Construction d'une extension régulière de $\mathbb{Q}(T)$ de groupe de Galois M_{24}

Louis Granboulan

TABLE DES MATIÈRES

Matzat a prouvé que le groupe de Mathieu de degré 24 est groupe de Galois sur l'extension transcendante $\mathbb{Q}(T)$. Il utilise pour cela une construction dite *non rigide* et prouve l'existence d'un point rationnel dans un espace de Hurwitz adéquat. Nous donnons ici une telle extension explicitement. Nous en déduisons aussi l'existence d'une extension régulière de $\mathbb{K}(T)$ de groupe de Galois M_{23} pour tout $\mathbb{K}$ tel que l'équation $x^2+y^2+z^2=0$ ait une solution non triviale. Pour obtenir ces résultats, il a fallu remplacer les outils habituels du calcul formel par des constructions numériques et retrouver ensuite les objets algébriques en paramétrisant certaines courbes de genre 0. Cela nous permet d'illustrer la puissance des techniques de calcul de revêtements développées dans [Couveignes 1994; Couveignes et Granboulan 1994].

Matzat has proved that the Mathieu group of degree 24 is a Galois group over the transcendent extension $\mathbb{Q}(T)$. He does this by using a construction called *nonrigid*, proving the existence of a rational point in an appropriate Hurwitz space. Here we perform such a construction explicitly. We also deduce that, for any $\mathbb{K}$ such that the equation $x^2+y^2+z^2=0$ has a nontrivial solution, there is a regular extension of $\mathbb{K}(T)$ with Galois group M_{23}. To achieve this, we had to replace the usual tools of symbolic calculation by numerical constructions, and then to recover the algebraic objects by parametrizing certain curves of genus 0. This allows us to illustrate the power of covering map techniques developed in [Couveignes 1994; Couveignes et Granboulan 1994].

1. INTRODUCTION

Le groupe de Mathieu M_{23} est le seul groupe sporadique simple pour lequel on ignore si la propriété inverse de Galois est satisfaite [Serre 1992]. Quant au groupe M_{24}, Matzat [1989] a prouvé à partir de calculs dûs à F. Häfner l'existence d'une extension

1058-6458/96 $0.50 per page

finie de $\mathbb{Q}(T)$, galoisienne et régulière, de groupe de Galois M_{24} et ramifiée au dessus de 4 points. (T est un paramètre formel transcendant sur $\mathbb{C}$.) Cependant, aucun modèle explicite n'avait été calculé jusqu'à ce jour. Or cette extension contient un corps de genre 0 et de degré 24 correspondant au groupe M_{23} vu comme le stabilisateur d'un point dans M_{24}. Un calcul explicite était nécessaire pour déterminer la classe d'isomorphisme sur $\mathbb{Q}$ de ce sous-corps. On trouve qu'il est associé à la conique d'équation $x^2 + y^2 + z^2 = 0$. On obtient alors une extension régulière de $\mathbb{K}(T)$ et de groupe de Galois M_{23} pour tout corps de nombres $\mathbb{K}$ tel que la conique ci-dessus ait des points $\mathbb{K}$-rationnels.

Dans la section suivante, nous exprimons les résultats de [Malle et Matzat 1993] selon la terminologie développée dans [Fried et Völklein 1991]. Les résultats de nos calculs sont présentés dans la troisième section, la preuve de leur validité est dans la quatrième section.

Conformément à [Todd 1970] nous faisons agir les permutations à droite. Ainsi le produit de $(1,2)$ et de $(2,3)$ est $(1,2)(2,3) = (1,3,2)$. Par souci de simplicité, on identifie $\mathbb{C}$ à un ouvert de $\mathbb{P}_1(\mathbb{C})$.

2. PREUVE D'EXISTENCE

Dans cette section, nous présentons la preuve de Matzat de l'existence d'une extension régulière de $\mathbb{Q}(T)$ de groupe de Galois M_{24}.

On trouve dans [Todd 1970] une définition point trop ineffective du groupe de Mathieu M_{24} comme le sous-groupe de $\mathfrak{S}_{24}$ engendré par les dix permutations suivantes:

$A = (6,17)(8,20)(9,10)(11,15)(12,18)(13,23)(14,21)(22,24)$
$B = (6,12)(8,13)(9,14)(10,21)(11,24)(15,22)(17,18)(20,23)$
$C = (6,22)(8,10)(9,20)(11,18)(12,15)(13,21)(14,23)(17,24)$
$D = (6,10)(8,22)(9,17)(11,23)(12,21)(13,15)(14,18)(20,24)$
$T = (7,19,16)(8,20,17)(9,14,12)(10,11,23)(13,22,21)(15,18,24)$
$G = (5,6)(7,24)(8,20)(9,14)(10,23)(13,21)(15,16)(18,19)$
$H = (4,5)(8,20)(11,23)(12,14)(13,15)(16,19)(18,21)(22,24)$
$I = (3,4)(8,17)(9,12)(10,13)(11,21)(16,19)(18,24)(22,23)$
$J = (2,3)(7,19)(8,10)(9,14)(11,17)(13,21)(18,24)(20,23)$
$K = (1,2)(8,12)(9,17)(11,23)(14,20)(16,19)(18,24)(21,22)$

Matzat et Malle remarquent que les classes $12B$ et $2A$ (selon les notations de l'Atlas des groupes finis [Conway et al. 1985, pp. 94–96]) sont rationnelles et que le quadruplet $(12B, 2A, 2A, 2A)$ est non-rigide. Nous étudierons la famille de classes de conjugaison $(12B, 2A, 2A, 2A)$.

Suivant les notations de [Serre 1992, p. 70], qui sont proches de celles de [Matzat 1993], on note $\bar{\Sigma}$ l'ensemble des quadruplets $(\sigma_a, \sigma_b, \sigma_c, \sigma_d) \in (12B, 2A, 2A, 2A)$ tels que $\sigma_a\sigma_b\sigma_c\sigma_d = 1$. On note Σ l'ensemble des $(\sigma_a, \sigma_b, \sigma_c, \sigma_d) \in \bar{\Sigma}$ tels que $\sigma_a, \sigma_b, \sigma_c, \sigma_d$ engendrent le groupe M_{24}.

Selon la formule dans [Serre 1992], on trouve:

$$|\bar{\Sigma}| = \frac{|M_{24}|^3}{|Z(12B)|\,|Z(2A)|^3} \sum_{\chi} \frac{\chi(12B)\chi(2A)^3}{\chi(1)^2}$$

Le tableau 1, extrait de l'Atlas, nous donne donc $|\bar{\Sigma}| = 180\,|M_{24}|$.

M_{24} n'a pas de centre, l'action de $\mathrm{Inn}(M_{24})$ sur Σ est donc libre et on peut définir une relation d'équivalence sur les quadruplets de Σ et sur ceux de $\bar{\Sigma}$. On a donc $|\bar{\Sigma}/\mathrm{Inn}(M_{24})| = 180$. Par ailleurs Matzat et Malle montrent que $|\Sigma/\mathrm{Inn}(M_{24})| = 144$. Le groupe de tresses à quatre brins de Hurwitz H_4 agit transitivement sur ces 144 classes de quadruplets.

Comme M_{24} n'a pas de centre, on en déduit, en appliquant par exemple des résultats de Fried [Debès et Fried 1994, § 4, théorème 4.3] l'existence d'une famille de revêtements (famille de Hurwitz)

$$\mathcal{F} : \mathcal{T} \to \mathcal{H} \times \mathbb{P}_1(\mathbb{C})$$

avec les définitions et propriétés suivantes:

- $\mathcal{F}$ est un morphisme fini de variétés quasi-projectives, définies sur $\mathbb{Q}$.
- $\mathcal{H}$ est irréductible et la fibre générique $\mathcal{F}^{-1}(h \times \mathbb{P}_1(\mathbb{C}))$ est irréductible. La restriction de $\mathcal{F}$ à cette fibre est un revêtement galoisien de $\mathbb{P}_1(\mathbb{C})$ de groupe de Galois M_{24}. On note ce revêtement $\mathcal{R}_h$.
- Soit $\mathcal{S} = \mathbb{P}_1(\mathbb{C})^4 - \mathcal{D}$, où $\mathcal{D}$ est la variété discriminant. Il existe un morphisme Ψ de $\mathcal{H}$ dans $\mathcal{S}$, de degré 144, tel que pour h un point de $\mathcal{H}$, le revêtement $\mathcal{R}_h$ est ramifié au dessus de

classe	ordre de $Z(\cdot)$	χ_1	χ_2	χ_3	χ_4	χ_8	χ_{10}	χ_{11}	χ_{12}	χ_{13}	χ_{15}	χ_{16}	χ_{18}
$1A$	244823040	1	23	45	45	253	770	770	990	990	1035	1035	1771
$2A$	21504	1	7	-3	-3	13	-14	-14	-18	-18	-21	-21	-21
$12B$	12	1	-1	1	1	1	1	1	1	1	-1	-1	-1

TABLEAU 1. Table partielle de caractères.

$\Psi(h) = (a, b, c, d)$. La ramification en a est dans la classe $12B$. Celles en b, c, d sont dans la classe $2A$.

- Un point h de $\mathcal{H}$ est défini sur un corps de nombres $\mathbb{K}$ si et seulement si le revêtement associé $\mathcal{R}_h$ ainsi que tous ses automorphismes peuvent être définis sur $\mathbb{K}$.
- La variété $\mathcal{H}$ est birationnellement équivalente à $\mathcal{C} \times \mathbb{P}_1(\mathbb{C}) \times \mathbb{P}_1(\mathbb{C}) \times \mathbb{P}_1(\mathbb{C})$, où $\mathcal{C}$ est obtenue par restriction du revêtement Ψ à la sous-variété $\mathcal{D}$ de dimension 1 de $\mathcal{S}$ formée de l'adhérence des points de la forme $(\infty, -1, 1, \lambda)$ avec $\lambda \in \mathbb{C}$.

Dans le cas qui nous intéresse, le genre de $\mathcal{C}$ est 1. On le calcule grâce à la formule de Hurwitz en regardant l'action du groupe de tresses sur les 144 classes de quadruplets. Il est malaisé de prouver l'existence de points rationnels sur une courbe de genre 1, surtout quand on ne connaît ni son j-invariant ni sa classe d'isomorphismes !

Malle et Matzat [1993, théorème 6.8] remarquent que l'action naturelle de la permutation des second et troisième termes du quadruplet se relève en une action sur $\mathcal{H}$. Si l'on appelle σ l'application de $\mathcal{S}$ dans $\mathcal{S}$ définie par

$$\sigma(a, b, c, d) = (a, c, b, d),$$

il existe un automorphisme de $\mathcal{H}$, défini sur $\mathbb{Q}$, tel que le diagramme suivant commute:

$$\begin{array}{ccc} \mathcal{H} & \xrightarrow{\Sigma} & \mathcal{H} \\ {\scriptstyle\Psi}\downarrow & & \downarrow{\scriptstyle\Psi} \\ \mathcal{S} & \xrightarrow{\sigma} & \mathcal{S} \end{array}$$

On considère alors la variété $\mathcal{H}^{(2,3)} = \mathcal{H}/\Sigma$ que l'on appelle espace de Hurwitz symétrisé en $(2, 3)$ et de même on note $\mathcal{S}^{(2,3)} = \mathcal{S}/\sigma$. Un point de $\mathcal{S}^{(2,3)}$ se note $(a, \{b, c\}, d)$ avec $(a, b, c, d) \in \mathbb{P}_1(\mathbb{C})^4$. On obtient alors un revêtement

$$\Psi^{(2,3)} : \mathcal{H}^{(2,3)} \to \mathcal{S}^{(2,3)}.$$

La restriction de ce revêtement à la sous-variété $\mathcal{D}^{(2,3)}$ de $\mathcal{S}^{(2,3)}$ formée de l'adhérence des points de la forme $(\infty, \{-1, 1\}, \lambda)$ donne un revêtement de $\mathcal{D}^{(2,3)}$ par une courbe $\mathcal{C}^{(2,3)}$, ramifié au dessus de trois points. La courbe $\mathcal{D}^{(2,3)}$ est isomorphe à $\mathbb{P}_1$ sur $\mathbb{Q}$. La courbe $\mathcal{C}^{(2,3)}$ est un quotient de degré 2 de $\mathcal{C}$. La monodromie de $\Psi^{(2,3)}$ est donnée par l'action de H_4 sur les quadruplets et on peut à nouveau calculer le genre de $\mathcal{C}^{(2,3)}$ par la formule de Hurwitz. Cette fois, le genre est 0 et on trouve même un diviseur rationnel de degré impair parmi les points de ramifications, ce qui prouve que $\mathcal{C}^{(2,3)}$ est elle aussi isomorphe sur $\mathbb{Q}$ à la droite $\mathbb{P}_1$ et en particulier qu'elle a une infinité de points rationnels. Ces points correspondent à des revêtements galoisiens de $\mathbb{P}_1$, de groupe de Galois M_{24}, définis sur $\mathbb{Q}$ ainsi que tous leurs automorphismes et ramifiés au dessus de quadruplets de la forme (a, b, c, d) avec a et d dans $\mathbb{P}_1(\mathbb{Q})$ et la paire $\{b, c\}$ définie sur $\mathbb{Q}$ (i.e., stable par action de $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$).

3. DESCRIPTION D'UN REVÊTEMENT

Dans cette section, nous nous attachons à obtenir une description explicite d'un revêtement $\mathcal{R}_h$ qui nous mènera à une extension explicite de $\mathbb{Q}(T)$ de groupe de Galois M_{24}.

Si $\mathcal{R}_h$ est un revêtement de la famille décrite plus haut, alors on peut le quotienter par le stabilisateur d'un point dans M_{24}. On obtient alors un revêtement de genre

$$\tfrac{1}{2}(2-2\cdot 24+2(12-1)+8(2-1)+8(2-1)+8(2-1)) = 0$$

et sans automorphismes car le centralisateur de M_{24} dans $\mathfrak{S}_{24}$ est trivial. En fait, M_{24} est autonormalisateur et n'a pas de centre.

Conformément à une gymnastique qui est désormais classique [Fried 1977; Matzat 1987], il nous suffit d'étudier ce revêtement de degré 24. On a en effet:

Théorème 3.1. *Soit $\{r_1, \ldots, r_n\}$ un ensemble fini et rationnel de points de $\mathbb{P}_1(\mathbb{C})$. Si un revêtement χ de $\mathbb{P}_1(\mathbb{C}) - \{r_1, \ldots, r_n\}$, fini de degré d, connexe, sans automorphismes, admet un modèle défini sur $\mathbb{Q}$, et si le groupe de Galois G de ce revêtement est autonormalisateur dans $\mathfrak{S}_d$, alors sa clôture galoisienne admet un modèle défini sur $\mathbb{Q}$ ainsi que tous ses automorphismes.*

Démonstration. Appelons $\mathbb{M}$ l'extension maximale de $\mathbb{Q}(T)$ non ramifiée en dehors de $\{r_1, \ldots, r_n\}$ et soit $\mathbb{K} \subset \mathbb{M}$ une extension géométrique de $\mathbb{Q}(T)$ (non galoisienne) associée à un modèle rationnel du revêtement χ. On note $\mathbb{L}$ la clôture galoisienne de $\mathbb{K}$ dans $\mathbb{M}$. On appelle G le groupe de Galois géométrique de $\mathbb{L} \otimes \bar{\mathbb{Q}}/\bar{\mathbb{Q}}(T)$ et H le stabilisateur de $\mathbb{K} \otimes \bar{\mathbb{Q}}$ dans G. Puisque le revêtement χ n'a pas d'automorphismes, le normalisateur de H dans G est H. Puisque $\mathbb{K}$ est défini sur $\mathbb{Q}$, tout élément σ de $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ stabilise $\mathbb{K}$ et donc l'automorphisme de G induit par σ stabilise H. En appliquant le lemme 3.2 qui suit, on en déduit que l'action de $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ sur G est intérieure et l'on peut alors invoquer la descente de Weil. □

Lemme 3.2 (du stabilisateur stabilisé). Soit G est un groupe de permutations transitif de degré d et H le stabilisateur d'un point. Si H est égal à son normalisateur dans G, alors tout automorphisme de G qui stabilise H provient de l'action de $\mathfrak{S}_d$ sur G par conjugaison.

Démonstration. Soit σ un automorphisme de G qui stabilise H. Appelons H_i le stabilisateur de i pour tout $i \in \{1, 2, \ldots, d\}$. On a par exemple $H_1 = H$ et tous les H_i sont conjugués. Ainsi, σ induit une permutation des H_i que l'on représente par $\Sigma \in \mathfrak{S}_d$ telle que ${}^{\sigma}H_i = H_{\Sigma(i)}$. Pour toute permutation p de G et pour tout couple $(i, j) \in \{1, 2, \ldots, d\}^2$ les conditions $p(i) = j$ et ${}^{p}H_j = H_i$ sont équivalentes. En faisant agir σ sur cette dernière identité on trouve que $\sigma(p) = {}^{\Sigma^{-1}}p$. □

Ainsi, il nous suffit d'exhiber un modèle rationnel pour un revêtement de genre 0, de degré 24 et de groupe de Galois M_{24}. Ce revêtement se présentera sous la forme d'une conique définie sur $\mathbb{Q}$ et d'une application rationnelle sur cette conique. On ne se préoccupe pas tout de suite de la classe d'isomorphisme de courbes de genre 0 associée à ce revêtement. On le cherche d'abord sous la forme d'une fonction rationnelle de $\mathbb{P}_1(\mathbb{C})$ dans $\mathbb{P}_1(\mathbb{C})$. On n'attend pas d'une telle fonction qu'elle soit définie sur $\mathbb{Q}$, mais du moins sur une extension au plus quadratique de $\mathbb{Q}$. En effet, toute courbe définie sur $\mathbb{Q}$ de genre 0 est isomorphe à $\mathbb{P}_1(\mathbb{C})$ sur un corps quadratique. Quitte à composer à gauche cette fonction par une homographie rationnelle, on peut supposer qu'elle est ramifiée au dessus de $(a, b, c, d) = (\infty, b, c, 0)$ avec $\{b, c\}$ rationnelle. De même, en composant à droite par une homographie, on peut faire en sorte que les deux points au dessus de ∞ correspondant aux deux cycles de la classe $12B$ soient 0 et ∞. Étant donnés les types des permutations $(\sigma_a, \sigma_b, \sigma_c, \sigma_d)$, la fonction rationnelle recherchée est de la forme $X \mapsto \varphi(X) = N(X)/X^{12}$, où N est un polynôme de degré 24 qui se factorise en $N(X) = P_0(X)^2 Q_0(X)$ avec P_0 et Q_0 polynômes de degré 8. De même, il existe des polynômes P_b, Q_b, P_c, Q_c tous de degré 8 tels que

$$\begin{aligned} N(X) &= P_b(X)^2 Q_b(X) + bX^{12} \\ &= P_c(X)^2 Q_c(X) + cX^{12}. \end{aligned} \tag{3.1}$$

On pourrait essayer de trouver une telle fonction à l'aide d'un système de calcul formel en choisissant comme inconnues les coefficients des P et des Q ainsi que b et c. C'est bien évidemment sans espoir, la solution étant un idéal de dimension 2 et de degré 144 à cause de la grave non rigidité du vecteur $(12B, 2A, 2A, 2A)$.

La méthode que nous utilisons est numérique. On observe d'abord que les points singuliers de l'application Ψ correspondent à des revêtements dégénérés ramifiés au dessus de trois points seulement. Étant donnée la monodromie $(\sigma_a, \sigma_b, \sigma_c, \sigma_d)$ d'un revêtement non dégénéré de la famille, on obtient un revêtement dégénéré en «collant» deux ramifications pour obtenir par exemple le triplet $(\sigma_a,\ \sigma_t\ =\ \sigma_b\sigma_c,\ \sigma_d)$. Cela se justifie visuellement si on observe les dessins correspondants: on trace l'image réciproque d'une courbe passant par les quatre valeurs de ramification d'un revêtement régulier φ. Ce dessin permet de voir la monodromie du revêtement. Lorsqu'on rapproche l'une de l'autre les ramifications au dessus de b et de c, jusqu'à les confondre en t, l'action sur les drapeaux autour de t est $\sigma_b\sigma_c$. L'étude théorique de ce phénomène, dans un cadre plus général, a été faite dans [Matzat 1993].

Il se trouve que certains de ces revêtements «limites» sont si simples qu'on peut les calculer à la main. L'un d'eux correspond au dessin de la figure 1. Il est défini par la fonction rationnelle $X \overset{\varphi}{\mapsto} \tilde{N}(X)/X^{12}$ où

$$\tilde{N}(X) = \tilde{P}_0(X)^2\tilde{Q}_0(X)^2 = \tilde{P}_t(X)^3 + 27X^{12}$$

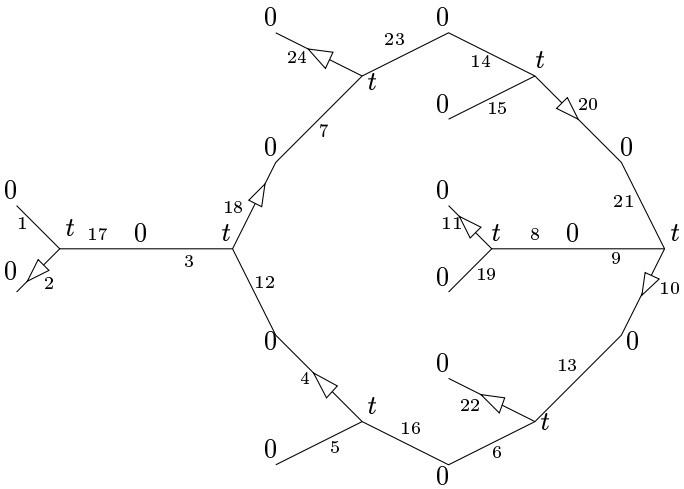


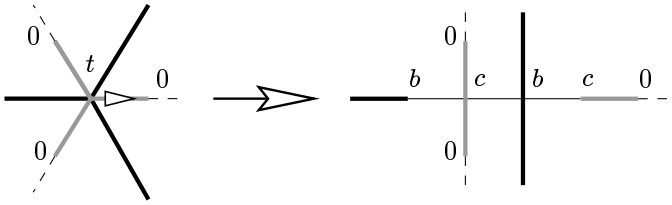
FIGURE 1. Dessin de $\tilde{\varphi}^{-1}([0,t])$ pour un revêtement dégénéré, avec flèches indiquant la direction d'éclatement des singularités.

avec

$$\tilde{P}_0(X) = (X^4+X^3-\tfrac{1}{2}X+\tfrac{1}{4})(X^2+2X-\tfrac{1}{2})(X^2+\tfrac{1}{2}),$$
$$\tilde{Q}_0(X) = X^8+6X^7+11X^6+9X^5+ \\ +\tfrac{15}{2}X^4-\tfrac{9}{2}X^3+\tfrac{11}{4}X^2-\tfrac{3}{4}X+\tfrac{1}{16},$$
$$\tilde{P}_t(X) = X^8+4X^7+4X^6+2X^5+ \\ +\tfrac{1}{2}X^4-X^3+X^2-\tfrac{1}{2}X+\tfrac{1}{16}.$$

Ensuite, on les déforme numériquement pour obtenir, par éclatement des singularités, un revêtement générique correspondant à un point régulier de Ψ. Il est alors très facile de déformer ce dernier revêtement pour obtenir, toujours numériquement, n'importe quel revêtement dans la famille de Hurwitz.

L'éclatement de chaque singularité se fait comme sur la figure ci-dessous:



Les positions des flèches sur la figure 1 se déduisent facilement de l'égalité $\sigma_t = \sigma_b\sigma_c$.

Après avoir obtenu suffisamment de valeurs numériques décrivant des revêtements de la famille de Hurwitz, il est possible, quoique non trivial, de deviner un point rationnel dans $\mathcal{H}$. Pour cela, on cherche une paramétrisation de $\mathcal{H}$ puis on choisit une valeur rationnelle du paramètre. On se déplace alors vers ce point en calculant le revêtement grâce aux techniques de déformation numérique décrites plus haut.

On obtient alors le revêtement défini par les valeurs de b, c, P_0, Q_0, P_bP_c, Q_bQ_c donnés dans la page suivante.

4. PREUVE DE LA VALIDITÉ DES CALCULS

Dans cette section, nous montrons d'abord que le revêtement calculé dans la section précédente et illustré par les figures 2 et 3 ci-après vérifie toutes

$$\left.\begin{aligned} b &= g - h\sqrt{13/23} \\ c &= g + h\sqrt{13/23} \end{aligned}\right\} \quad \text{avec} \quad \left\{\begin{aligned} g &= -23^{12}(23\cdot 176732341\cdot 3160016746668571006373927243119026548599 1)/(2^2 3^3) \\ h &= 23^{12}(2^2 13^2 89^2 1031^3 57768053971^3) \end{aligned}\right.$$

$$\begin{aligned} P_0 = {} & (37914193680139158016 - 302128730888608915440i)x^8 + (-48708956418448918825 6 - 96463506862623248038 4i)x^7 \\ & + (-70551870958592638045 0 - 569348221330342289928i)x^6 + (-66559927859311204282 4 - 29728672020245641880 4i)x^5 \\ & - 16582221192797629108 81/3x^4 + (66559927859311204282 4 - 29728672020245641880 4i)x^3 \\ & + (-70551870958592638045 0 + 569348221330342289928i)x^2 + (48708956418448918825 6 - 96463506862623248038 4i)x \\ & + (37914193680139158016 + 302128730888608915440i) \end{aligned}$$

$$\begin{aligned} Q_0 = {} & (-29505670101849448263 84 + 752382831784862668 80i)x^8 + (-11091625984525246696 96 + 174352595357375209177 6i)x^7 \\ & + (13205816204140551440 00 + 407529948833715416017 2i)x^6 + (48844089604017911222 56 + 203626977484840857321 6i)x^5 \\ & + 84671363110963879416371/12x^4 + (-48844089604017911222 56 + 203626977484840857321 6i)x^3 \\ & + (13205816204140551440 00 - 407529948833715416017 2i)x^2 + (11091625984525246696 96 + 174352595357375209177 6i)x \\ & + (-29505670101849448263 84 - 752382831784862668 80i) \end{aligned}$$

$$\begin{aligned} P_b(x)P_c(x) = {} & (35796772560141751751668622352726694272 0 - 44921440075472002198172388834794283008i)x^{16} \\ & + (22351165834532969560166882870007950704 64 - 24302348646137523722247550444905007413 76i)x^{15} \\ & + (14937709615908958973497742606162600371 2 - 11290702718566151589167319244788699428640i)x^{14} \\ & + (-13820453300845488466791143803490890981600 - 15319753001105493958806923394239564713280i)x^{13} \\ & + (-26933069196708829089178196131144865076500 - 47025465156024351583023945660262899384 32i)x^{12} \\ & + (-21430541752671632771288988599268601728384 + 85029651581117490557382333254122133161 56i)x^{11} \\ & + (-39650399017292766224983103548104264625 08 + 96624494831199626358318822224514640634 35/2i)x^{10} \\ & + (92785366023641983512267612718236303312 1/2 + 43377603452203253664655247644824784473 27i)x^9 \\ & - 69326366502826336942233805196756761980 0x^8 \\ & + (-92785366023641983512267612718236303312 1/2 + 43377603452203253664655247644824784473 27i)x^7 \\ & + (-39650399017292766224983103548104264625 08 - 96624494831199626358318822224514640634 35/2i)x^6 \\ & + (21430541752671632771288988599268601728384 + 85029651581117490557382333254122133161 56i)x^5 \\ & + (-26933069196708829089178196131144865076500 + 47025465156024351583023945660262899384 32i)x^4 \\ & + (13820453300845488466791143803490890981600 - 15319753001105493958806923394239564713280i)x^3 \\ & + (14937709615908958973497742606162600371 2 + 11290702718566151589167319244788699428640i)x^2 \\ & + (-22351165834532969560166882870007950704 64 - 24302348646137523722247550444905007413 76i)x \\ & + (35796772560141751751668622352726694272 0 + 44921440075472002198172388834794283008i) \end{aligned}$$

$$\begin{aligned} Q_b(x)Q_c(x) = {} & (59341251103458113229452133168020973632782338 56 + 15131782597278736393254149361761570751816499 20i)x^{16} \\ & + (53824266652704740199580656828392346960907632640 - 20393864042342649773092277830169236135290657280i)x^{15} \\ & + (12060922842272854938124168032423999313044809856 0 - 16543617762030762859648333683721393352261807596 8i)x^{14} \\ & + (46950446994958343639037816131819832827931760512 - 40285872529613329119419375981446295911021719820 8i)x^{13} \\ & + (-21349696414216600235686894940420039950380986474 0 - 62533245117790120250561515829513461622937841472 0i)x^{12} \\ & + (-52421492204212746817524777154822836561487571467 2 - 65364562273549618758354719336493034542312426328 8i)x^{11} \\ & + (-35013525118502317667738747920755554229463480022 0 - 43175136075086196666063540572673410161888008702 4i)x^{10} \\ & + (-32426941901394375960326867935156652748817931600 - 92013835848019006794292775487125636393072852760i)x^9 \\ & + 23490373219663310601067350678048115043180905688 0x^8 \\ & + (32426941901394375960326867935156652748817931600 - 92013835848019006794292775487125636393072852760i)x^7 \\ & + (-35013525118502317667738747920755554229463480022 0 + 43175136075086196666063540572673410161888008702 4i)x^6 \\ & + (52421492204212746817524777154822836561487571467 2 - 65364562273549618758354719336493034542312426328 8i)x^5 \\ & + (-21349696414216600235686894940420039950380986474 0 + 62533245117790120250561515829513461622937841472 0i)x^4 \\ & + (-46950446994958343639037816131819832827931760512 - 40285872529613329119419375981446295911021719820 8i)x^3 \\ & + (12060922842272854938124168032423999313044809856 0 + 16543617762030762859648333683721393352261807596 8i)x^2 \\ & + (-53824266652704740199580656828392346960907632640 - 20393864042342649773092277830169236135290657280i)x \\ & + (59341251103458113229452133168020973632782338 56 - 15131782597278736393254149361761570751816499 20i) \end{aligned}$$

Valeurs de b, c, P_0, Q_0, P_bP_c, Q_bQ_c qui définissent le revêtement cerché.

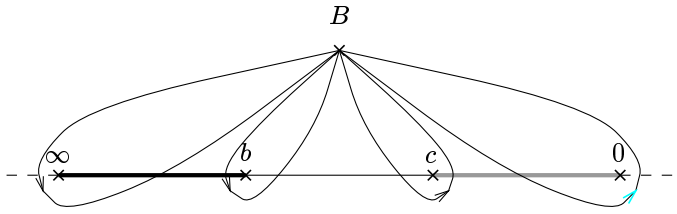
les propriétés demandées. Ce doit être un revêtement non ramifié hors de $\{\infty, b, c, 0\}$, de groupe de Galois M_{24} et de type $(12B, 2A, 2A, 2A)$. Nous réglons ensuite les problèmes liés à la descente sur $\mathbb{Q}$.

Les valeurs calculées pour P_0, Q_0, P_b, Q_b, P_c, Q_c vérifient la formule (3.1). On remarque que d'après (3.1) et la formule de Hurwitz, l'application φ ne peut être ramifiée en dehors de $\{\infty, b, c, 0\}$.

Pour calculer la monodromie de φ on choisit la base du groupe fondamental

$$\pi_1(B, \mathbb{P}_1(\mathbb{C}) - \{\infty, b, c, 0\})$$

représentée ci-dessous, où B est un point du demi-plan supérieur.



L'image réciproque de $\mathbb{R}$ par $\varphi(x) = {P_0}^2 Q_0 / x^{12}$ est le graphe des figures 2 et 3, tracé sur la sphère. Les traits noirs gras figurent les composantes connexes de la préimage du segment (∞, b). De même, on utilise des lignes minces pour le segment (b, c), des lignes grises pour le segment $(c, 0)$ et des lignes pointillées pour le segment $(0, \infty)$. Les composantes connexes de la préimage du demi-plan supérieur (drapeaux) sont marquées d'un nombre entre 1 et 24. La monodromie se calcule en chaque point de ramification en tournant dans le sens positif.

On trouve que la monodromie – en tant qu'action sur les drapeaux – est donnée par les quatre permutations données sur le tableau 2.

Proposition 4.1. $\sigma_\infty, \sigma_b, \sigma_c, \sigma_0$ sont éléments de M_{24}. Ces permutations engendrent le groupe.

Démonstration. Il s'agit d'exprimer ces permutations en fonction des générateurs exhibés dans [Todd 1970] et rappelés dans la section 2 ci-dessus. On construit une famille fortement génératrice (*strong generating set*) de M_{24} en utilisant l'algorithme de Sims Schreier avec Magma, ce qui nous donne l'ensemble $\{A, B, C, D, T, G, H, I, J, K, l, m, n, o, p, q\}$ où:

$$\begin{aligned} l &= m^H, \\ m &= n^I, \\ n &= (o^J T)^{-1}, \\ o &= p^K, \\ p &= T(CA)^{GHIJK}, \\ q &= K^{JIHGDW} \text{ avec } W = BJ^{IHGD(CG)^{T^{-1}}}. \end{aligned}$$

On exprime en fonction des éléments de la base ci-dessus les quatre permutations engendrant la monodromie, ce qui nous prouve que $\sigma_\infty, \sigma_b, \sigma_c, \sigma_0 \in M_{24}$:

$$\begin{aligned} \sigma_\infty &= Do^{-1}qTo^{-1}ql^{-1}m^{-1}n^{-1}o^{-1}p^{-1}, \\ \sigma_b &= mK, \\ \sigma_c &= DCBqT^{-1}Iql^{-1}Io^{-1}qn^{-1}o^{-1}qop, \\ \sigma_0 &= GCBT^{-1}nqlnqm^{-1}nqno^{-1}p. \end{aligned}$$

De façon similaire, on exprime $A, B, C, D, T, G, H, I, J, K$ en fonction de $\sigma_\infty, \sigma_b, \sigma_c, \sigma_0$. □

Proposition 4.2. On a $\sigma_\infty \in 12B$ et $\sigma_b, \sigma_c, \sigma_0 \in 2A$.

Démonstration. Nous remarquons que l'ordre d'une permutation détermine l'ordre de la classe de conjugaison. Il y a deux classes d'ordre 2 et deux classes d'ordre 12, qui peuvent être différenciées à l'aide de leur décomposition en cycles:

$$(1)^8(2)^8 \text{ pour } 2A, \qquad (2)^{12} \text{ pour } 2B,$$
$$(2)(4)(6)(12) \text{ pour } 12A, \qquad (12)^2 \text{ pour } 12B. \quad \square$$

$$\begin{aligned} \sigma_\infty &= (1,17,18,24,23,20,10,6,5,4,3,2)(7,12,16,22,13,9,19,11,8,21,15,14) \\ \sigma_b &= (1,2)(4,16)(8,11)(9,10)(12,18)(13,22)(15,20)(23,24) \\ \sigma_c &= (1,17)(3,12)(5,16)(6,13)(7,23)(8,19)(9,21)(14,15) \\ \sigma_0 &= (3,17)(4,12)(6,16)(7,18)(8,9)(10,13)(14,23)(20,21) \end{aligned}$$

TABLEAU 2. Monodromie des courbes de la figure ci-après.

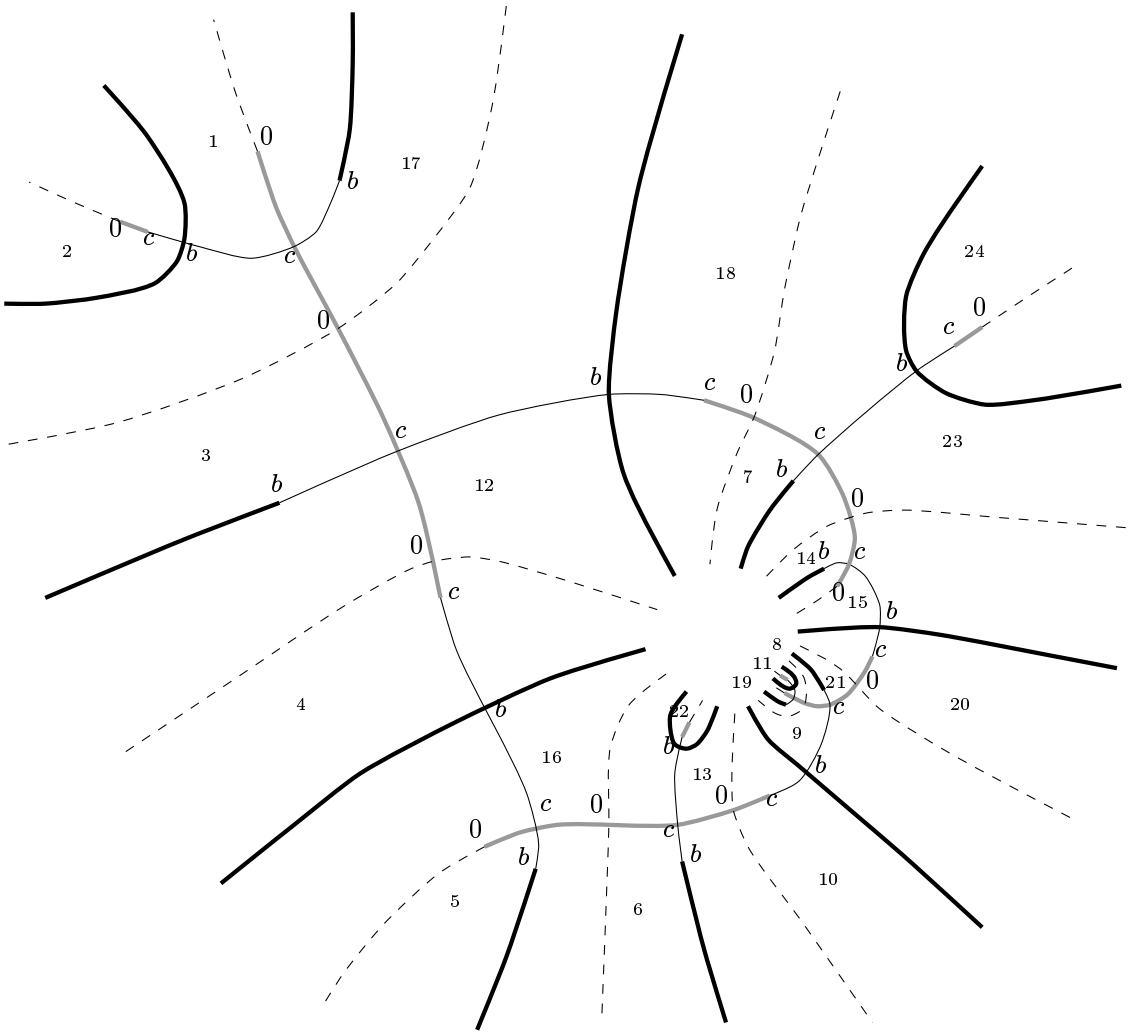


FIGURE 2. Préimage $\varphi^{-1}(\mathbb{R})$ de $\mathbb{R}$ par $\varphi(x)$. Lignes noires grasses: composantes connexes de $\varphi^{-1}((\infty, b))$. Lignes minces: $\varphi^{-1}((b, c))$. Lignes grises: $\varphi^{-1}((c, 0))$. Lignes pointillées: $\varphi^{-1}((0, \infty))$.

Les deux propositions ci-dessus nous montrent que pour $\mathbb{L} = \mathbb{C}(x, T)/(\varphi(x) - T)$, l'extension $\mathbb{L}/\mathbb{C}(T)$ est de groupe de Galois géométrique M_{24}.

Remarque. Pour calculer rigoureusement la monodromie d'un revêtement donné par un modèle algébrique (sans recourir à un *dessin*) on peut utiliser les méthodes données par Leila Schneps [1994]. Ces méthodes reposent sur des majorations de la dérivée qui rendent rigoureuse l'idée de *tourner* autour des points de ramification.

Il reste à voir que l'application φ ci-dessus conduit bien à une extension régulière de $\mathbb{Q}(T)$. C'est la descente de Weil. On observe tout d'abord que φ n'est pas définie sur $\mathbb{Q}$ mais que néanmoins la conjuguée $\bar{\varphi}$ de φ définit un revêtement isomorphe. En effet,

$$\bar{\varphi}(x) = \varphi\Big(-\frac{1}{x}\Big).$$

On va donc considérer la courbe $\mathcal{E}$ d'équation

$$\Gamma(u, v) = u^2 + v^2 + 1 = 0$$

et le morphisme $\varphi : \mathcal{E} \to \mathbb{P}_1(\mathbb{C})$ défini par $\varphi(u, v) = \varphi(u + iv)$, défini sur $\mathbb{Q}$ et isomorphe sur $\mathbb{C}$ à φ.

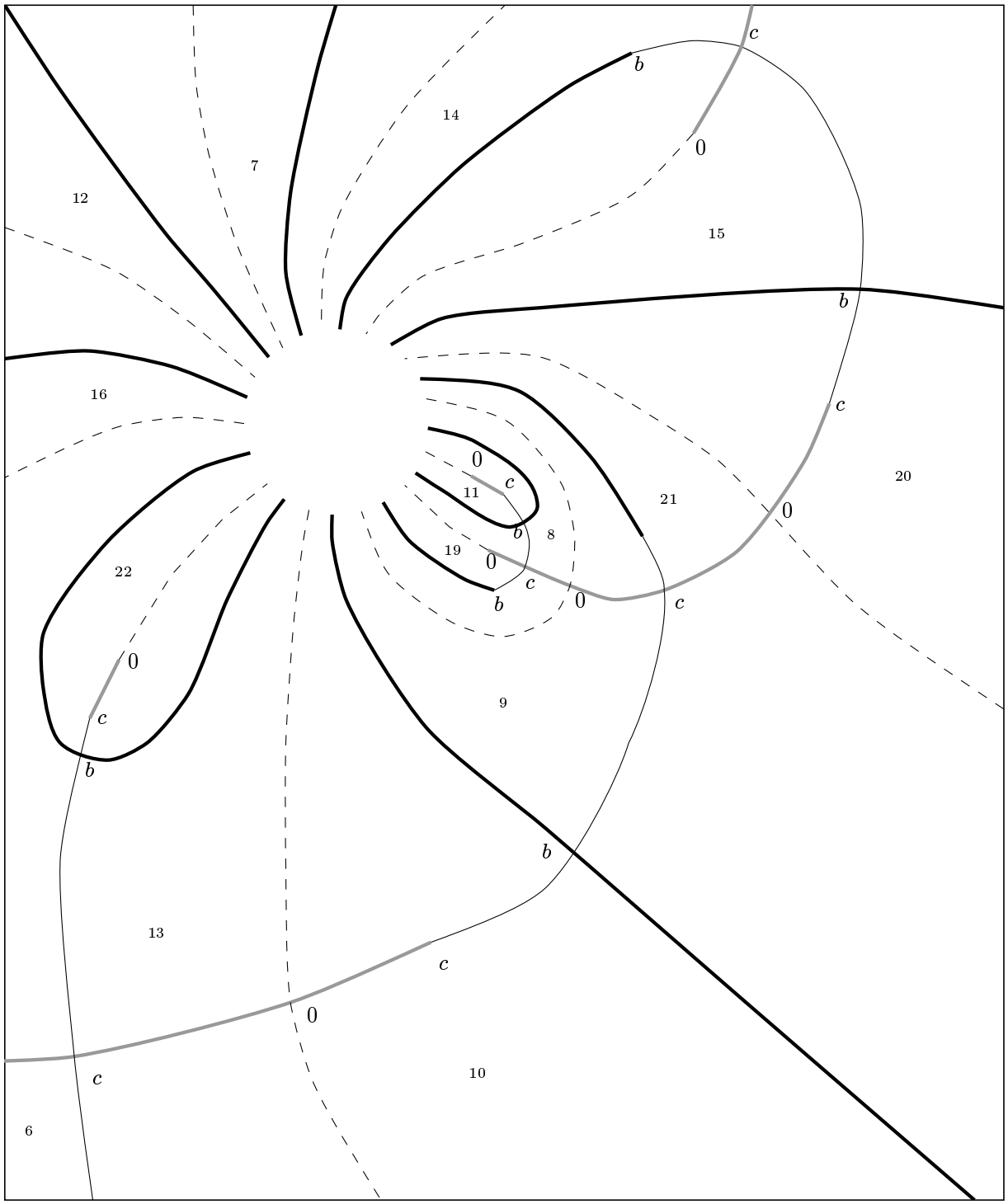


FIGURE 3. Agrandissement de la figure précédente.

Pratiquement, on écrit $x = u + iv$ et on calcule $\varphi(u+iv) \bmod \Gamma$. On pose

$$\begin{aligned}
p_0(u,v) &= \frac{P_0}{x^4}(u+iv) \bmod (u^2+v^2+1)\\
&= (48340596942177426470 40u^3 + 7717080549009859843072u^2 + 469442273243024048 3232u + 252384357765737779 8376)v\\
&\quad + 6066270988822265282 56u^4 - 3896716513475913506048u^3 - 2215447739461478993544u^2 - 4253735942293159215184u\\
&\quad - 5663849214714486245485/3
\end{aligned}$$

et

$$\begin{aligned}
q_0(u,v) &= \frac{Q_0}{x^4}(u+iv) \bmod (u^2+v^2+1)\\
&= (-1203812530855780270080u^3 - 1394820762859001673420 8u^2 - 1690310421877650677572 8u - 7559591456844321329984)v\\
&\quad - 4720907217359117222144u^4 - 8873300787620197357568u^3 + 5614192642971033538 56u^2 + 3113842330088434226336u\\
&\quad + 1092839611748625270391 55/12.
\end{aligned}$$

Notre revêtement est entièrement défini par les huit lignes ci-dessus. Plus précisément, φ est donnée comme l'application de $\mathcal{E}$ dans $\mathbb{P}_1$ définie par

$$\varphi(u,v) = p_0(u,v)^2 q_0(u,v),$$

et elle vérifie $\varphi = p_b(u,v)^2 q_b(u,v) + b = p_c(u,v)^2 q_c(u,v) + c$, avec

$$\begin{aligned}
p_b(u,v)p_c(u,v) &= \frac{P_b P_c}{x^8}(u+iv) \bmod (u^2+v^2+1)\\
&= (1149988865932083256273213154170733645004 8u^7 + 3110700626705603036447686456947840948961 28u^6\\
&\quad + 7398548069772149505508066289790377681080 32u^5 + 8790696743735761862377823557341461894451 20u^4\\
&\quad + 8050331486499481845912543269364648772915 2u^3 + 4163016242630979764322485369939958821755 20u^2\\
&\quad + 1545026488225809270999339812421281330523 94u + 9818524724774343817655840697670747382346)v\\
&\quad + 9163973775396288448427167322298033733632 0u^8 + 2860949226820220103701361007361017690193 92u^7\\
&\quad + 1928396096621075027115819017139047389102 08u^6 + 5841160906648288721042157457646958437273 6u^5\\
&\quad - 3020392337236150592069537136676763231972 48u^4 - 4739294087084233417680885727896954051991 04u^3\\
&\quad - 4185017568540404255653172738735959266063 20u^2 - 2345682976959021040762890574853270261666 87u\\
&\quad - 6147479221838346057827202372470036480 4952
\end{aligned}$$

et

$$\begin{aligned}
q_b(u,v)q_c(u,v) &= \frac{Q_b Q_c}{x^8}(u+iv) \bmod (u^2+v^2+1)\\
&= (-3873736344903356516673062236610962112465023795 20u^7 + 2610414597419859170955811562261662225317204131840u^6\\
&\quad + 1000685491596418475267397422209004742857780329267 2u^5 + 1615449745625108928190896476688989247317345550745 6u^4\\
&\quad + 2035112606498964768797270970051566047308854751027 2u^3 + 1587667986302361567843745711831467711652415841273 6u^2\\
&\quad + 8690688331714703051616056292335762025379058178752u + 2337824095843982270690252012993376354123409943072)v\\
&\quad + 1519136028248527698673974609101336924999227867136u^8 + 6889506131546206745546324074034220410996176977920u^7\\
&\quad + 1075726267555168255774741675895403341034713404211 2u^6 + 1355905003404452880115527724577812036937126047744u^5\\
&\quad + 1006145453761794432623176638203650410471109445984 0u^4 + 3712616368564244902512564037666909247819919558784u^3\\
&\quad - 9477620073438904202625896334945457729355852177 6u^2 - 2570784167193202525787633008243992313454865689152u\\
&\quad - 6392739913915965306494655631609465521776276082 08.
\end{aligned}$$

En écrivant $T = \varphi(u,v) = A(u) + vB(u) \bmod \Gamma$, on exprime $v = (T - A(u))/B(u)$ dans Γ:

$$u^2 + \left(\frac{T - A(u)}{B(u)}\right)^2 + 1.$$

Cela nous donne le polynôme minimal de u sur $\mathbb{Q}(T)$, $P(u)$ de degré 24 en u et de groupe de Galois géométrique M_{24}:

$$P(u) = (1+u^2)B(u)^2 + (T - A(u))^2.$$

Voyons maintenant ce que nous pouvons en déduire pour M_{23}. Posons $\mathbb{L} = \mathbb{Q}(T)[u]/P(u)$ et $\bar{\mathbb{L}}$ une clôture galoisienne de $\mathbb{L}/\mathbb{Q}(T)$. Le théorème 3.1 nous permet d'affirmer que $\bar{\mathbb{L}}$ est une extension régulière de $\mathbb{Q}(T)$. Le corps de fonctions $\mathbb{L}$ est associé à la courbe $\mathcal{E}$ et $\bar{\mathbb{L}}$ à une courbe $\bar{\mathcal{E}}$. On a la tour d'extensions et la tour de revêtements associée:

$$M_{24}\left\{\begin{array}{ccc} \bar{\mathbb{L}} & & \bar{\mathcal{E}} \\ {\scriptstyle M_{23}}\big| & & \big\downarrow \\ \mathbb{L} & & \mathcal{E} \\ \big| & & {\scriptstyle P}\big\downarrow \\ \mathbb{Q}(T) & & \mathbb{P}_1(\mathbb{C}) \end{array}\right.$$

Le revêtement $\bar{\mathcal{E}} \to \mathcal{E}$ est galoisien de groupe de Galois M_{23}. Il nous permet d'obtenir une extension régulière de $\mathbb{K}(T)$ de groupe de Galois M_{23} pour tout corps de nombre $\mathbb{K}$ tel que la courbe $\mathcal{E}$ de genre 0 ait des points $\mathbb{K}$-rationnels.

REMERCIEMENTS

Nous remercions G. Malle et R. Dentzer pour nous avoir suggéré ce problème. Nous remercions tout particulièrement J.-M. Couveignes pour ses suggestions et son aide dans la rédaction de cet article.

BIBLIOGRAPHIE

[Conway et al. 1985] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker et R. A. Wilson, *Atlas of Finite Groups: Maximal Subgroups and Ordinary Characters for Simple Groups*, Oxford University Press, Oxford, 1985.

[Couveignes 1994] Jean-Marc Couveignes, "Calcul et rationalité de fonctions de Belyĭ en genre 0", *Ann. Inst. Fourier* (Grenoble) **44** (1994), 1–38.

[Couveignes et Granboulan 1994] J.-M. Couveignes et L. Granboulan, "Dessins from a geometric point of view", pp. 79–113 dans *The Grothendieck theory of dessins d'enfants*: voir [Schneps 1994].

[Debès et Fried 1994] P. Debès et M. D. Fried, "Nonrigid construction in Galois theory", *Pacific J. Math.* **163** (1994), 81–122.

[Fried 1977] M. D. Fried, "Fields of definition of function fields and Hurwitz families: Groups as Galois groups", *Comm. Algebra* **5** (1977), 17–82.

[Fried et Völklein 1991] M. D. Fried et H. Völklein, "The inverse Galois problem and rational points on moduli spaces", *Mathematische Annalen* **290** (1991), 771–800.

[Matzat 1987] B. Heinrich Matzat, *Konstruktive Galoistheorie*, Lecture Notes in Math. **1284**, Springer, Berlin, 1987.

[Matzat 1989] B. Heinrich Matzat, "Rationality criteria for Galois extensions", pp. 361–383 in *Galois Groups over* $\mathbb{Q}$ (édité par Y. Ihara et al.), MSRI Publications **16**, Springer, New York, 1989.

[Matzat 1993] B. Heinrich Matzat, "Braids and Decomposition Groups", pp. 179–189 in *Séminaire de Théorie des Nombres, Paris*, 1991–92 (édité by S. David), Progress in Math. **116**, Birkhäuser, Boston, 1993.

[Malle et Matzat 1993] G. Malle et B. Heinrich Matzat, "Action of braids", chapitre 3 dans *Inverse Galois Theory*, preprint, University of Heidelberg, 1993.

[Schneps 1994] Leila Schneps, "Dessins d'enfants on the Riemann sphere", pp. 47–77 dans *The Grothendieck theory of dessins d'enfants*, Luminy, 1993 (édité par Leila Schneps), London Math. Soc. Lecture Notes Ser. **200**, Cambridge University Press, Cambridge, 1994.

[Serre 1992] Jean-Pierre Serre, *Topics in Galois Theory* (notes écrites par Henri Da[r]mon), Research Notes Math. **1**, Jones and Bartlett, Boston, 1992.

[Todd 1970] J. A. Todd, "Abstract definitions for the Mathieu groups", *Quart. J. Math. Oxford* **21** (1970), 421–424.

Louis Granboulan, Laboratoire d'Informatique, URA 1327 CNRS, DMI, École Normale Supérieure
(Louis.Granboulan@ens.fr)

Received November 16, 1994; accepted in revised form November 4, 1995