptiques (tores complexes).

On appelle courbe elliptique une surface de Riemann compacte de genre 1 ; on montre [Sil] qu'elle est isomorphe à une courbe algébrique dans $\mathbb{P}^2(\mathbb{C})$ d'équation

$$Y^2 Z = 4X^3 - g_2 X Z^2 - g_3 Z^3,$$

où g_2, g_3 sont des coefficients complexes vérifiant $\Delta := g_2^3 - 27g_3^2 \neq 0$. Ce Δ s'appelle alors le discriminant de la courbe elliptique — ce n'est autre que le discriminant du polynôme $4x^3 - g_2 x - g^3$, à un facteur près. Réciproquement, toute équation de cette forme est une courbe elliptique. On définit de plus l'invariant j de la courbe comme $1728 g_2^3/\Delta$.



La courbe elliptique d'invariant 1728.

Théorème. *Deux courbes elliptiques sont isomorphes (en tant que surfaces de Riemann) ssi elles ont le même invariant j. De plus, pour tout $j \in \mathbb{C}$ il existe une courbe elliptique d'invariant j.*

:-(On trouvera dans [Sil] une démonstration du fait que deux courbes elliptiques sont isomorphes en tant que courbes algébriques ssi elles ont le même invariant j, et dans [Dol], [Far] ou [Gun] une démonstration que deux surfaces de Riemann compactes sont isomorphes en tant que surfaces de Riemann ssi elles le sont en tant que courbes algébriques. Posons enfin $J = j/1728$ et $g_2 = g_3 = \frac{27J}{J-1}$ (si $J \neq 0, 1$; si $J = 0$, on prend $g_2 = 0$ et $g_3 = 1$; si $J = 1$, on prend $g_2 = 1$ et $g_3 = 0$). La courbe d'équation $Y^2Z = 4X^3 - g_2XZ^2 - g_3Z^3$ est alors une courbe elliptique d'invariant j. :-)

Proposition. *Une courbe elliptique X peut être définie par des équations algébriques à coefficients dans un sous-corps K de $\mathbb{C}$ ssi son invariant j appartient à K.*

:-(Si X est définie par des équations à coefficients dans K, alors on peut ramener par des transformations rationnelles sur K ces équations à une équation sous forme de Weierstraß, $Y^2Z = 4X^3 - g_2XZ^2 - g_3Z^3$, avec $g_2, g_3 \in K$ (voir [Sil] pour les détails). On a alors évidemment $j \in K$. Réciproquement, si $j \in K$, la courbe définie dans la démonstration du théorème précédent est à coefficients dans K, et puisqu'elle a le même invariant j que X, elle lui est isomorphe. Autrement dit, X peut être définie par une équation à coefficients dans K. :-)

On peut alors démontrer la réciproque du théorème de Belyĭ pour les courbes elliptiques ; on a tout d'abord besoin du

Lemme. *Soit G un groupe finiment engendré. Alors pour tout n, G n'a qu'un nombre fini de sous-groupes d'indice n.*

:-(Soit G un groupe engendré par $g_1, \ldots, g_k$. Si H est un sous-groupe de G d'indice n, identifions les classes à gauches de H à $\{1, \ldots, n\}$ où 1 représente H lui-même. L'action de G par multiplication à gauche définit alors un morphisme $G \to \mathfrak{S}_n$. Ces morphismes sont en nombre fini puisqu'il suffit pour en définir un de fixer les images de $g_1, \ldots, g_k$. Et de plus, H est alors le stabilisateur de 1 pour cette action. :-)

Théorème. *Soit X une courbe elliptique. On suppose qu'il existe une fonction de Belyĭ $\beta: X \to \Sigma$. Alors X peut être définie par des équations à coefficients algébriques.*

:-(Soit $\Sigma_0 = \Sigma \setminus \{0, 1, \infty\}$, et $X_0 = \beta^{-1}(\Sigma_0)$. Ainsi, la restriction $\beta: X_0 \to \Sigma_0$ est un revêtement (au sens topologique). Il en va de même de $\beta^\sigma: X_0^\sigma \to \Sigma_0$ pour tout automorphisme σ de $\mathbb{C}$ (β^σ s'obtient en appliquant σ à tous les coefficients de β, et de même pour X^σ). D'après la théorie générale des revêtements ([Dou], [God]), il lui correspond un sous-groupe H d'indice $\deg \beta$ de $\pi_1(\Sigma_0)$, lequel n'est autre que le groupe libre $\mathfrak{F}$ sur deux générateurs (précisément, H est le sous-groupe constitué des lacets dans Σ_0 qui se relèvent en un lacet dans X_0). De plus, deux revêtements correspondant au même sous-groupe (ou même à des sous-groupes conjugués) sont isomorphes. Or $\mathfrak{F}$ n'a qu'un nombre fini de sous-groupes d'indice fini donné, donc il n'existe qu'un nombre fini de revêtements $\beta^\sigma: X_0^\sigma \to \Sigma_0$ deux-à-deux non isomorphes. La théorie des revêtements des surfaces de Riemann (cf. [Dol]) assure alors que d'une part les isomorphismes obtenus sont holomorphes, et d'autre part qu'ils se prolongent en des isomorphismes $X^\sigma \to X^\tau$. Ainsi, il n'y a qu'un nombre fini de X^σ deux à deux non isomorphes, et donc qu'un nombre fini de j^σ distincts (puisque $j(X^\sigma) = j^\sigma$). Ceci implique que j est algébrique, et donc que X peut être définie par des équations à coefficients algébriques. :-)

Groupes de Galois.

Si $\beta: X \to \Sigma$ est une fonction de Belyĭ, où X est une surface de Riemann compacte, alors la composition par β induit un morphisme $\beta^*: \bar{\mathbb{Q}}(t) \hookrightarrow \bar{\mathbb{Q}}(X)$, où $\bar{\mathbb{Q}}(X)$ désigne le corps des fonctions rationnelles sur X à coefficients dans $\bar{\mathbb{Q}}$ (des équations algébriques de X à coefficients dans $\bar{\mathbb{Q}}$ étant choisies). De plus ([Dol], [Sil]), si l'extension $\bar{\mathbb{Q}}(X)/\bar{\mathbb{Q}}(t)$ est galoisienne (on dit que β est galoisien), le groupe de Galois de $\bar{\mathbb{Q}}(X)/\bar{\mathbb{Q}}(t)$ est le groupe $\mathrm{Aut}(\beta)$ des automorphismes de β (automorphismes de X au-dessus de Σ) — et celui-ci est le quotient de $\pi_1(\Sigma_0)$ par un sous-groupe distingué d'indice $\deg \beta$, soit $\mathfrak{F}/H$ avec $\mathfrak{F}$ le groupe libre sur deux générateurs et H un sous-groupe distingué d'indice fini de $\mathfrak{F}$.

Si $\beta_1: X_1 \to \Sigma$ et $\beta_2: X_2 \to \Sigma$ sont deux fonctions de Belyĭ, il existe $\beta: X \to \Sigma$ une fonction de Belyĭ réalisant un revêtement galoisien, et se factorisant à la fois par β_1 et β_2 ; par conséquent, $\bar{\mathbb{Q}}(X_1)$ et $\bar{\mathbb{Q}}(X_2)$ se plongent tous deux dans le corps $\bar{\mathbb{Q}}(X)$. On peut donc considérer l'union (ou plus précisément la limite inductive, cf. [Bou]) des corps $\mathbb{Q}(X)$ avec $\beta: X \to \Sigma$ fonction de Belyĭ réalisant un revêtement galoisien. Soit $\mathbf{F}$ le groupe de Galois de $M/\bar{\mathbb{Q}}(t)$. On peut vérifier que $\mathbf{F}$ est la limite projective des $\mathfrak{F}/H$ avec H distingué d'indice fini dans $\mathfrak{F}$: cela signifie qu'un élément de $\mathbf{F}$ est une famille $(x_H)_H$ avec $x_H \in \mathfrak{F}/H$ pour tout H, vérifiant de plus $\varpi(x_H) = x_{H'}$ si $H \leq H'$, avec $\varpi: \mathfrak{F}/H \to \mathfrak{F}/H'$ la surjection canonique. On dit que $\mathbf{F}$ est le complété profini de $\mathfrak{F}$.

La tour de corps $\mathbb{Q}(t) \subseteq \bar{\mathbb{Q}}(t) \subseteq M$ donne lieu à la suite exacte de groupes de Galois

$$1 \to \mathbf{F} \to \mathrm{Gal}(M/\mathbb{Q}(t)) \to \mathbf{G} \to 1$$

où $\mathbf{G}$ est le groupe de Galois de $\bar{\mathbb{Q}}(t)/\mathbb{Q}(t)$, autrement dit celui de $\bar{\mathbb{Q}}/\mathbb{Q}$. La conjugaison par un élément de $\mathbf{G}$ définit alors un morphisme $\mathbf{G} \to \mathrm{Aut}\,\mathbf{F}/\,\mathrm{Int}\,\mathbf{F}$. En fait, on peut dire plus : il est prouvé dans [Bel] que cette suite exacte se scinde, autrement dit que $\mathrm{Gal}(M/\mathbb{Q}(t))$ est un produit semi-direct de $\mathbf{F}$ par $\mathbf{G}$, et donc que l'on a un morphisme $\mathbf{G} \to \mathrm{Aut}\,\mathbf{F}$.

Théorème ([Bel], [Jon]). *Cette action de* $\mathbf{G}$ *sur* $\mathbf{F}$ *est fidèle.*

> :-(Soit $\sigma \in \mathbf{G}$ différent de l'identité. Alors il existe $j \in \bar{\mathbb{Q}}$ tel que $j^\sigma \neq j$. Considérons la courbe elliptique X d'invariant j. D'après le théorème de Belyĭ, il existe une fonction de Belyĭ $\beta: X \to \Sigma$. Puisque les courbes elliptiques X et X^σ ne sont pas isomorphes (elles n'ont pas le même invariant), les revêtements β et β^σ ne le sont pas non plus, donc les sous-groupes de $\mathfrak{F}$ qui leur sont associés, disons H et H^σ, ne sont pas égaux dans $\mathfrak{F}$. Or H et H^σ sont d'indice fini, donc correspondent à des sous-groupes, également notés H et H^σ, de $\mathbf{F}$, qui ne sont toujours pas conjugués (vérification aisée). Mais l'action de σ sur $\mathbf{F}$ envoie H sur H^σ, donc n'est pas l'identité. :-)

On en déduit que $\mathbf{G}$ peut se voir comme un sous-groupe de $\mathrm{Aut}\,\mathbf{F}$. On peut alors chercher à caractériser plus précisément ce sous-groupe. Il est montré ([Sch]) qu'il est contenu dans le groupe dit “de Grothendieck-Teichmüller”. Par ailleurs, on peut utiliser des arguments similaires à ceux présentés ici pour étudier le problème de Galois inverse (à savoir celui de construire une extension galoisienne de $\mathbb{Q}$ ayant pour groupe de Galois un groupe fini donné).

Bibliographie.

[Bel] G. V. Belyĭ, “О расширениях Галуа максимального кругового поля” (“On Galois extensions of a maximal cyclotomic field”), *Известия Академии Наук СССР* 43 (1979) 269–276 (en russe), *Math. USSR-Izvestija* 14 (1980) 247–256 (traduction anglaise).

[Bou] N. Bourbaki, *Théorie des ensembles*.

[Dol] P. Dolbeault, *Analyse complexe*, Maîtrise de mathématiques pures, Masson.

[Dou] R. Douady & A. Douady, *Algèbre et théories galoisiennes, tome 2*, Nathan.

[Far] H. Farkas & I. Kra, *Riemann Surfaces, 2nd ed.*, Graduate Texts in Mathematics (71), Springer-Verlag.

[God] C. Godbillon, *Éléments de topologie algébrique*, Hermann.

[Gun] R. C. Gunning, *Lectures on Riemann Surfaces*, Princeton Mathematical Notes.

[Hir] Morris W. Hirsch, *Differential Topology*, Graduate Texts in Mathematics (33), Springer-Verlag.

[Jon] Gareth Jones & David Singerman, “Belyĭ functions, hypermaps and Galois groups”, *Bulletin of the London Mathematical Society*, 28 (1996) 561–590.

[Sch] L. Schneps, *The Grothendieck Theory of Dessins d’Enfants*, London Mathematical Society Lecture Notes (200).

[Sil] Joseph Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics (106), Springer-Verlag.