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

Louis Granboulan *

28 octobre 1994

Résumé

Matzat et Malle ont prouvé que le groupe de Mathieu de degré 24 est groupe de Galois sur $\mathbb{Q}(T)$. Ils utilisent pour cela une construction dite *non rigide* et prouvent 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 [Cou94, CG94a].

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, [Ser92]. Quant au groupe M_{24}, Matzat et Malle ont prouvé dans [MM93] l'existence d'une extension finie de $\mathbb{Q}(T)$, galoisienne et régulière, de groupe de Galois M_{24} et ramifiée au dessus de 4 points. 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 Matzat et Malle selon la terminologie développée dans [FV]. Les résultats de nos calculs sont présentés dans la troisième section, la preuve de leur validité est dans la quatrième section. Les données numériques sont en annexe.

Conformément à [Tod70] 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 $\mathbb{P}_1(\mathbb{C})$. 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.

2 Preuve d'existence

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

*. Laboratoire d'Informatique, URA 1327 CNRS, DMI, École Normale Supérieure

On trouve dans [Tod70] une définition point trop ineffective du groupe de Mathieu M_{24} comme le sous-groupe de $\mathfrak{S}_{24}$ engendré par les dix permutations :

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

Matzat et Malle remarquent que les classes $12B$ et $2A$ (selon les notations de l'Atlas des groupes finis [CCN+85]) 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 [Ser92, p70], 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 donnée par [Ser92], on trouve :

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

Un extrait de l'Atlas nous donne la table de caractères ci-dessous :

|Centralisateur|	244823040	21504	12
Classe	$1A$	$2A$	$12B$
χ_1	1	1	1
χ_2	23	7	-1
χ_3	45	-3	1
χ_4	45	-3	1
χ_8	253	13	1
χ_{10}	770	-14	1
χ_{11}	770	-14	1
χ_{12}	990	-18	1
χ_{13}	990	-18	1
χ_{15}	1035	-21	-1
χ_{16}	1035	-21	-1
χ_{18}	1771	-21	-1

D'où on déduit $|\bar{\Sigma}| = 180\,|M_{24}|$.

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 ([DF] paragraphe 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 $h \in \mathcal{H}$ un point de $\mathcal{H}$, le revêtement $\mathcal{R}_h$ est ramifié au dessus de $\Psi(h) = (a, b, c, d)$. 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!

Matzat et Malle font alors la remarque suivante. Puisque les classes associées à b, c, et d sont les mêmes, l'action naturelle du groupe de permutation $\mathfrak{S}_3$ sur $\mathcal{S}$ (permutations des trois derniers termes du quadruplet) se relève en une action sur $\mathcal{H}$. Par exemple, 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

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

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 $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$).

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 gourpe 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 $(2-2\cdot 24+2(12-1)+8(2-1)+8(2-1)+8(2-1))/2=0$ et sans automorphismes car le centralisateur de M_{24} dans S_{24} est trivial. En fait, M_{24} est autonormalisateur et n'a pas de centre.

Conformement a une gymnastique desormais classique (cf. [Fri77],[Mat87]), il nous suffit d'étudier ce revêtement de degré 24. On a en effet :

Théorème 1 *Soit $\{r_1,...,r_n\}$ un ensemble fini et rationnel de points de $\mathbb{P}_1(\mathbb{C})$. Si un revêtement χ de $\mathbb{P}_1(\mathbb{C})-\{r_1,...,r_n\}$, 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 S_d, alors sa clôture galoisienne admet un modèle défini sur $\mathbb{Q}$ ainsi que tous ses automorphismes.*

Preuve : Appelons $\mathbb{M}$ l'extension maximale de $\mathbb{Q}(T)$ non ramifiée en dehors de $\{r_1,...,r_n\}$ 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 $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ stabilise $\mathbb{K}$ et donc l'automorphisme de G induit par σ stabilise H. En appliquant le lemme 1 qui suit, on en déduit que l'action de $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ sur G est intérieure et l'on peut alors invoquer la descente de Weil.

□

Lemme 1 *(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.*

Preuve : Soit σ un automorphisme de G qui stabilise H. Appelons H_i le stabilisateur de i pour tout $i\in\{1,2,...,d\}$. 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 $(i,j)\in\{1,2,...,d\}^2$ 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 $N(X)=P_0^2(X)Q_0(X)$ 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

$$N(X)=P_b(X)^2Q_b(X)+bX^{12}=P_c(X)^2Q_c(X)+cX^{12}. \tag{1}$$

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 $(\sigma_a\sigma_b, \sigma_c, \sigma_d)$.

Il se trouve que certains de ces revêtements « limites » sont si simples qu'on peut les calculer à la main. 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. À partir d'une telle description, il est possible, quoique non trivial, de deviner un point rationnel dans $\mathcal{H}$. On se déplace alors vers ce point par la technique décrite plus haut. On se réfèrera à [CG94b] pour l'intégralité des calculs.

On obtient d'abord le revêtement défini par les valeurs suivantes de b, c, P_0, Q_0, P_bP_c, Q_bQ_c.

$$b = g - h\sqrt{13/23}, \quad c = g + h\sqrt{13/23}$$

avec

$$g = -23^{12}(23 \cdot 176732341 \cdot 3160016746668571006373927243119026548599 1)/(2^2 3^3)$$
$$h = 23^{12}(2^2 13^2 89^2 1031^3 57768053971^3)$$

$$\begin{aligned}P_0 = {} & (37914193680139158016 - 302128730888608915440i)x^8 \\ & +(-48708956418448918825 6 - 964635068626232480384i)x^7 + (-70551870958592638045 0 \\ & -569348221330342289928i)x^6 + (-665599278593112042824 - 297286720202456418804i)x^5 \\ & -16582221192797629108 81/3x^4 + (665599278593112042824 - 297286720202456418804i)x^3 \\ & +(-70551870958592638045 0 + 569348221330342289928i)x^2 + (48708956418448918825 6 \\ & -964635068626232480384i)x + (37914193680139158016 + 302128730888608915440i)\end{aligned}$$

$$\begin{aligned}Q_0 = {} & (-295056701084944826384 + 752382831784862668 80i)x^8 \\ & +(-110916259845252466969 6 + 174352595357375209177 6i)x^7 + (132058162041405514400 0 \\ & +407529948833715416017 2i)x^6 + (488440896040179112225 6 + 203626977484840857321 6i)x^5 \\ & +846713631109638794163 71/12x^4 + (-488440896040179112225 6 + 203626977484840857321 6i)x^3 \\ & +(132058162041405514400 0 - 407529948833715416017 2i)x^2 + (110916259845252466969 6 \\ & +174352595357375209177 6i)x + (-295056701084944826384 - 752382831784862668 80i)\end{aligned}$$

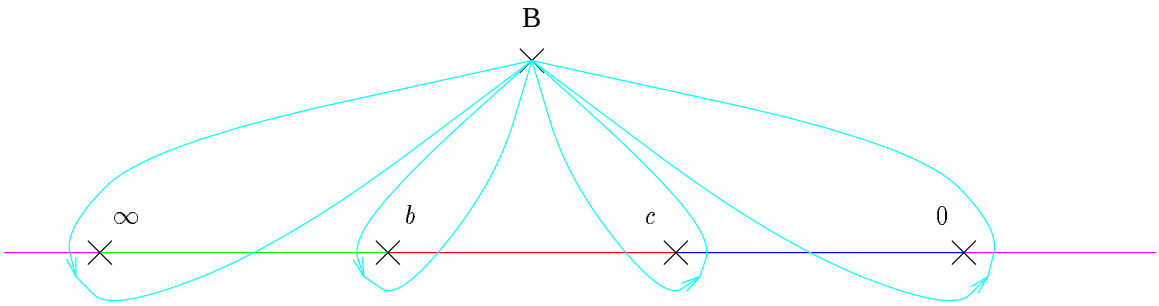
Les valeurs de P_bP_c et Q_bQ_c sont données en annexe.

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 1 et 2 ci-après vérifie toutes 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 (1). On remarque que d'après (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 $\pi_1(\mathrm{B}, \mathbb{P}_1(\mathbb{C}) - \{\infty, b, c, 0\})$ représentée ci-dessous, où B est un point du demi-plan supérieur.



L'image réciproque de $\mathbb{R}$ par $\varphi(x) = \frac{{P_0}^2 Q_0}{x^{12}}$ est le graphe des figures 1 et 2, tracé sur la sphère. Les traits représentés en vert figurent les composantes connexes de la préimage du segment (∞, b). De même, on utilise le rouge pour le segment (b, c) , le bleu pour le segment $(c, 0)$ et le mauve 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 ci-dessous.

- $\sigma_\infty : (1, 17, 18, 24, 23, 20, 10, 6, 5, 4, 3, 2)(7, 12, 16, 22, 13, 9, 19, 11, 8, 21, 15, 14)$
- $\sigma_b : (1, 2)(4, 16)(8, 11)(9, 10)(12, 18)(13, 22)(15, 20)(23, 24)$
- $\sigma_c : (1, 17)(3, 12)(5, 16)(6, 13)(7, 23)(8, 19)(9, 21)(14, 15)$
- $\sigma_0 : (3, 17)(4, 12)(6, 16)(7, 18)(8, 9)(10, 13)(14, 23)(20, 21)$

Proposition 1 *$\sigma_\infty, \sigma_b, \sigma_c, \sigma_0$ sont éléments de M_{24}. Ces permutations engendrent le groupe.*

Preuve : Il s'agit d'exprimer ces permutations en fonction des 10 générateurs exhibés dans [Tod70] et rappelés dans la section 2 ci-dessus. On construit un *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 :

- $l = m^H$
- $m = n^I$
- $n = (o^J T)^{-1}$
- $o = p^K$
- $p = T(CA)^{GHIJK}$
- $q = K^{JIHGDW}$ avec $W = BJ^{IHGD(CG)^{T^{-1}}}$

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

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

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

□

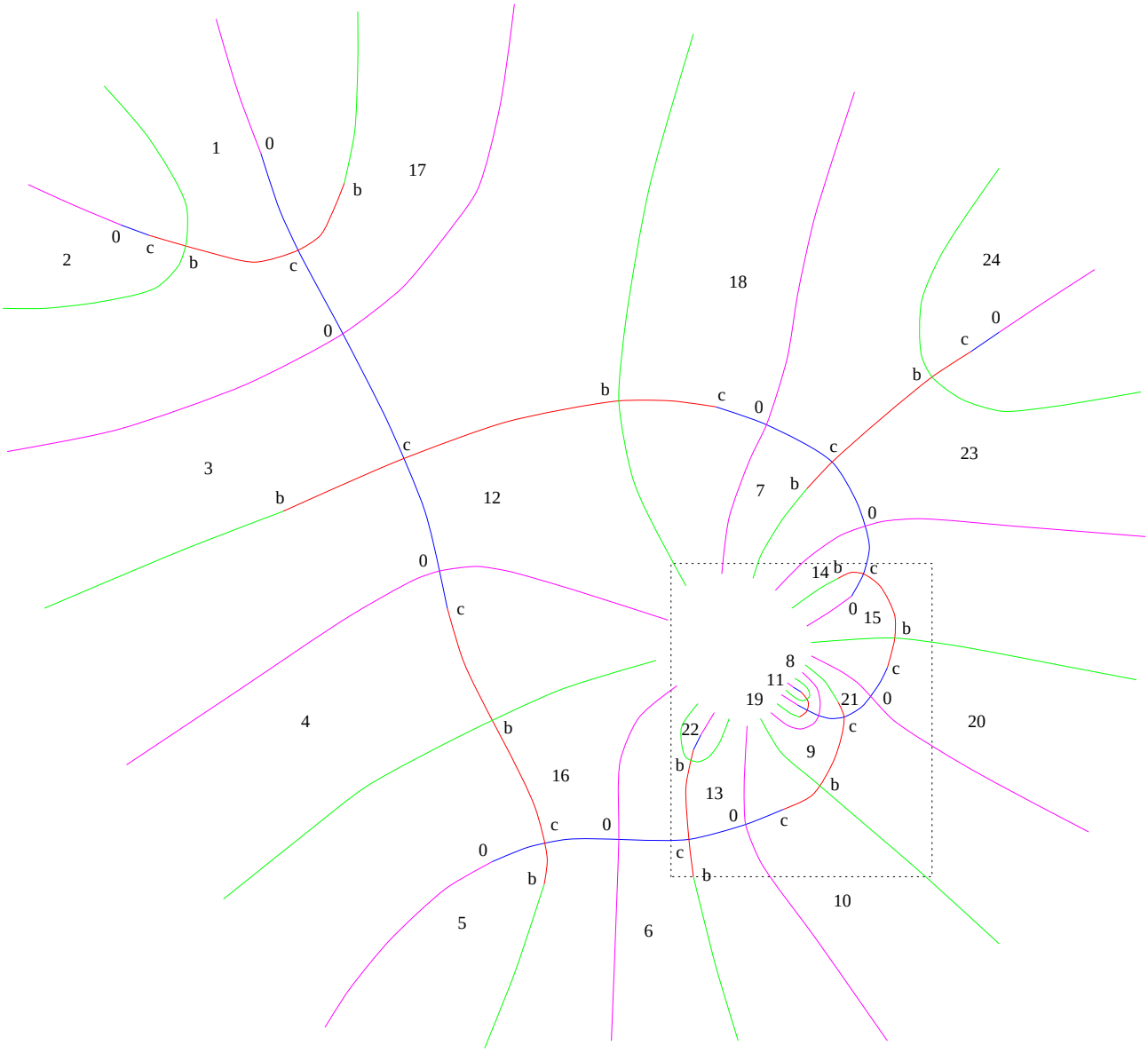


FIG. 1 - $\varphi^{-1}(\mathbb{R})$

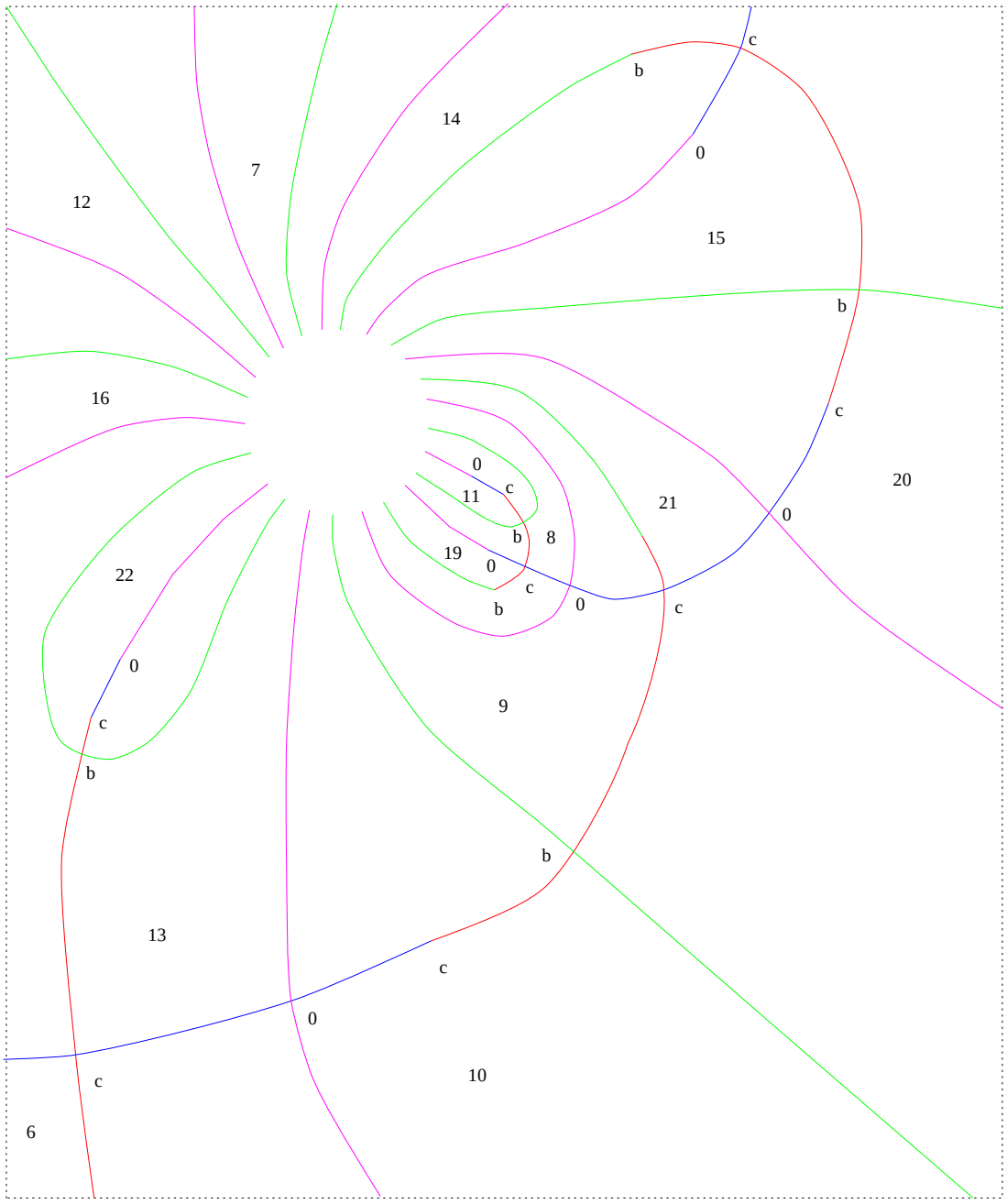


FIG. 2 - *Agrandissement de la figure précédente :* $\varphi^{-1}(\mathbb{R})$

Proposition 2 *$(\sigma_\infty, \sigma_b, \sigma_c, \sigma_0)$ sont éléments des classes de conjugaison $(12B, 2A, 2A, 2A)$.*

PREUVE : Nous remarquons d'abord que l'ordre d'une permutation détermine l'ordre de la classe de conjugaison. Pour distinguer deux classes du même ordre, on regarde l'ordre de leurs stabilisateurs.

On utilise les notations et les données de l'Atlas ([CCN+85]) :

|Centralisateur|	244823040	21504	7680	1080	504	12	12
p power	A	A	A	A	A	AA	BC
Classe	$1A$	$2A$	$2B$	$3A$	$3B$	$12A$	$12B$

On remarque que σ_b, σ_c et σ_0 sont d'ordre 2. On veut prouver que ces permutations sont de type $2A$ et non $2B$. Or le centralisateur d'un élément de la classe $2A$ est d'ordre $21504 = 2^{10}.3.7$ tandis que le centralisateur d'un élément de la classe $2B$ est d'ordre $7680 = 2^{10}.7$. Il suffit donc d'exhiber un élément d'ordre 3 commutant avec σ_b, σ_c ou σ_0.

On remarque que σ_∞ est d'ordre 12. Pour prouver que σ_∞ est de type $12B$ et non $12A$, on ne peut utiliser la même méthode à l'identique : les ordres des centralisateurs des éléments des classes $12A$ et $12B$ sont égaux. En revanche, on peut appliquer cette méthode à une puissance de σ_∞. On a $(12A)^4 = 3A$ et $(12B)^4 = 3B$. Or le centralisateur d'un élément de la classe $3A$ est d'ordre $1080 = 2^3.3^3.5$ tandis que le centralisateur d'un élément de la classe $3B$ est d'ordre $504 = 2^3.3^2.7$. Il suffit donc d'exhiber un élément d'ordre 7 commutant avec $(\sigma_\infty)^4$.

- $(2, 19, 7, 22, 21, 20, 18)(3, 6, 16, 8, 14, 9, 17)(4, 10, 24, 15, 13, 11, 12)$ commute avec $(\sigma_\infty)^4$.
- $(1, 4, 18)(2, 16, 12)(3, 14, 17)(6, 7, 21)(8, 24, 13)(11, 23, 22)$ commute avec σ_b.
- $(2, 11, 24)(3, 5, 8)(7, 9, 14)(10, 22, 18)(12, 16, 19)(15, 23, 21)$ commute avec σ_c.
- $(1, 2, 24)(3, 4, 6)(8, 14, 21)(9, 23, 20)(11, 19, 22)(12, 16, 17)$ commute avec σ_0.

□

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 dans [Sch94]. 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,

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

On va donc considérer la courbe $\mathcal{E}$ d'équation $\Gamma(u, v) = u^2 + v^2 + 1 = 0$ et le morphisme $\phi : \mathcal{E} \to \mathbb{P}_1(\mathbb{C})$ défini par $\phi(u, v) = \varphi(u + iv)$, défini sur $\mathbb{Q}$ et isomorphe sur $\mathbb{C}$ à φ.

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

$$p_0(u, v) = \tfrac{P_0}{x^4}(u + iv) \bmod (u^2 + v^2 + 1) =$$
$$(48340596942177426470 40u^3 + 771708054900985984 3072u^2 + 469442273243024048 3232u$$
$$+252384357765737779 8376)v + (606627098882226528256u^4 - 3896716513475913506048u^3$$
$$-2215447739461478993544u^2 - 4253735942293159215184u - 5663849214714486245485/3)$$

$$q_0(u, v) = \tfrac{Q_0}{x^4}(u + iv) \bmod (u^2 + v^2 + 1) =$$
$$(-1203812530855780270080u^3 - 1394820762859001673 4208u^2 - 1690310421877650677 5728u$$
$$-7559591456844321329984)v + (-4720907217359117222144u^4 - 8873300787620197357568u^3$$
$$+5614192642971033538 56u^2 + 3113842330088434226336u + 1092839611748625270 39155/12)$$

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

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

et elle vérifie

$$\phi = p_b(u,v)^2 q_b(u,v) + b = p_c(u,v)^2 q_c(u,v) + c.$$

Les valeurs de $p_b p_c$ et $q_b q_c$ sont données en annexe.

En écrivant $T = \phi(u,v) = A(u) + vB(u) \bmod \Gamma$, on exprime $v = \frac{T-A(u)}{B(u)}$ 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 cloture galoisienne de $\mathbb{L}/\mathbb{Q}(T)$. Le théorème 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 :

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

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.

Annexe : Données numériques

$$\begin{aligned}
&P_b(x)P_c(x) = \\
&(3579677256014175175166862235272669427 20 - 4492144007547200219817238883479428300 8i)x^{16} \\
&+(2235116583453296956016688287000795070464 - 2430234864613752372224755044490500741376i)x^{15} \\
&+(1493770961590895897349774726061626003712 - 1129070271856615158916731924478869942864 0i)x^{14} \\
&+(-1382045330084548846679114380349089098160 0 - 1531975300110549395880692339423956471328 0i)x^{13} \\
&+(-2693306919670882908917819613114486507650 0 - 4702546515602435158302394566026289938432i)x^{12} \\
&+(-2143054175267163277128898859926860172838 4 + 8502965158111749055738233325412213316156i)x^{11} \\
&+(-3965039901729276622498310354810426462508 + 9662449483119962635831882222451644063435/2i)x^{10} \\
&+(9278536602364198351226761271823630331 21/2 + 4337760345220325366465524764482478447327i)x^{9} \\
&-6932636650282633694223380519675676198 00x^{8} \\
&+(-9278536602364198351226761271823630331 21/2 + 4337760345220325366465524764482478447327i)x^{7} \\
&+(-3965039901729276622498310354810426462508 - 9662449483119962635831882222451644063435/2i)x^{6} \\
&+(2143054175267163277128898859926860172838 4 + 8502965158111749055738233325412213316156i)x^{5} \\
&+(-2693306919670882908917819613114486507650 0 + 4702546515602435158302394566026289938432i)x^{4} \\
&+(1382045330084548846679114380349089098160 0 - 1531975300110549395880692339423956471328 0i)x^{3} \\
&+(1493770961590895897349774726061626003712 + 1129070271856615158916731924478869942864 0i)x^{2} \\
&+(-2235116583453296956016688287000795070464 - 2430234864613752372224755044490500741376i)x \\
&+(3579677256014175175166862235272669427 20 + 4492144007547200219817238883479428300 8i)
\end{aligned}$$

$$Q_b(x)Q_c(x) =$$
$$(59341251103458113229452133168020973632782338 56 + 151317825972787363932541493617615707518164992 0i)x^{16}$$
$$+(53824266652704740199580656828392346960907632640 - 203938640423426497730922778301692361352906572 80i)x^{15}$$
$$+(12060922842272854938124168032423999313044809856 0 - 165436177620307628596483336837213933522618075 968i)x^{14}$$
$$+(46950446994958343639037816131819832827931760512 - 402858725296133291194193759814462959110217198 208i)x^{13}$$
$$+(-21349696414216600235686894940420039950380986474 0 - 625332451177901202505615158295134616229378414 720i)x^{12}$$
$$+(-52421492204212746817524777154822836561487571467 2 - 653645622735496187583547193364930345423124263 288i)x^{11}$$
$$+(-35013525118502317667738747920755554229463480022 0 - 431751360750861966660635405726734101618880087 024i)x^{10}$$
$$+(-32426941901394375796032686793515665274881793160 0 - 920138358480190067942927754871256363930728527 60i)x^{9}$$
$$+2349037321966331060106735067804811504318090568 80x^{8}$$
$$+(32426941901394375796032686793515665274881793160 0 - 920138358480190067942927754871256363930728527 60i)x^{7}$$
$$+(-35013525118502317667738747920755554229463480022 0 + 431751360750861966660635405726734101618880087 024i)x^{6}$$
$$+(52421492204212746817524777154822836561487571467 2 - 653645622735496187583547193364930345423124263 288i)x^{5}$$
$$+(-21349696414216600235686894940420039950380986474 0 + 625332451177901202505615158295134616229378414 720i)x^{4}$$
$$+(-46950446994958343639037816131819832827931760512 - 402858725296133291194193759814462959110217198 208i)x^{3}$$
$$+(12060922842272854938124168032423999313044809856 0 + 165436177620307628596483336837213933522618075 968i)x^{2}$$
$$+(-53824266652704740199580656828392346960907632640 - 203938640423426497730922778301692361352906572 80i)x$$
$$+(59341251103458113229452133168020973632782338 56 - 151317825972787363932541493617615707518164992 0i)$$

$$p_b(u,v)p_c(u,v) = \tfrac{P_bP_c}{x^8}(u+iv) \bmod (u^2+v^2+1) =$$
$$(11499888659320832562732131541707336450048u^{7} + 31107006267056030364476864569478409489612 8u^{6}$$
$$+7398548069772149505508066289790377681080 32u^{5} + 87906967437357618623778235573414618944512 0u^{4}$$
$$+8050331486499481845912543269364648772915 2u^{3} + 41630162426309797643224853699399588217552 0u^{2}$$
$$+1545026488225809270999339812421281330523 94u + 98185247247743438176558406976707473823 46)v$$
$$+(91639737753962884484271673222980337336320u^{8}$$
$$+2860949226820220103701361007361017690193 92u^{7} + 19283960966210750271158190171390473891020 8u^{6}$$
$$+5841160906648288721042157457646958437273 6u^{5} - 30203923372361505920695371366767632319724 8u^{4}$$
$$-4739294087084233417680885727896954051991 04u^{3} - 41850175685404042556531727387359592660632 0u^{2}$$
$$-2345682976959021040762890574853270261666 87u - 61474792218383460578272023724700364804952)$$

$$q_b(u,v)q_c(u,v) = \tfrac{Q_bQ_c}{x^8}(u+iv) \bmod (u^2+v^2+1) =$$
$$(-38737363449033565166730622366109621124650237952 0u^{7} + 26104145974198591709558115622616622253172041318 40u^{6}$$
$$+1000685491596418475267397422209004742857780329267 2u^{5} + 16154497456251089281908964766889892473173455507456u^{4}$$
$$+2035112606498964768797270970051566047308854751027 2u^{3} + 15876679863023615678437457118314677116524158412736u^{2}$$
$$+8690688331714703051616056292335762025379058178752u + 23378240958439822706902520129933763541234094307 2)v$$
$$+(15191360282485276986739746091013369249992278671 36u^{8}$$
$$+6889506131546206745546324074034220410996176977920u^{7} + 10757262675551682557747416758954033410347134042112u^{6}$$
$$+1355905003404452880115527245778120369737126047744u^{5} + 10061454537617944326231766382036504104711094459840u^{4}$$
$$+3712616368564244902512564037666909247819919558784u^{3} - 94776200734389042026258963349454577293558521776u^{2}$$
$$-2570784167193202525787633008243992313454865689152u - 63927399139159653064946556316094655217762760 8)$$

Références

[CCN+85] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker, and R.A. Wilson. *Atlas of finite groups*. Clarendon Press, 1985.

[CG94a] Jean-Marc Couveignes and Louis Granboulan. Dessins from a geometric point of view. In Leila Schneps, editor, *The Grothendieck Theory of Dessins d'Enfants*, volume 200 of *Lecture Notes in Math.* Cambridge University Press, 1994.

[CG94b] Jean-Marc Couveignes and Louis Granboulan. Manuscrit. 1994.

[Cou94] Jean-Marc Couveignes. Calcul et rationalité de fonctions de Belyi en genre 0. *Annales de l'Institut Fourier*, 44(1), janvier 1994.

[DF] P. Debès and M. D. Fried. Nonrigid construction in Galois Theory. *Pacific Journal of Math.* à paraître.

[Fri77] M. D. Fried. Fields of definition of function fields and Hurwitz families – Groups as Galois groups. *Comm. Algebra*, 5:17–82, 1977.

[FV] M. D. Fried and H. Völklein. The inverse Galois problem and rational points on moduli spaces. *Israel J. of Math.* à paraître.

[Mat87] B. H. Matzat. *Konstruktive Galoistheorie.*, volume 1284 of *Lecture Notes in Math.* Springer Verlag, 1987.

[MM93] G. Malle and B. H. Matzat. Action of Braids. In *Inverse Galois Theory*, chapter 3. 1993. Preprint. University of Heidelberg.

[Sch94] Leila Schneps. Dessins d'enfant on the Riemann sphere. In Leila Schneps, editor, *The Grothendieck Theory of Dessins d'Enfants*, volume 200 of *Lecture Notes in Math.* Cambridge University Press, 1994.

[Ser92] J.-P. Serre. *Topics in Galois theory.* Jones and Bartlett, 1992.

[Tod70] J.A. Todd. Abstract definitions for the Mathieu groups. *Quart. J. Math. Oxford*, 21:421–424, 1970.