Factorisations explicites de g(y) - h(z)

Pierrette Cassou-Noguès, Jean-Marc Couveignes

Factorisations explicites de g(y)-h(z)

Pierrette Cassou-Noguès*et Jean-Marc Couveignes†

22 juin 1998

Résumé

Nous donnons toutes les paires de polynômes $(g,h) \in \mathbb{C}[y] \times \mathbb{C}[z]$ non constants, indécomposables et non linéairement reliés tels que $g(y) - h(z)$ se factorise dans $\mathbb{C}[y,z]$. D'après un résultat de Feit et Fried, si la classification des groupes simples finis est correcte, il n'existe qu'un nombre fini de telles paires. Une étude attentive de leurs comportements possibles à l'infini nous a permis de les déterminer toutes explicitement.

1 Introduction

Nous considérons le problème suivant :

Problème 1 . *Soient* $g(y) \in \mathbb{C}[y]$ *et* $h(z) \in \mathbb{C}[z]$. *Quand le polynôme* $g(y) - h(z) \in \mathbb{C}[y,z]$ *est-il réductible?*

Ce problème a été étudié entre autres par Davenport, Lewis, Schinzel puis Cassels, Fried et Feit [14, 13, 8, 18, 19, 20, 21, 22, 23].

Rappelons quelques cas particuliers bien connus

- $(y-z)|(g(y)-g(z))$.
- Si $\pi(y,z)|(g(y)-h(z))$ alors $\pi(Y(y),Z(z))|(g(Y(y))-h(Z(z)))$ avec $Y \in \mathbb{C}[y]$ et $Z \in \mathbb{C}[z]$.
- Si $g(y) = T_4(y) = 8y^4 - 8y^2 + 1$ et $h(z) = -T_4(z)$. Alors $g(y) - h(z) = (\sqrt{2}(2x^2+2y^2-1)+4xy)(\sqrt{2}(2x^2+2y^2-1)-4xy)$.
- Si g et h sont une solution au problème 1 alors pour $(A,B) \in \mathbb{C}^* \times \mathbb{C}$ les polynômes $Ag+B$ et $Ah+B$ forment une solution.

*Laboratoire de Mathématiques Pures, Université Bordeaux I

†Algorithmique Arithmétique Expérimentale, Université Bordeaux I et Délégation Générale pour l'Armement

Mots clefs : Polynômes, Revêtements de la sphère, Configurations, Calcul numérique, Calcul formel

On dit que deux polynômes $g, h \in \mathbb{C}[x]$ sont *linéairement reliés* (l.r. pour simplifier) s'il existe $(a, b) \in \mathbb{C}^* \times \mathbb{C}$ tel que

$$h(x) = g(ax + b).$$

On dit que deux polynômes $g, h \in \mathbb{C}[x]$ sont *faiblement linéairement reliés* (f.l.r. pour simplifier) s'il existe $(a, b), (A, B) \in \mathbb{C}^* \times \mathbb{C}$ tels que

$$h(x) = Ag(ax + b) + B.$$

On dit que deux paires de polynômes $(g_1, g_2), (h_1, h_2) \in \mathbb{C}[x]^2$ sont *faiblement linéairement reliées* (f.l.r. pour simplifier) s'il existe $(a, b), (c, d), (A, B) \in \mathbb{C}^* \times \mathbb{C}$ tels que

$$h_1(x) = Ag_1(ax + b) + B \text{ et } h_2(x) = Ag_2(cx + d) + B.$$

On dit qu'un polynôme $f(x)$ non constant est *décomposable* s'il existe des polynômes $a(x)$ et $b(x)$ de degrés plus grands que 1 tels que $f = a \circ b$. Dans le cas contraire on dit que f est *indécomposable*. Le problème 1 est mal éclairci dans le cas des polynômes décomposables. En revanche, si l'on se restreint aux polynômes indécomposables, et en admettant la classification des groupes simples finis, les solutions au problème 1 sont en nombre fini comme l'ont montré Feit et Fried qui en donnent aussi les groupes de monodromie.

Nous admettons donc l'assertion suivante qui n'est autre que la classification des groupes simples finis.

Assertion 1 . *Les groupes simples finis sont les groupes de Lie, les groupes alternés et les 26 groupes sporadiques.*

Dans cet article nous construisons tous les couples (g, h) non constants et non linéairement reliés, tels que g et h soient indécomposables et $g(y) - h(z)$ réductible. Ceci n'avait été réalisé que pour g et h de degré $n = 7$ et 11, par Birch "apparently by low-brow fiddling" [8]. L'idée est exprimée dans [23] qu'un tel calcul n'est pas envisageable pour les valeurs supérieures de n.

Dans les sections 2.1.1 à 2.2.3 nous rappelons les résultats de Feit et Fried [21, 22, 23, 18, 19, 20] dont nous avons besoin et nous les complétons dans les sections 2.2.4 et 2.2.5 et 3 par une étude plus attentive de leur comportement à l'infini. Nous en déduisons tout naturellement une méthode simple de calcul. Les résultats sont présentés à la section 5. La section 4 est consacrée à leur exploitation combinatoire. L'application de cette méthode donne l'intégralité des solutions au problème considéré. Observons en particulier que le degré des polynômes g et h ne peut prendre que les six valeurs $\{7, 11, 13, 15, 21, 31\}$ comme l'ont montré Feit et Fried mais que de surcroît il existe une *unique* solution pour chacun de ces degrés à action de tresses et de Galois près. Ceci nous permet de les décrire toutes.

Énonçons le résultat principal de cet article

Théorème 1 . *Supposons vraie l'assertion (1). Soit $(g, h) \in \mathbb{C}[y] \times \mathbb{C}[z]$ une paire de polynômes non constants, indécomposables et non linéairement reliés telle que $g(y) - h(z)$ soit réductible. Alors (g, h) est faiblement linéairement reliée à l'une des paires présentées à la fin de cet article.*

Les auteurs remercient Arkadiusz Ploski et Alexandre Zvonkin pour leur avoir parlé de ce problème.

2 Relations avec les configurations cycliques

Dans cette section nous rappelons et nous developpons les méthodes de Cassels, Fried et Feit pour classifier les solutions au problème 1.

Il s'agit d'expliquer le résultat suivant,

Théorème 2 . *Supposons vraie l'assertion (1). Alors si g et h sont deux polynômes non constants, indécomposables et non linéairement reliés, tels que $g(y) - h(z)$ soit réductible dans l'anneau $\mathbb{C}[y, z]$ alors*

$$\deg(g) = \deg(h) \in \{7, 11, 13, 15, 21, 31\}.$$

On veut établir des propriétés du groupe de Galois des polynômes g et h qui soient aussi contraignantes que possible. Nous procédons en plusieurs étapes. Nous aboutirons au théorème (8) qui sert de point de départ à nos calculs.

2.1 Le groupe de Galois et ses deux représentations par permutations

On note $A(y, z)$ un facteur non constant de $g(y) - h(z)$ et $B(y, z)$ son cofacteur. On suppose que $B(y, z)$ est non constant. Soit k le degré total de $A(y, z)$. Soit d_g le degré de g et d_h celui de h. Le degré en z de $A(y, z)$ n'est pas nul sinon $A(y, z)$ ou $h(z)$ serait constant. De même, les degrés en y et z de $A(y, z)$ et $B(y, z)$ sont non nuls.

On note Ω_0 une clôture algébrique de $\mathbb{C}(x)$ et on appelle Ω_1 et Ω_2 les corps de décomposition de $g(y) - x$ et $h(z) - x$ dans Ω_0. On appelle y_1, y_2, ..., y_{d_g} les racines de $g(y) - x$ et z_1, z_2,..., z_{d_h} celles de $h(z) - x$.

2.1.1 Les deux polynômes ont même corps de décomposition

Suivant [23] on montre tout d'abord que $\Omega_1 = \Omega_2$. Il suffit d'observer que $g(y_1) - h(z_i) = A(y_1, z_i)B(y_1, z_i) = 0$ pour tout i. Puisque le degré en z de $A(y, z)$ est non nul, on a pour au moins un i (disons $i = 1$) l'identité $A(y_1, z_1) = 0$. Donc l'extension $\mathbb{C}(y_1, z_1)/\mathbb{C}(y_1)$ est de degré inférieur à d_h. On en déduit que les extensions $\mathbb{C}(z_1)/\mathbb{C}(x)$ et $\Omega_1/\mathbb{C}(x)$ sont non-disjointes (voir par exemple [24] page 305). Comme le polynôme h est indécomposable, l'extension $\mathbb{C}(z_1)/\mathbb{C}(x)$ l'est aussi et n'étant pas disjointe de $\Omega_1/\mathbb{C}(x)$ elle y est contenue. Par symétrie, on déduit que $\Omega_1 = \Omega_2$. En particulier $d_g = d_h$. Ainsi k est le degré total de $A(y, z)$ mais c'est aussi le degré en y et le degré en z (exercice trivial mais essentiel).

On note $n = d_g = d_h$ et on appelle G le groupe de Galois de $\Omega = \Omega_1 = \Omega_2$ sur $\mathbb{C}(x)$. Ce groupe est muni de deux représentations $\mathcal{R}_1$ et $\mathcal{R}_2$, par permutation des $(y_i)_{1 \le i \le d}$ et des $(z_i)_{1 \le i \le d}$ respectivement. On notera ces représentations par . et $*$ de telle sorte que pour $\sigma \in G$ on ait

$$\sigma(y_i) = y_{\sigma.i} \text{ et } \sigma(z_i) = z_{\sigma * i}.$$

Si U est un sous-ensemble de $\{1, 2, ..., n\}$ on notera de même $\sigma.U$ et $\sigma * U$.

2.1.2 Rappels sur les revêtements de la sphère

Les valeurs singulières d'un polynôme irréductible correspondent aux places ramifiées de son corps de décomposition. Puisque $\Omega_1 = \Omega_2$ les polynômes g et h ont les mêmes valeurs singulières. Appelons a_1, a_2, ..., a_s les valeurs critiques finies communes à g et h. Soit Γ une courbe fermée orientée positivement sur $\mathbb{P}_1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$ passant par a_1, a_2, ..., a_s, ∞ dans cet ordre. Elle délimite une calote supérieure $\mathcal{H}^+$ et une calote inférieure $\mathcal{H}^-$. Soit B un point de $\mathcal{H}^+$. On définit une base $(\Sigma_i)_{1 \leq i \leq s}$ de $\pi_1(\mathbb{P}_1(\mathbb{C}) - \{a_1, ..., a_s, \infty\}, B)$ comme sur la figure (1). On pose $\Sigma_\infty = (\Sigma_1.\Sigma_2...\Sigma_s)^{-1}$.

Soit $\mathcal{M}_{a_1,a_2,...,a_s,\infty}$ l'extension maximale de $\mathbb{C}(x)$ non ramifiée en dehors de a_1, a_2, ..., ∞. Le groupe fondamental algébrique de $\mathbb{P}^1_{/\mathbb{C}} - \{a_1, ..., a_s, \infty\}$ est par définition le groupe de Galois $\mathrm{Gal}(\mathcal{M}_{a_1,...,a_s,\infty}/\mathbb{C}(x))$. On montre que c'est le complété profini $\hat{\pi}_1(\mathbb{P}_1(\mathbb{C}) - \{a_1, ..., a_s, \infty\}, B)$ du groupe fondamental topologique. C'est donc un groupe prolibre à s générateurs $\hat{\Sigma}_1$, ..., $\hat{\Sigma}_s$ où $\hat{\Sigma}_i$ est l'image de Σ_i dans $\hat{\pi}_1(\mathbb{P}_1(\mathbb{C}) - \{a_1, ..., a_s, \infty\}, B)$. Le lacet $\hat{\Sigma}_i$ engendre le groupe d'inertie d'un point au dessus de a_i. On identifie Ω à un sous-corps de $\mathcal{M}_{a_1,...,a_s,\infty}$. Le groupe G est ainsi un quotient du groupe fondamental algébrique. Nous appelons σ_1, ..., σ_s, σ_∞ les images dans G des $\hat{\Sigma}_i$. Puisque $\mathbb{C}(y_1)/\mathbb{C}(x)$ et $\mathbb{C}(z_1)/\mathbb{C}(x)$ sont totalement ramifiées en ∞, l'élément σ_∞ est représenté par un n-cycle dans $\mathcal{R}_1$ et $\mathcal{R}_2$.

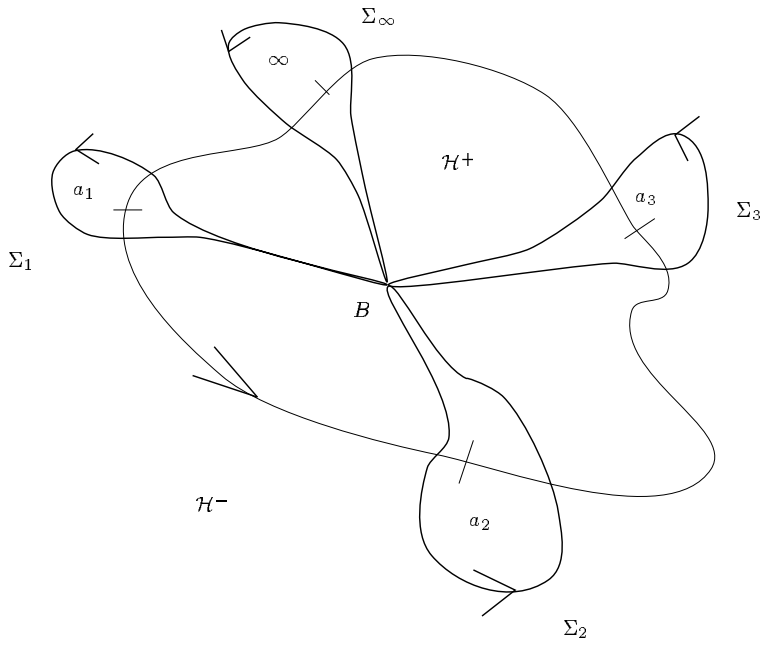

Figure 1: Groupe fondamental

2.1.3 Les deux représentations sont doublement transitives

Suivant [21] nous montrons que chacune de ces deux représentations est doublement transitive. On a vu que le groupe de Galois d'un polynôme indécomposable est un groupe de permutations primitif contenant un cycle complet. Si le degré n d'un tel groupe est composé, Schur a montré dans [28] que le groupe est doublement

transitif. Si G est un groupe de degré n premier et si G n'est pas doublement transitif, Burnside a montré dans [6] que l'ordre de G divise $n(n-1)$. Voir aussi [7, page 234] pour ces deux résultats. Fried complète cette argumentation et montre que si le groupe G d'un polynôme indécomposable n'est pas doublement transitif alors ce polynôme est faiblement linéairement relié à un polynôme cyclique $C_n(x) = x^n$ ou de Tchebitchev $T_n(\cos\theta) = \cos(n\theta)$. Il nous reste à prouver que cette dernière possibilité est exclue par les hypothèses du théorème (1). Supposons donc que g et h sont f.l.r. à des polynômes cycliques ou de Tchebitchev et montrons qu'alors les conditions du théorème (1) ne sont pas satisfaites. On distingue plusieurs cas.

- Si g n'est pas f.l.r. à un polynôme cyclique alors h ne peut pas être f.l.r. à un polynôme cyclique (sans quoi Ω_1 ne pourrait pas être égal à Ω_2 pour des raisons évidentes de ramification). Dans ce cas g et h sont f.l.r. au polynôme de Tchebitchev $T_n(x)$ et donc ils sont f.l.r. entre eux. Si le degré n est supérieur à deux, les deux polynômes ont trois valeurs critiques. Par des considérations évidentes de ramification on se ramène toujours à l'un des deux cas

  $$g = h = T_n \text{ ou } g = -h = T_n.$$

  Dans le premier cas les deux polynômes sont linéairement reliés. Dans le second cas, ou bien n est impair et alors $h(z) = -g(z) = -T_n(z) = T_n(-z)$ et donc g et h sont linéairement reliés ou bien n est pair et $T_n = T_{n/2} \circ T_2$ et g n'est pas indécomposable si $n \geq 4$. Enfin si $n = 2$, $T_2(x)$ est f.l.r. au polynôme $C_2(x) = x^2$, contradiction.

- Si g est f.l.r à un polynôme cyclique alors h doit l'être aussi (ramification) et l'on a, à faible équivalence près, $g(x) = x^2$ et $h(y) = Ky^2 = (\sqrt{K}y)^2$. Donc f et g sont f.l.r.

On voit que sous les hypothèses du théorème (1) les représentations du groupe de Galois G associées à g et h sont doublement transitives.

2.1.4 Les deux représentations par permutations ne sont pas équivalentes mais elles ont même caractère

On montre d'abord que $\mathcal{R}_1$ et $\mathcal{R}_2$ ne sont pas équivalentes en tant que représentations par permutations. Si elles l'étaient, le stabilisateur de 1 pour $\mathcal{R}_1$ serait le stabilisateur d'un élément i de $\{1, 2, ..., n\}$ pour $\mathcal{R}_2$ et on aurait $\mathbb{C}(y_1) = \mathbb{C}(z_i)$ ce qui n'est pas car les deux polynômes g et h ne sont pas linéairement reliés.

En revanche, $\mathcal{R}_1$ et $\mathcal{R}_2$ sont des représentations de G équivalentes (i.e. elles ont le même caractère). Pour le prouver, on utilise un théorème classique de théorie des groupes (Th. 16.6.15 de [25])

Théorème 3 . *Soit G un groupe fini. Soit $\mathcal{R}$ une représentation par permutations de G, doublement transitive. Alors, vue comme représentation $\mathbb{C}$-linéaire, $\mathcal{R}$ est la somme de la représentation unité et d'une unique représentation irréductible.*

Appelons alors V_1 et V_2 les G-modules associés à $\mathcal{R}_1$ et $\mathcal{R}_2$. Ce sont des espaces vectoriels de dimension n sur $\mathbb{C}$, de bases $(Y_i)_{1\leq i\leq n}$ et $(Z_i)_{1\leq i\leq n}$ telles que $\sigma(Y_i) = Y_{\sigma.i}$ et $\sigma(Z_i) = Z_{\sigma * i}$. Comme $\mathcal{R}_1$ et $\mathcal{R}_2$ sont doublement transitives, V_1 et V_2 sont chacun somme d'un module irréductible de dimension $n-1$ et d'un module invariant de dimension 1.

Appelons $\mathcal{M}_1$ et $\mathcal{M}_2$ les $\mathbb{C}$-espaces vectoriels engendrés par les $(y_i)_i$ et les $(z_i)_i$ respectivement. Soient γ_1 et γ_2 les applications $\mathbb{C}[G]$-linéaires définies par

$$\gamma_1 : \quad V_1 \longrightarrow \mathcal{M}_1$$

$$Y_i \longmapsto y_i$$

et

$$\gamma_2 : \quad V_2 \longrightarrow \mathcal{M}_2$$

$$Z_i \longmapsto z_i$$

L'image $\mathcal{M}_1$ de γ_1 est isomorphe à un facteur de V_1. Or la dimension sur $\mathbb{C}$ de $\mathcal{M}_1$ est plus grande que 1, sinon le stabilisateur de y_1 stabiliserait tous les y_i et $\mathcal{R}_1$ ne serait pas doublement transitive. Donc $V_1 = I \oplus \mathcal{M}_1$. De même $V_2 = I \oplus \mathcal{M}_2$.

Revenons alors à l'équation $A(y_1, z_1) = 0$. Suivant [22] on note $z_1, z_{\alpha_2}, ..., z_{\alpha_k}$ les k solutions de l'équation $A(y_1, z) = 0$. Puisque le degré total de $A(y, z)$ est k, le terme en z^{k-1} est de la forme $ay + b$ avec $a, b \in \mathbb{C}$. On a donc

$$ay_1 + b = z_1 + z_{\alpha_2} + ... + z_{\alpha_k}. \tag{1}$$

On montre que a n'est pas nul. Comme $\mathcal{M}_2$ est de dimension $n-1$, il n'y a qu'une relation linéaire entre les $(z_i)_i$ et c'est

$$z_1 + z_2 + ... + z_n - c = 0 \tag{2}$$

avec $c \in \mathbb{C}$. En particulier, puisque $k < n$ on sait que a est non nul.

On voit que les $(y_i)_i$ et les $(z_i)_i$ engendrent le même espace vectoriel sur $\mathbb{C}$ (à cause de l'équation (1) et de ses conjuguées). On pose $\mathcal{M} = \mathcal{M}_1 = \mathcal{M}_2$ et on obtient

$$V_1 = V_2 = I \oplus \mathcal{M}.$$

Ainsi $\mathcal{R}_1$ et $\mathcal{R}_2$ ont le même caractère.

2.1.5 Le groupe G est un groupe linéaire

Il résulte de ce qui précède que si deux polynômes g et h de degré n satisfont les hypothèses du théorème (1), leur groupe de Galois G satisfait les conditions suivantes

Hypothèses 1 . *Le groupe G est fini et il admet deux représentations fidèles de degré n, doublement transitives, non-équivalentes et de même caractère. Il existe un élément σ_∞ dans G qui est représenté dans l'une des deux (et donc dans chaque) représentations par un cycle complet d'ordre n.*

Comme Feit le remarque dans [20] les résultats de Curtis, Kantor et Seitz ([12]) impliquent le

Théorème 4 . *Sous les hypothèses (1) et si l'assertion (1) est vraie alors le groupe G est soit $PSL_2(11)$ soit un sous-groupe de $P\Gamma L_{\kappa+1}(q)$ contenant $PSL_{\kappa+1}(q)$ pour $\kappa \geq 2$ et $n = (q^{\kappa+1}-1)/(q-1)$.*

2.2 Configuration associée

On suit la présentation de [27]. Pour avancer encore dans la caractérisation des groupes de Galois de nos polynômes nous leur associons des configurations cycliques.

2.2.1 Rappels sur les configurations

Si n, k et ℓ sont trois entiers positifs tels que

$$0 < \ell < k < n-1$$

on appelle (n,k,ℓ)-*configuration* un couple $\mathcal{U} = (X, (U_v)_{1\leq v\leq n})$ où X est un ensemble de cardinalité n et les U_v sont des parties de X de cardinalité k telles que pour toute paire (v_1, v_2) avec $v_1 \neq v_2$, le cardinal de $U_{v_1} \cap U_{v_2}$ soit ℓ. On déduit [27] que

$$k(k-1) = \ell(n-1).$$

On dit que deux (n,k,ℓ)-configurations $\mathcal{U} = (X, (U_v)_{1\leq v\leq n})$ et $\mathcal{V} = (Y, (V_v)_{1\leq v\leq n})$ sont *isomorphes* s'il existe une bijection $\Pi : X \to Y$ et une permutation $\pi \in S_n$ telles que $\Pi(U_v) = V_{\pi(v)}$. On appelle *groupe d'automorphismes* de la configuration $\mathcal{U}$ et on note $\mathrm{Aut}(\mathcal{U})$ le groupe des permutations de X qui permutent les U_v. Lorsque ce groupe contient un cycle de longueur n on dit que la configuration est *cyclique*. On peut alors identifier X à $\mathbb{Z}/n\mathbb{Z}$ de façon qu'un cycle de longueur n noté par exemple $\sigma_\infty \in \mathrm{Aut}(\mathcal{U})$ agisse par $\sigma_\infty(i) = i+1$.

Dans cette situation, U_1 est un sous-ensemble de cardinalité k de $\mathbb{Z}/n\mathbb{Z}$ tel que chaque résidu non nul x mod n s'écrive de ℓ manières distinctes comme différence de deux éléments de U_1. On dit que U_1 est un *ensemble aux différences* modulo n.

On peut ainsi construire un ensemble aux différences à partir d'une configuration $\mathcal{U}$ et d'un automorphisme cyclique σ_∞.

Réciproquement, un ensemble aux différences donne une configuration munie d'un automorphisme cyclique.

On dit que deux ensembles aux différences U_a et U_b sont *égaux* s'ils sont translatés l'un de l'autre c'est-à-dire $U_b = U_a + t$ avec $t \in \mathbb{Z}/n\mathbb{Z}$. On dit qu'ils sont *équivalents* ou *conjugués* s'il existe $\chi \in (\mathbb{Z}/n\mathbb{Z})^*$ et $t \in \mathbb{Z}/n\mathbb{Z}$ tels que $U_b = \chi U_a + t$. On dit qu'ils sont *isomorphes* si les configurations associées sont isomorphes.

Si deux ensembles aux différences sont équivalents ils sont clairement isomorphes. La réciproque est incertaine. Cela revient à demander si l'ensemble aux différences dépend à équivalence près du cycle σ_∞ choisi.

Étant donné un ensemble aux différences, on considère un sous-groupe du groupe des automorphismes de la configuration associée :

Définition 1 . *Soit $U \subset \mathbb{Z}/n\mathbb{Z}$ un ensemble aux différences. On appelle multiplicateur de U un élément μ de $(\mathbb{Z}/n\mathbb{Z})^*$ tel que μU soit un translaté de U c'est-à-dire $\mu U = U + t_\mu$ avec $t_\mu \in \mathbb{Z}/n\mathbb{Z}$. Les multiplicateurs sont des automorphismes de la configuration associée. On note $\mathbb{M}$ le groupe des multiplicateurs.*

Si $n \geq 3$ est premier alors $\mathbb{M}$ est cyclique et l'on peut translater U de telle sorte que les t_μ soient nuls. On a alors $\mu U = U$ pour tout multiplicateur et on dit que U est bien normalisé.

Nous avons besoin d'un résultat essentiel de Feit [18]

Théorème 5 . *Tout automorphisme non trivial d'une configuration déplace au moins la moitié des points.*

Ce théorème est utilisé plus bas avec la formule de Riemann-Hurwitz.

2.2.2 Construction de la configuration

On se replace dans les hypothèses du théorème (1) et on examine les conséquences de la formule (1).

Soit $U_1 = \{1, \alpha_2, \alpha_3, ..., \alpha_k\}$ et soit $\sigma \in G$. Si $\sigma * U_1 = U_1$ alors $\sigma.1 = 1$ à cause de l'équation (1). Réciproquement si $\sigma.1 = 1$ alors $\sum_{i \in U_1} z_i - \sum_{i \in \sigma * U_1} z_i = 0$ et donc $\sigma * U_1 = U_1$ puisque (2) est la seule relation linéaire entre les z_i. On peut donc associer à tout $i \in \{1, 2, ..., n\}$ un unique sous ensemble U_i de $\{1, 2, ..., n\}$ tel que $\#U_i = k$ et $\sigma * U_i = U_{\sigma.i}$.

L'ensemble $\{1, 2, ..., n\}$ muni des n sous-ensembles $(U_i)_{1 \leq i \leq n}$ forme une (n, k, ℓ) - configuration selon la définition donnée plus haut. En effet, pour $i \neq j$ la cardinalité de $U_i \cap U_j$ est indépendante de (i, j) à cause de la double transitivité de $\mathcal{R}_2$. On note ℓ cette quantité et on vérifie les conditions de non-trivialité

$$0 < \ell < k < n - 1.$$

D'autre part le groupe G est inclus dans le groupe des automorphismes de la configuration.

On a vu que puisque $\mathbb{C}(y_1)/\mathbb{C}(x)$ et $\mathbb{C}(z_1)/\mathbb{C}(x)$ sont totalement ramifiées en ∞, l'automorphisme $\sigma_\infty \in G$ est représenté par un n-cycle dans $\mathcal{R}_1$ et $\mathcal{R}_2$. Ainsi la configuration est cyclique. On peut alors construire un ensemble aux différences.

On identifie $\{1, 2, ..., n\}$ à $\mathbb{Z}/n\mathbb{Z}$ et on renumérote $\mathcal{R}_1$ et $\mathcal{R}_2$ de façon que $\sigma_\infty * i = i + 1 \bmod n$ et $\sigma_\infty.i = i + 1$. On a alors $U_{i+\delta} = U_i + \delta \bmod n$.

2.2.3 Caractérisation des groupes de Galois

On exploite les conditions imposées par la formule de Riemann-Hurwitz à la ramification d'un polynôme. Nous rappelons la définition suivante

Définition 2 . *Soit $\sigma \in S_n$ une permutation. Soit $c(\sigma)$ le nombre de cycles de σ. On appelle défaut de σ et on note $\delta(\sigma)$ la quantité $n - c(\sigma)$.*

Dans notre situation, si g est un élément de G, on notera $\delta_i(g)$ son défaut dans la représentation $\mathcal{R}_i$ pour $i \in \{1,2\}$.

La formule de Riemann-Hurwitz impose

$$\delta_i(\sigma_\infty) + \sum_{1 \leq u \leq s} \delta_i(\sigma_u) = 2n-2 \text{ pour } i \in \{1,2\}.$$

Comme le théorème de Feit cité plus haut affirme qu'un automorphisme non trivial d'une configuration déplace au moins la moitié des points nous en déduisons que s est inférieur ou égal à 4. En effet, pour tout élément $\sigma \in G$ on a $c(\sigma) \leq 3n/4$ puisque on a au plus $n/2$ points fixes et $n/4$ cycles de longueur 2. Donc $\delta(\sigma) \geq n/4$. De plus $\delta(\sigma_\infty) = n-1$ et donc

$$2n-2 = \delta(\sigma_\infty) + \sum_{1 \leq u \leq s} \delta(\sigma_u) \geq n-1+sn/4$$

d'où le résultat.

Ainsi $s \in \{0,1,2,3\}$. Comme $s=0$ est impossible, $s=1$ correspond aux revêtements cycliques, il reste $s=2$ et $s=3$.

Nous nous trouvons donc dans la situation suivante

Hypothèses 2 . *Le groupe G est égal à $PSL_2(11)$ ou à un sous-groupe de $P\Gamma L_{\kappa+1}(q)$ contenant $PSL_{\kappa+1}(q)$ pour $\kappa \geq 2$ et $n = (q^{\kappa+1}-1)/(q-1)$.*

Le groupe G a deux représentations fidèles par permutations de degré n, $\mathcal{R}_1$ et $\mathcal{R}_2$, doublement transitives, non équivalentes et de même caractère. On a un entier $s \in \{2,3\}$ et des éléments de G, $(\sigma_u)_{1 \leq u \leq s}$ et σ_∞ tels que $\sigma_1 ... \sigma_s = \sigma_\infty^{-1}$ et les $(\sigma_u)_{1 \leq u \leq s}$ engendrent G. De plus pour $i \in \{1,2\}$ on a

$$\delta_i(\sigma_\infty) = n-1 \text{ et } \sum_{1 \leq u \leq s} \delta_i(\sigma_u) = n-1.$$

Un théorème de Feit [19, Théorème 3] affirme alors

Théorème 6 . *Sous les hypothèses (2) le groupe G est $PSL_2(11)$ ou $P\Gamma L_{\kappa+1}(q)$ pour $(\kappa,q) \in \{(2,2),(3,2),(4,2),(2,3),(2,4)\}$. En particulier $n \in \{7,11,13,15,21,31\}$.*

2.2.4 Caractérisation de la configuration

Nous venons de caractériser précisément le groupe G. Il nous reste à décrire les (n,k,ℓ)-configurations possibles. Chacun des groupes énumérés au théorème (6) est le groupe d'automorphismes d'une configuration cyclique doublement transitive classique que nous allons décrire maintenant. Nous construisons une configuration $H(11)$ de groupe d'automorphismes $PSL_2(11)$ ainsi que des configurations $D_\kappa(q)$ de groupes d'automorphismes $P\Gamma L_{\kappa+1}(q)$. Nous voyons ensuite que cette configuration est en un sens unique.

La configuration $D_\kappa(q)$ est une $((q^{\kappa+1}-1)/(q-1),(q^\kappa-1)/(q-1),(q^{\kappa-1}-1)/(q-1))$-configuration cyclique. Les points sont les points de l'espace projectif $\mathbb{P}_\kappa(q)$ de dimension κ sur le corps $\mathbb{F}_q$ et les blocs sont les hyperplans de cet espace projectif.

La construction de cette configuration par Singer dans [29] repose sur l'observation que $\mathbb{P}_\kappa(q)$ peut être assimilé au groupe cyclique $\mathbb{F}^*_{q^{\kappa+1}}/\mathbb{F}^*_q$.

La configuration $H(11)$ a pour points les éléments de $\mathbb{Z}/11\mathbb{Z}$ et pour blocs les translatés du groupe des résidus quadratiques. Todd a montré que son groupe d'automorphismes est $PSL_2(11)$ et qu'il agit doublement transitivement [30].

Nous avons le résultat d'unicité suivant

Théorème 7 . *Si (G, n) est un couple formé d'un groupe fini et d'un entier correspondant à l'une des 7 lignes du tableau suivant :*

G	n
$P\Gamma L_3(2)$	7
$PSL_2(11)$	11
$P\Gamma L_3(3)$	13
$P\Gamma L_4(2)$	15
$P\Gamma L_3(4)$	21
$P\Gamma L_5(2)$	31

alors il existe seulement deux configurations cycliques doublement transitives de degré n munies d'un groupe d'automorphismes isomorphe à G. Ces deux configurations sont réciproques l'une de l'autre et l'une d'elles est $H(11)$ ou $D_\kappa(q)$ avec $(\kappa, q) \in \{(2,2),(3,2),(4,2),(2,3),(2,4)\}$. De plus, G est exactement le groupe d'automorphismes de l'une de ces configurations.

Ceci résulte du théorème 4 de [19] qui classifie les (n, k, ℓ)-configurations cycliques doublement transitives avec $k \leq 50$. On en déduit que $g(y) - h(z)$ a exactement deux facteurs irréductibles de degrés k et $n - k$. Des informations plus précises sont données dans le tableau à la fin de la section 2.2.5.

2.2.5 Unicité des ensembles aux différences associés aux configurations considérées

On a vu comment à une (n, k, ℓ)-configuration cyclique $\mathcal{U} = (X, (U_v)_{1 \leq v \leq n})$ associer un ensemble aux différences modulo n. On choisit un cycle σ de longueur n dans le groupe d'automorphismes G de la configuration et un élément b de X et on construit la bijection

$$\beta_{\sigma,b} : \quad \mathbb{Z}/n\mathbb{Z} \longrightarrow X$$

$$x \longmapsto \sigma^x(b)$$

L'ensemble aux différences est alors $\beta^{-1}_{\sigma,b}(U_v)$ pour un v entier compris entre 1 et n. Le choix de v est sans importance puisqu'un ensemble aux différences est défini à translation près. Observons que si l'on remplace b par b' l'application β est composée par une translation modulo n. On obtient donc le même ensemble aux différences. Si l'on remplace σ par un conjugué $\sigma' = \delta\sigma\delta^{-1}$ avec $\delta \in G$ on obtient encore le même ensemble aux différences. En effet $\beta_{\sigma',\delta(b)}(i) = \delta\beta_{\sigma,b}(i)$.

Dans la série de lemmes qui suivent nous étudions donc les cycles de longueur maximale dans les groupes linéaires classiques.

Pour étudier ces groupes nous rappelons quelques définitions et quelques résultats relatifs aux géométries finies. On peut se reporter au premier chapitre de [15]. Si p est un nombre premier et $q = p^e$ une puissance de p, on note $\mathcal{A}_{\kappa+1}(q)$ l'espace affine de dimension $\kappa + 1$ sur $\mathbb{F}_q$. On rappelle que $\Gamma L_{\kappa+1}(q)$ est l'ensemble des permutations de $\mathcal{A}_{\kappa+1}(q)$ qui fixent l'origine et respectent la relation d'alignement des points. Ses éléments sont les transformations semilinéaires de l'espace affine $\mathcal{A}_{\kappa+1}(q)$. De même $P\Gamma L_{\kappa+1}(q)$ est le groupe des permutations de $\mathbb{P}_\kappa(q)$ qui respectent la relation d'alignement des points. Le groupe projectif linéaire $PGL_{\kappa+1}(q)$ est un sous-groupe normal d'indice e de $P\Gamma L_{\kappa+1}(q)$. Tous les sous-groupes de $P\Gamma L_{\kappa+1}(q)$ sont munis de la représentation naturelle sur $\mathbb{P}_\kappa(q)$.

Lemme 1 . *Les cardinalités de $GL_{\kappa+1}(q)$, $PGL_{\kappa+1}(q)$, $\Gamma L_{\kappa+1}(q)$, $P\Gamma L_{\kappa+1}(q)$ sont*

$$|GL_{\kappa+1}(q)| = q^{\kappa(\kappa+1)/2} \prod_{1\leq i\leq \kappa+1} (q^i - 1) \quad (3)$$

$$|PGL_{\kappa+1}(q)| = q^{\kappa(\kappa+1)/2} \prod_{2\leq i\leq \kappa+1} (q^i - 1) \quad (4)$$

$$|\Gamma L_{\kappa+1}(q)| = eq^{\kappa(\kappa+1)/2} \prod_{1\leq i\leq \kappa+1} (q^i - 1) \quad (5)$$

$$|P\Gamma L_{\kappa+1}(q)| = eq^{\kappa(\kappa+1)/2} \prod_{2\leq i\leq \kappa+1} (q^i - 1) \quad (6)$$

Voir [16] pour une preuve de ce lemme.

Considérons l'extension de corps $\mathbb{F}_{q^{\kappa+1}}/\mathbb{F}_q$ et soit α un générateur de $\mathbb{F}^*_{q^{\kappa+1}}$. L'application $x \mapsto \alpha x$ est un endomorphisme du $\mathbb{F}_q$-espace vectoriel sous-jacent à $\mathbb{F}_{q^{\kappa+1}}$. On lui associe une matrice d'ordre $q^{\kappa+1} - 1$ dans $GL_{\kappa+1}(q)$. La permutation associée est un cycle complet. On construit ainsi un cycle complet dans $GL_{\kappa+1}(q)$ et donc dans $PGL_\kappa(q)$, $\Gamma L_{\kappa+1}(q)$ et $P\Gamma L_\kappa(q)$. On se propose de montrer que tous les cycles complets de ces groupes sont obtenus ainsi.

On utilise deux faits bien connus de théorie élémentaire des nombres.

Lemme 2 . *Notons (a, b) le pgcd de deux entiers positifs a et b. Soit n un entier positif. Alors pour a et b entiers positifs*

$$(n^a - 1, n^b - 1) = n^{(a,b)} - 1.$$

Lemme 3 . *Soit $n > 1$ et $k > 2$ deux entiers. Il existe un entier premier l tel que $l|(n^k - 1)$ et $l \not|(n^i - 1)$ pour $1 \leq i < k$ sauf si $n = 2$ et $k = 6$.*

Ce lemme est prouvé dans [4] et [10] de deux façons différentes. Nous montrons maintenant le

Lemme 4 . *Si p est un nombre premier et e un entier positif, notons $q = p^e$. Soit $\kappa > 1$ un entier. Soient σ et σ' deux cycles de longueur $q^{\kappa+1} - 1$ dans $GL_{\kappa+1}(q)$. Alors σ' est conjugué à une puissance de σ.*

Supposons d'abord que $(q, \kappa+1)$ est différent de $(2,6)$. Soit l un nombre premier qui divise $q^{\kappa+1}-1$ et ne divise pas q^i-1 pour $1 \leq i < \kappa+1$. Posons $q^{\kappa+1}-1 = l^v m$ avec l premier à m et soit $\mu = \sigma^m$, $\mu' = \sigma'^m$. Puisque l est premier à p le théorème de Mashke ([24, page 641]) affirme que le groupe $<\mu>$ est complètement réductible, i.e. $\mathcal{A}_{\kappa+1}(q)$ se décompose comme somme directe de sous-espaces irréductibles sous l'action de $<\mu>$. On montre que μ est irréductible, i.e. n'admet pas de sous-espace stable non trivial. Dans le cas contraire, μ serait contenu dans un produit de groupes linéaires de dimensions inférieures à $\kappa+1$ correspondants aux espaces isotypiques. Son ordre serait donc premier à l par le lemme (1) ce qui n'est pas.

On appelle $C(\mu)$ l'ensemble des matrices de dimension $\kappa+1$ qui commutent à μ. Puisque μ est irréductible, $C(\mu)$ est un corps (Lemme de Schur). Puisque σ commute à μ on a $\#C(\mu) \geq q^{\kappa+1}$. En outre le degré de l'extension de corps $C(\mu)/\mathbb{F}_q$ est inférieur ou égal à $\kappa+1$ (théorème de Cayley-Hamilton). Donc $C(\mu)$ est isomorphe à $\mathbb{F}_{q^{\kappa+1}}$. Les éléments inversibles de $C(\mu)$ forment le centralisateur $Z(\mu)$ de μ dans $GL_{\kappa+1}(q)$. Ainsi $Z(\mu) =<\sigma>$. Or $<\mu>$ est un l-groupe de Sylow de $GL_{\kappa+1}(q)$ (l^{v+1} ne divise pas $\#GL_{\kappa+1}(q)$). De même, σ' engendre le centralisateur d'un l-groupe de Sylow. Donc $<\sigma>$ et $<\sigma'>$ sont des sous-groupes cycliques conjugués et il existe un entier χ premier à $q^{\kappa+1}-1$ tel que σ' soit conjugué à σ^χ.

Considérons maintenant le cas $q=2$, $\kappa+1=6$. Le groupe $GL_6(2)$ a six classes de conjugaisons d'ordre $2^6-1=63$. Elles sont conjuguées par le sous groupe engendré par 5 dans $(\mathbb{Z}/63\mathbb{Z})^*$. Ceci se vérifie avec le logiciel magma V2.20-1 [5].

Un énoncé similaire vaut pour les groupes projectifs linéaires :

Lemme 5 . *Soit p est un nombre premier et e un entier positif, $q=p^e$. Soit $\kappa>1$ un entier. Soient σ et σ' deux cycles de longueur $(q^{\kappa+1}-1)/(q-1)$ dans $PGL_{\kappa+1}(q)$. Alors σ' est conjugué à une puissance de σ.*

On note par une barre l'application quotient dans la suite exacte

$$1 \to \mathbb{F}_q{}^* \to GL_{\kappa+1}(q) \to PGL_{\kappa+1}(q) \to 1.$$

On relève σ et σ' dans $GL_{\kappa+1}(q)$. Soient donc Σ et Σ' dans $GL_{\kappa+1}(q)$ telles que $\bar{\Sigma} = \sigma$ et $\bar{\Sigma}' = \sigma'$. Il est clair que $\Sigma^{\frac{q^{\kappa+1}-1}{q-1}}$ est dans $\mathbb{F}_q$. Puisque $(q^{\kappa+1}-1)/(q-1)$ est premier à $q-1$ par le lemme (2), il est possible de choisir Σ d'ordre $q^{\kappa+1}-1$ dans $GL_{\kappa+1}(q)$. On suppose de même que Σ' est d'ordre $q^{\kappa+1}-1$. Alors il existe un entier χ tel que Σ^χ et Σ' soient conjuguées d'après le lemme (4). Donc σ^χ et σ' le sont aussi.

De même on prouve le

Lemme 6 . *Soit p est un nombre premier et e un entier positif, $q=p^e$. Soit $\kappa>1$ un entier. Soient σ et σ' deux cycles de longueur $q^{\kappa+1}-1$ dans $\Gamma L_{\kappa+1}(q)$. Alors σ' est conjugué à une puissance de σ.*

Supposons d'abord que $(q,(\kappa+1)e)$ est différent de $(2,6)$. On remarque simplement que $\Gamma L_{\kappa+1}(q)$ est inclus dans $GL_{(\kappa+1)e}(p)$. Choisissons l premier divisant $p^{(\kappa+1)e}-1$ et ne divisant pas les p^i-1 pour $1 \leq i < (\kappa+1)e$. On pose $p^{(\kappa+1)e}-1 = l^v m$ avec m premier à l et on définit $\mu = \sigma^m$ et de même μ'. C'est possible puisque

$(p,(\kappa+1)e)$ est différent de $(2,6)$. Le centralisateur de μ dans $GL_{(\kappa+1)e}(p)$ est $<\sigma>$. Comme ce dernier groupe est inclus dans $\Gamma L_{\kappa+1}(q)$ il est aussi le centralisateur de μ dans $\Gamma L_{\kappa+1}(q)$. On termine comme pour le lemme (4).

Si $p=2$, $q=4$ et $\kappa=2$ le groupe $GL_3(4)$ est normal d'indice deux dans $\Gamma L_3(4)$. Si σ et σ' sont deux éléments d'ordre $(q^3-1)/(q-1)=21$ dans $\Gamma L_3(4)$ alors ils sont dans $GL_3(4)$ et ils engendrent donc des groupes conjugués d'après le lemme (4).

Si $p=2$, $q=2$ et $\kappa=5$ alors le groupe $\Gamma L_6(2)$ n'est autre que $GL_6(2)$. On applique le lemme (4).

Enfin, on a le

Lemme 7 . *Soit p est un nombre premier et e un entier positif, $q=p^e$. Soit $\kappa>1$ un entier. Soient σ et σ' deux cycles de longueur $(q^{\kappa+1}-1)/(q-1)$ dans $P\Gamma L_{\kappa+1}(q)$. Alors σ' est conjugué à une puissance de σ.*

Ce dernier lemme se prouve comme le lemme (5).

Il reste à regler le cas de $PSL_2(11)$. L'examen de sa table de caractères dans l'Atlas [11] page 7 montre que ce groupe admet deux classes d'ordre 11, conjuguées l'une de l'autre.

Afin de construire les ensembles aux différences que nous cherchons on peut dans tous les cas choisir n'importe quel cycle et procéder comme dans [29].

Les ensembles aux différences ci-dessous sont bien normalisés.

G	n	k	ℓ	U_1	$\mathbb{M}$
$P\Gamma L_3(2)$	7	3	1	$\{1,2,4\}$	$\{1,2,4\}$
$PSL_2(11)$	11	5	2	$\{1,3,4,5,9\}$	$\{1,3,4,5,9\}$
$P\Gamma L_3(3)$	13	4	1	$\{0,7,8,11\}$	$\{1,3,9\}$
$P\Gamma L_4(2)$	15	7	3	$\{0,5,7,10,11,13,14\}$	$\{1,2,4,8\}$
$P\Gamma L_3(4)$	21	5	1	$\{7,9,14,15,18\}$	$\{1,2,4,8,16,11\}$
$P\Gamma L_5(2)$	31	15	7	$\{1,2,4,7,8,14,15,16,19,23,25,27,28,29,30\}$	$\{1,2,4,8,16\}$

On a prouvé le

Théorème 8 . *Si G et n sont un groupe et un entier donnés par l'une des lignes du tableau ci-dessus alors il existe seulement deux ensembles aux différences modulo n de groupe d'automorphismes G, à conjugaison près, réciproques l'un de l'autre. L'un d'entre eux est donné dans le tableau.*

3 Méthode de calcul

Dans cette section, nous exploitons les données combinatoires du tableau précédent. Nous aurons aussi besoin d'une normalisation appropriée.

Définition 3 . *On dit qu'une paire de polynômes $(g,h)\in\mathbb{C}[y]\times\mathbb{C}[z]$ de degré n est normalisée si $g_0=h_0=1$ et $g_1=h_1=0$ et $g_n=0$ avec les notations de la formule (7).*

Il est clair que toute paire est f.l.r. à une paire normalisée, c'est-à-dire, si $(g(y), h(z))$ sont des polynômes de degré n il existe $(a_x, b_x), (a_y, b_y), (A, B) \in \mathbb{C}^* \times \mathbb{C}$ tels que $(Ag(a_x x + b_x) + B, Ah(a_y y + b_y) + B)$ soit normalisée. De plus, si deux paires normalisées (g_1, h_1) et (g_2, h_2) sont f.l.r. alors il existe $\lambda \in \mathbb{C}$ tel que $(g_2(y), h_2(z)) = (\lambda^{-n} g_1(\lambda y), \lambda^{-n} h_1(\lambda z))$ si bien que g_i et h_i sont des formes homogènes de degré i.

On cherchera désormais des paires normalisées de degré n pour chacune des lignes du tableau donné au théorème (8). On rappelle que k et $n-k$ sont les degrés des facteurs de $g(y) - h(z)$. On note ces facteurs $A(y,z)$ et $B(y,z)$.

On étudie la situation au voisinage de ∞. L'extension galoisienne $\Omega/\mathbb{C}(x)$ est ramifiée d'ordre n au dessus de $x = \infty$. Soit donc φ l'unique plongement de $\Omega/\mathbb{C}$ dans le corps $\mathbb{C}[[t]]/\mathbb{C}$ des séries de Puiseux tel que $\varphi(z) = t^n$ et $\varphi(y_1) = 1/t + O(1)$. On écrira par abus de notation $t^n = z$ et $y_1^{-1} = t + O(1)$. Écrivons

$$g(y) = y^n + g_2 y^{n-2} + ... + g_{n-1} y \text{ et } h(z) = z^n + h_2 z^{n-2} + ... h_n. \tag{7}$$

On a alors $x^{-1} = t^n + O(t^{n+1})$. On sait que

$$\sigma_\infty(t) = \zeta_n t \text{ avec } \zeta_n = \exp(2i\pi/n).$$

Quitte à renuméroter les y_i et les z_i on peut toujours supposer $\sigma_\infty(y_i) = y_{\sigma_\infty . i} = y_{i+1}$ et $\sigma_\infty(z_i) = z_{\sigma_\infty * i} = z_{i+1}$. Rappelons que

$$a y_1 + b = \sum_{i \in U_1} z_i \text{ avec } U_1 = \{1, \alpha_2, ..., \alpha_k\}$$

Le développement de z_1 donne $z_1^{-1} = \zeta_n^r t + O(t^2)$ avec $0 \leq r \leq n-1$. On a alors

$$y_{i+1}^{-1} = \zeta_n^i t + O(t^2) \text{ et } z_{i+1}^{-1} = \zeta_n^{r+i} t + O(t^2).$$

Quitte à remplacer $h(z)$ par $h(\zeta_n^r z)$ on peut toujours supposer que $r = 0$.

Écrivons aussi $g(y) - h(z) = A(y,z)B(y,z)$ avec A et B irréductibles. On normalise de sorte que A et B soient unitaires en y. Soient

$$A(y,z) = \sum_{1 \leq u \leq k} A_u(y,z) \text{ et } B(y,z) = \sum_{1 \leq u \leq n-k} B_u(y,z)$$

les décompositions de A et B en termes homogènes. Si $i \in U_1$ alors $A_k(y_1, z_i) = 0$. Divisons par y_1^k et remplaçons y_1 et z_i par leurs expressions en t. Faisons tendre t vers 0, on obtient $A_k(1, \zeta_n^{-i-1}) = 0$ et donc

$$A_k(y,z) = \prod_{i \in U_1} (y - \zeta_n^{i+1} z) \text{ et } B_{n-k}(y,z) = \prod_{i \notin U_1} (y - \zeta_n^{i+1} z). \tag{8}$$

Cette identité est à la base de notre méthode.

Puisque

$$g(y) - h(z) = A(y,z)B(y,z) \tag{9}$$

on a pour tout $0 \leq l \leq n$

$$g_{n-l}y^l - h_{n-l}z^l = \sum_{0\leq u\leq l} A_u B_{l-u} \tag{10}$$

Pour $l = n-1$ on obtient

$$A_{k-1}B_{n-k} + A_k B_{n-k-1} = 0$$

et comme A_k et B_{n-k} sont premiers entre eux d'après (8) on en déduit

$$A_{k-1} = B_{n-k-1} = 0.$$

On examine alors l'équation (10) pour $l = n-2$. On trouve

$$A_{k-2}B_{n-k} + A_k B_{n-k-2} = g_2 y^{n-2} - h_2 z^{n-2}. \tag{11}$$

Soit (W, K) la paire de Bezout de (A_k, B_{n-k}) c'est-à-dire l'unique couple de polynômes tels que $\deg W < \deg B_{n-k}$ et $\deg K < \deg A_k$ et $WA_k + KB_{n-k} = 1$.

Dans l'anneau euclidien $\mathbb{C}(z)[y]$ on note $a \wr_y b$ le reste de la division de a par b. L'équation (11) implique alors

$$A_{k-2} = \{(g_2 y^{n-2} - h_2 z^{n-2})K\} \wr_y A_k \text{ et } B_{n-k-2} = \{(g_2 y^{n-2} - h_2 z^{n-2})W\} \wr_y B_{n-k}.$$

On en déduit donc A_{k-2} et B_{n-k-2} en fonction de g_2 et h_2. On obtient aussi des équations non triviales en écrivant que le coefficient en y^{n-1} de

$$\{(g_2 y^{n-2} - h_2 z^{n-2})K\} \wr_y A_k$$

et le coefficient en y^{n-k-1} de

$$\{(g_2 y^{n-2} - h_2 z^{n-2})W\} \wr_y B_{n-k}$$

sont nuls. Ces équations sont linéaires en h_2. On exprime ainsi h_2 en fonction de g_2.

On s'intéresse alors a l'équation (10) pour $l = n-3$ que l'on traite de la même manière. On calcule ainsi les A_{k-l} et les B_{n-k-l} pour $l = 0, 1, 2, ...$ en fonction des $g_2, ..., g_l, h_2, ..., h_l$. On utilise toutes les equations trouvées en cours de route pour éliminer autant de g_i et de h_i que possible.

Nous illustrons ce processus dans le cas simple mais générique où $n = 7$. On a alors $k = 3$ et $\ell = 1$. On prend $U_1 = \{0, 1, 3\}$. Posant $\zeta = \zeta_7$ on a donc

$$A_3 = (y - \zeta z)(y - \zeta^2 z)(y - \zeta^4 z) \text{ et } B_4 = (y - z)(y - \zeta^3 z)(y - \zeta^5 z)(y - \zeta^6 z).$$

On sait que $A_1 = \{g_2 y^5 - h_2 z^5)K\} \wr_y A_3$. On calcule donc $\{g_2 y^5 - h_2)K\} \wr_y A_3$. Son coefficient en y^2 est $C.(2g_2 + (2 + \zeta + \zeta^2 + \zeta^4)h_2)$ avec C constante. On en déduit que

$$h_2 = \frac{-1 + a_1}{2} g_2 \text{ avec } a_1 = \zeta + \zeta^2 + \zeta^4.$$

On a $A_0 = \{g_3 y^4 - h_3 z^4)K\}\wr_y A_3$. On calcule donc $\{g_3 y^4 - h_3)K\}\wr_y A_3$. Son coefficient en y^2 est $C.(2h_3 + (1-a_1)g_3)$ avec C constante. On en déduit que

$$h_3 = \frac{-1+a_1}{2} g_3.$$

Enfin $0 = \{g_4 y^3 - h_4 z^3)K\}\wr_y A_3$. On calcule donc $\{g_4 y^3 - h_4)K\}\wr_y A_3$. Ses coefficient en y^2 et y forment un système linéaire non singulier en g_4 et h_4 dont la résolution donne

$$\begin{aligned} g_4 &= g_2^2(9-a_1)/28 \\ h_4 &= g_2^4(-1-7a_1)/28 \end{aligned}$$

On a alors déterminé A et B en fonction des variables homogènes g_2 et g_3. On déshomogénéise en posant $g_2 = g_3 = T$ et on obtient la solution présentée dans la section 5.

On voit que A, B, P et Q sont définis sur la sous-extension d'indice 3 de $\mathbb{Q}(\zeta_7)/\mathbb{Q}$. En fait l'action de $\mathrm{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q})$ sur A_k et B_{n-k} est donnée par l'action de $(\mathbb{Z}/7\mathbb{Z})^*$ sur U_1. Or cette dernière action a $\mathbb{M}$ pour noyau et $\#\mathbb{M} = 3$.

Tous les calculs ont été menés de la même manière. On élimine toutes les inconnues sauf g_2 et g_3 en resolvant des équations linéaires. Si $n \in \{7, 13, 15\}$ on pose $g_2 = g_3 = T$. Si $n \in \{11, 21, 31\}$ il reste une équation du type $C.g_3^2 = g_2^3$ avec C constante. On pose $g_2 = g_3 = C$.

Réciproquement, on vérifie que les 6 quadruplets $(g(y), h(z), A(y,z), B(y,z))$ donnés dans la dernière section vérifient l'identité $g - h = AB$.

On a calculé dans un premier temps une solution numérique approchée avec le système PARI version 1.920.24 [3]. Les expressions algébriques exactes ont été retrouvées par des techniques d'interpolation. Les résultats ont ensuite été vérifiés avec Maple [9].

Les théorèmes (4), (6), (7), (8) et les calculs précédents prouvent le théorème (1).

4 Exploitation des formules explicites

Nous expliquons brièvement comment le calcul algébrique réalisé ci-dessus peut être exploité. Nous utiliserons les polynômes donnés dans la dernière section pour décrire la topologie des revêtements associés. Observons que cette description topologique peut s'obtenir aussi par des considérations combinatoires (voir [1, 2, 26]). Cependant, la connaissance du modèle algébrique que nous avons calculé doit nous permettre de retrouver la monodromie sans aucun effort. Notre propos n'est pas d'accumuler des données combinatoires mais de décrire brièvement des méthodes efficaces. C'est pourquoi nous traiterons seulement deux cas (le plus facile et le plus difficile).

Dans le cas $n = 7$, il y a trois valeurs critiques finies et le polynôme $g(y)$ dépend d'un paramètre T et d'une racine a_1 du polynôme $X^2 + X + 2$. Nous prenons pour a_1 celle de ces deux racines qui a une partie imaginaire négative et nous choisissons $T = 1$. Les trois valeurs singulières finies sont alors solutions de

$$S(X) = 343X^3 - 4802X^2 + 17220X + 24200$$

soit une réelle et deux complexes conjuguées. Soit

$$\mathcal{A} : [0,1] \to \mathbb{C}$$

une fonction dérivable telle que $\mathcal{A}(0)$ et $\mathcal{A}(1)$ soient les deux racines imaginaires de $S(X)$ et $\mathcal{A}(1/2)$ son unique racine réelle. On suppose aussi que la partie imaginaire de $\mathcal{A}(0)$ est positive. On prend comme point base b un réel inférieur à $\mathcal{A}(1/2)$ comme sur la figure (2).

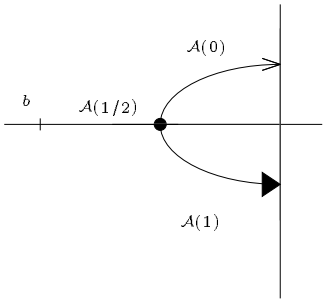

Figure 2: Points singuliers de g

On calcule points par points l'image réciproque de l'arc $\mathcal{A}([0,1])$ par l'application polynomiale $y \mapsto g(y)$. Le graphe obtenu est représenté schématiquement figure (3). Les nombres de 1 à 7 portés sur la figure représentent les points au dessus de b. Les flêches creuses correspondent aux points au dessus de $\mathcal{A}(0)$ et les flêches pleines aux points au dessus de $\mathcal{A}(1)$. Les gros points noirs sont les points au dessus de $\mathcal{A}(1/2)$.

La monodromie de g se déduit aisément de ce graphe qui n'est autre qu'un *dessin d'enfant* à ceci près que les *dessins* ordinaires correspondent à des revêtements ramifiés au dessus de trois points et non quatre. On pourra consulter les premiers articles de de [17] pour plus d'information.

Soit $(\Sigma_1, \Sigma_{1/2}, \Sigma_0)$ la base de $\pi_1(\mathbb{P}_1(\mathbb{C}) - \{\mathcal{A}(1), \mathcal{A}(1/2), \mathcal{A}(0)\}, b)$ représentée figure (4).

La monodromie de g dans cette base est alors

$$\begin{aligned} \sigma_1 &= [1,2][3,6] \\ \sigma_{1/2} &= [2,3][4,5] \\ \sigma_0 &= [3,4][6,7] \end{aligned}$$

On vérifie avec Maple [9] que le produit $\sigma_0\sigma_{1/2}\sigma_1$ est un cycle et que le groupe engendré par ces trois permutations est bien $P\Gamma L_3(2)$de cardinal 168.

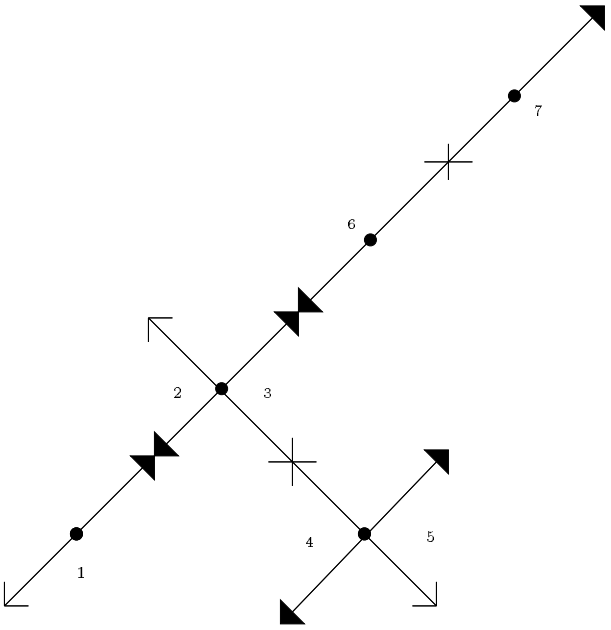

Figure 3: Dessin

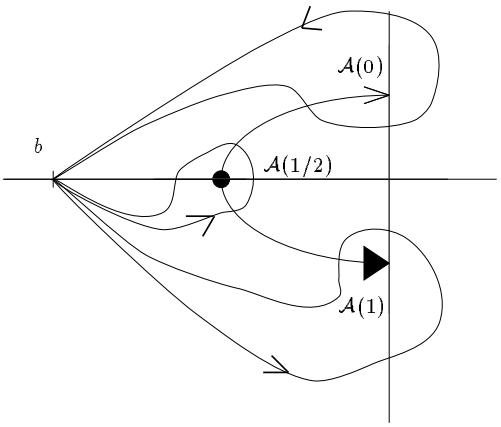

Figure 4: Groupe fondamental

Dans le cas $n = 31$, il y a deux valeurs critiques finies et le polynôme g dépend d'une racine a_1 du polynôme $X^6+X^5+3X^4+11X^3+44X^2+36X+31$. On choisit celle qui vaut $\zeta^{15}+\zeta^{23}+\zeta^{27}+\zeta^{29}+\zeta^{30}$ avec $\zeta = \exp(2i\pi/31)$. Les deux valeurs critiques c_1 et c_2 sont alors réelles et de parties entières -270281660985 et -140529620128. On considère l'image réciproque par g du segment $[c_1, c_2]$ représenté figure (5) et on obtient le graphe schématiquement représenté figure (6) où les nombres de 1 à 31 représentent les points au dessus du point base b.

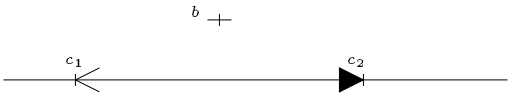

Figure 5: Lieu de ramification

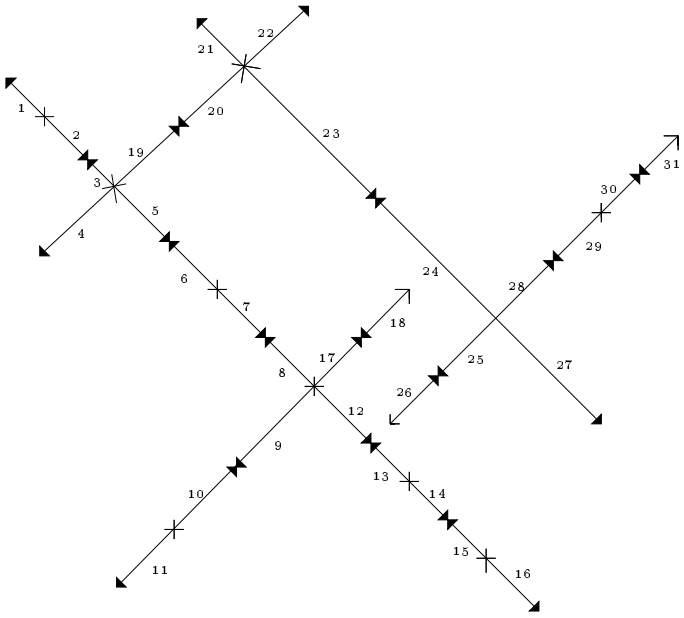

Figure 6: Dessin

On en déduit la monodromie $(\sigma_{c_1}, \sigma_{c_2})$.

$$\sigma_{c_1} = [1,2],[3,4,5,19],[6,7],[8,9,12,17],[10,11],[13,14],[15,16],[20,23,22,21],[24,25,27,28],[29,30]$$
$$\sigma_{c_2} = [2,3],[5,6],[7,8],[9,10],[12,13],[14,15],[17,18],[19,20],[23,24],[25,26],[28,29],[30,31]$$

On vérifie avec Maple [9] que le produit $\sigma_{c_2}\sigma_{c_1}$ est un cycle et que le groupe engendré par ces deux permutations est bien $P\Gamma L_5(2)$.

5 Résultats numériques

Les polynômes présentés ici ne sont pas exactement ceux calculés plus haut. On a procédé à quelques changements de paramètres pour simplifier un peu les expres-

sions. Les corps de définition de ces polynômes sont abéliens. On donne les automorphismes de ces corps en exprimant toutes les racines d'un polynôme en fonction de l'une d'elles, appellée a_1. Pour $n = 21$ et $n = 31$ on a placé les coefficients des polynômes dans des tableaux.

5.1 Données pour $n = 7$

$$a_1^2 + a_1 + 2 = 0 \text{ et } a_2 = -1 - a_1$$

$$g(y) = 1/7y^7 + (1+a_1)Ty^5 + (1+a_1)Ty^4 - (3-2a_1)y^3T^2 - 2(1-2a_1)y^2T^2 \\ -1/28(5+3a_1)y(28T - 2 - 11a_1)T^2 - (1+a_1)T^3$$

$$h(z) = \bar{g}(z)$$

où la barre exprime l'action de la conjugaison complexe sur les coefficients.

$$A = y^3 + a_1y^2z + y^2z + a_1yz^2 - z^3 + 5Ty + 3a_1Ty - 2Tz + 3a_1Tz + 2a_1T + T$$

divise $g(y) - h(z)$.

5.2 Données pour $n = 11$

$$a_1^2 + a_1 + 3 = 0 \text{ et } a_2 = -1 - a_1$$

$$g(y) = 1/11y^{11} - (1+a_1)y^9 + 2y^8 + (-9+3a_1)y^7 - 16(1+a_1)y^6 + (36+21a_1)y^5 + (-90+30a_1)y^4 \\ -63a_1y^3 + (120+100a_1)y^2 + (-117+24a_1)y - 18(1+a_1)$$

$$h(z) = \bar{g}(z)$$

où la barre exprime l'action de la conjugaison complexe sur les coefficients.

$$A = y^5 + y^4z + a_1y^4z - y^3z^2 + y^2z^3 + a_1yz^4 - z^5 - 2(1+2a_1)y^3 + (5-a_1)y^2z - (6+a_1)yz^2 \\ -2(1+2a_1)z^3 + 2(6+a_1)y^2 + 6(1+2a_1)yz + 2(a_1-5)z^2 - (15+8a_1)y + (7-8a_1)z - 6(2a_1+1)$$

divise $g(y) - h(z)$.

5.3 Données pour $n = 13$

$$a_1^4 + a_1^3 + 2a_1^2 - 4a_1 + 3 = 0 \text{ et } a_2 = (-6 + 4a_1 + 3a_1^2 + 2a_1^3)/3$$

$$a_3 = (3 - 2a_1 - a_1^3)/3 \text{ et } a_4 = (-5a_1 - 3a_1^2 - a_1^3)/3$$

$$g(y) = 1/13y^{13} - (-9 + 9a_1^2 + 16a_1 + 5a_1^3)Ty^{11} - (7a_1^3 - 30 + 9a_1^2 + 14a_1)Ty^{10}$$
$$+3(58a_1^2 + 58a_1 + 77a_1^3 - 508)T^2y^9 - 6(529a_1 + 270a_1^2 + 249 + 92a_1^3)T^2y^8$$
$$+1/8610741(3309a_1^2 - 1098 + 1547a_1^3 + 6070a_1)(77496669T - 1112205 - 2910893a_1 - 1133160a_1^2$$
$$-630415a_1^3)T^2y^7 + 9(27332a_1 + 16437a_1^2 - 33474 + 10516a_1^3)T^3y^6 - 1/812770767(-158880 +$$
$$88519a_1 + 40334a_1^3 + 55959a_1^2)(7314936903T - 614980158 - 1535903404a_1 - 656078493a_1^2$$
$$-300828668a_1^3)T^3y^5 - 1/122955093(-123237 + 3343a_1^3 - 20943a_1^2 - 51571a_1)(6639575022T$$
$$+6427461 - 88257175a_1 - 37716960a_1^2 - 37860440a_1^3)T^3y^4 + 1/17468217(-67683a_1^2 - 165626a_1$$
$$-387975 + 9764a_1^3)(471641859T - 29195376 - 447462832a_1 - 218260983a_1^2 -$$
$$102457574a_1^3)y^3T^4 - 1/1756673217(3268213a_1 + 1857678a_1^2 - 2010315$$
$$+1009604a_1^3)(47430176859T - 1093589412 - 3157157296a_1 - 1104020166a_1^2$$
$$-1067244536a_1^3)y^2T^4 + 1/255879(754764a_1^2 + 1383328a_1 + 354725a_1^3 - 267150)(9211644T^2$$
$$+14106879T - 34239186Ta_1 - 18557424Ta_1^2 - 9829593Ta_1^3 - 268320 + 26320a_1 - 34152a_1^2$$
$$+30392a_1^3)yT^4 + 5832a_1(19095T + 5236)T^5 + 324a_1^2(149259T + 40928)T^5$$

$$h(z) = \bar{g}(z)$$

où la barre exprime l'action de la conjugaison complexe sur les coefficients.

$$A = 3y^4 + (3a_1^2 + a_1^3 - 3 + 5a_1)y^3z + (-a_1 - 6 + a_1^3)y^2z^2 - (3a_1^2 + 2a_1^3 - 3 + 4a_1)yz^3 + 3z^4$$
$$-3(51a_1^2 + 88a_1 + 29a_1^3 - 63)Ty^2 - 27(-11 - a_1 + a_1^3)Tyz + 9(17a_1^2 + 9a_1^3 + 30a_1 - 18)Tz^2$$
$$-3(14a_1^3 - 72 + 15a_1^2 + 22a_1)Ty + 9(11a_1 + 12 + a_1^3 + 5a_1^2)Tz + 12(47a_1^3 - 465 - 47a_1)T^2$$

divise $g(y) - h(z)$.

5.4 Données pour $n = 15$

$$a_1^2 - a_1 + 4 = 0 \text{ et } a_2 = 1 - a_1$$

$$g(y) = 1/15y^{15} + (-1 + a_1)y^{13}T + (a_1 + 7)y^{12}T - (5a_1 + 21)y^{11}T^2 + 2(37a_1 - 71)y^{10}T^2$$
$$-1/454794(-349 + 261a_1)(151598T - 109260 + 141075a_1)T^2y^9 - (649a_1 + 703)y^8T^3 +$$
$$3/76579(239 + 46a_1)(76579T - 462560 + 198260a_1)T^3y^7 - 4/259891(548a_1 - 1939)(259891T$$
$$+106365a_1 - 26420)T^3y^6 + 3/36391540(-1581 + 1945a_1)(7278308T + 14685825a_1$$
$$-113700500)T^4y^5 + 3/877444(3233a_1 + 2051)(877444T - 2162500 + 1339725a_1)y^4T^4$$

$$+9/16816(-133+9a_1)(50448T^2-1260960T-162040Ta_1+23500-320375a_1)y^3T^4$$
$$+9/2554(403a_1-1559)(5108T-39620+9165a_1)y^2T^5$$
$$-135/16(7a_1+5)y(4T-100-75a_1)(5a_1-4+4T)T^5+675T^6(-8+a_1)(-16+T)$$

$$h(z)=-\bar{g}(z)$$

où la barre exprime l'action de la conjugaison complexe sur les coefficients (attention au signe moins).

$$A=y^7+(1-a_1)y^6z-2y^5z^2+(a_1+1)y^4z^3+(-a_1+2)y^3z^4-2y^2z^5+a_1yz^6+z^7$$
$$+T((7a_1-3)y^5+22y^4z-(10a_1+2)y^3z^2+(-12+10a_1)y^2z^3+22yz^4+(-7a_1+4)z^5+(5a_1+65)y^4$$
$$+(-50a_1+70)y^3z-90y^2z^2+(50a_1+20)yz^3+(-5a_1+70)z^4)+T^2((-69+9a_1)y^3+(39a_1+33)y^2z$$
$$+(72-39a_1)yz^2+(-60-9a_1)z^3+(210a_1-150)y^2+450yz+(60-210a_1)z^2$$
$$+(-45T-63a_1T+900+225a_1)y+(-108T+63a_1T+1125-225a_1)z-675T)$$

divise $g(y)-h(z)$.

5.5 Données pour $n = 21$

$$a_1^2 - a_1 + 2 = 0 \text{ et } a_2 = 1 - a_1$$

l	g
21	y^{21}
19	$(21a_1+21/2a_2)y^{19}$
18	$(21a_1+21/2a_2)y^{18}$
17	$(735/8a_1-861/16a_2)y^{17}$
16	$(777/4a_1-651/8a_2)y^{16}$
15	$(-2219/8a_1-8071/8a_2)y^{15}$
14	$(-4949/8a_1-19145/8a_2)y^{14}$
13	$(-516705/128a_1-725235/128a_2)y^{13}$
12	$(-345891/32a_1-423969/32a_2)y^{12}$
11	$(-625177/32a_1-4588885/256a_2)y^{11}$
10	$(-1251789/32a_1-6846609/256a_2)y^{10}$
9	$(-25490563/512a_1-52258213/2048a_2)y^9$
8	$(-13945715/256a_1-4008641/1024a_2)y^8$
7	$(-103106169/2048a_1+33268293/2048a_2)y^7$
6	$(-17064691/2048a_1+125391175/2048a_2)y^6$
5	$(1380474361/65536a_1+5721876405/65536a_2)y^5$
4	$(400333395/8192a_1+671121087/8192a_2)y^4$
3	$(3945694235/65536a_1+9121050141/131072a_2)y^3$
2	$(2279021283/65536a_1+4130941717/131072a_2)y^2$
1	$(8921290833/524288a_1+9205492695/1048576a_2)y$
0	$1174191921/524288a_1$

$$g(z) = \bar{h}(z)$$

où la barre exprime l'action de la conjugaison complexe sur les coefficients.

l	A
5	$(a_1+a_2)y^5+(2a_1+a_2)y^4z+2a_1y^3z^2-2a_2y^2z^3+(-a_1-2a_2)yz^4+(-a_1-a_2)z^5$
3	$(7a_1+9/2a_2)y^3+(6a_1-2a_2)y^2z+(2a_1-6a_2)yz^2+(-9/2a_1-7a_2)z^3$
2	$(3a_1+1/2a_2)y^2+(2a_1-2a_2)yz+(-1/2a_1-3a_2)z^2$
1	$(81/8a_1+55/16a_2)y+(-55/16a_1-81/8a_2)z$
0	$17/8a_1-17/8a_2$

5.6 Données pour $n = 31$

$$
\begin{aligned}
& a_1^6 + a_1^5 + 3a_1^4 + 11a_1^3 + 44a_1^2 + 36a_1 + 32 = 0 \\
a_2 &= (-3a_1^5 - 5a_1^3 - 36a_1^2 - 84a_1)/(-32) \\
a_3 &= -3/32a_1^5 - 5/32a_1^3 - 5/8a_1^2 - 25/8a_1 \\
a_4 &= -(1/32a_1^5 + 7/32a_1^3 + 3/8a_1^2 + 11/8a_1 + 1) \\
a_5 &= -(1/32a_1^5 + 1/8a_1^4 - 1/32a_1^3 + 3/4a_1^2 + 17/8a_1 + 3) \\
a_6 &= 1/16a_1^5 + 1/8a_1^4 + 3/16a_1^3 + 5/8a_1^2 + 3a_1 + 3
\end{aligned}
$$

l	g
31	y^{31}
29	$(-93/4a_1-93/2a_2-93/2a_3-93/4a_4-155/4a_5-31a_6)y^{29}$
28	$(-93/4a_1-93/2a_2-93/2a_3-93/4a_4-155/4a_5-31a_6)y^{28}$
27	$(-18631/16a_1-9889/8a_2-27745/16a_3-1767/4a_4-21111/16a_5-18073/16a_6)y^{27}$
26	$(-18693/8a_1-10075/4a_2-27807/8a_3-961a_4-21421/8a_5-18383/8a_6)y^{26}$
25	$(-1814709/64a_1-866605/32a_2-624309/16a_3-316355/64a_4-1190059/64a_5-603973/32a_6)y^{25}$
24	$(-5147395/64a_1-2518347/32a_2-1792823/16a_3-1046901/64a_4-3532605/64a_5-1786251/32a_6)y^{24}$
23	$(-48001733/128a_1-37050549/128a_2-56350033/128a_3+22124793/128a_4-19040107/256a_5-2554183/64a_6)y^{23}$
22	$(-40060401/32a_1-31160115/32a_2-47268955/32a_3+18912573/32a_4-16714301/64a_5-2271959/16a_6)y^{22}$
21	$(-4323168581/1024a_1-768047413/512a_2-1520408113/512a_3+4745553067/1024a_4+1857825257/1024a_5+747177841/256a_6)y^{21}$
20	$(-14659969905/1024a_1-2056268161/512a_2-4500771053/512a_3$ $+17346491967/1024a_4+7817974661/1024a_5+2986677485/256a_6)y^{20}$
19	$(-119843538693/4096a_1+30331029765/2048a_2+29850280897/4096a_3$ $+75706755307/1024a_4+224657788485/4096a_5+305619861293/4096a_6)y^{19}$
18	$(-138404038989/2048a_1+89781187509/1024a_2+155805874357/2048a_3$ $+33799962749/128a_4+449176714237/2048a_5+597732451225/2048a_6)y^{18}$
17	$(-414476468925/16384a_1+3866716837851/8192a_2+2053003491883/4096a_3$ $+14090945703197/16384a_4+13502889259497/16384a_5+8812618062775/8192a_6)y^{17}$
16	$(5315316005561/16384a_1+15253434724609/8192a_2+8573778338645/4096a_3$ $+43929691137559/16384a_4+45825486529419/16384a_5+29604845158317/8192a_6)y^{16}$
15	$(123724401874249/65536a_1+393485992147063/65536a_2+227876737150537/32768a_3$ $+471229666268369/65536a_4+530755953555193/65536a_5+339631984073411/32768a_6)y^{15}$
14	$(62349868655863/8192a_1+148468463917925/8192a_2+87858114193675/4096a_3$ $+150580302226759/8192a_4+183223059601663/8192a_5+116171222289461/4096a_6)y^{14}$
13	$(6011524549363305/262144a_1+6147762114076917/131072a_2+7375025018359641/131072a_3$ $+11024866503968041/262144a_4+14273754394569183/262144a_5+4490869117768911/65536a_6)y^{13}$
12	$(16305204150026913/262144a_1+14639323464803565/131072a_2+17784726128988817/131072a_3$ $+22913903349419489/262144a_4+31901094032572327/262144a_5+9950014292036055/65536a_6)y^{12}$
11	$(153365375536010163/1048576a_1+125776001332843507/524288a_2+308555926731051657/1048576a_3$ $+21836069220139675/131072a_4+260138324490043523/1048576a_5+322065388414388593/1048576a_6)y^{11}$
10	$(159315427817158941/524288a_1+120301589078562317/262144a_2+297874391879773795/524288a_3$ $+36492232937005523/131072a_4+235488295164858533/524288a_5+288986638052813187/524288a_6)y^{10}$
9	$(2383960866279742769/4194304a_1+1670519244378610509/2097152a_2+1043373236878871465/1048576a_3$ $+173880472523568906 3/4194304a_4+308827921323922375 9/4194304a_5+187629568516605146 5/2097152a_6)y^{9}$

8	$(3909655649890121055/4194304a_1+2553788590435858371/2097152a_2+160946048170541679 5/1048576a_3$ $+2212578136343562425/4194304a_4+44408357745551078 41/4194304a_5+2667046386263681375/2097152a_6)y^8$
7	$(1413668116667533179/1048576a_1+6836080785859493631/4194304a_2+1741660493820188908 5/8388608a_3$ $+2253368618313920039/4194304a_4+2199530080387681563 5/16777216a_5+1624797789450652845/1048576a_6)y^7$
6	$(1779509082135132243/1048576a_1+1980436569083562397/1048576a_2+5107310888752124013/2097152a_3$ $+6500120884756193/16384a_4+5777081177663442527/4194304a_5+83434368417710104 1/524288a_6)y^6$
5	$(1206135287949284242 49/67108864a_1+6046963244569167969 3/33554432a_2+7927818421802867200 5/33554432a_3$ $5406069368367483913/67108864a_4+7563294488341077937 9/67108864a_5+2095187156665027899 1/16777216a_6)y^5$
4	$(1054372181954717452 29/67108864a_1+4567312309263985764 9/33554432a_2+6144767276259268384 9/33554432a_3$ $-1992206971755022697 9/67108864a_4+4204166343273576923 1/67108864a_5+1039353926325989865 1/16777216a_6)y^4$
3	$(2872684981963774558 41/268435456a_1+9859243006414934132 5/134217728a_2+2783556027824871635 59/268435456a_3$ $-893294813838853246 5/16777216a_4+2796656331252664508 7/268435456a_5-690820172352427845/268435456a_6)y^3$
2	$(6706283646869925696 5/134217728a_1+1193233612816686892 9/67108864a_2+4076723782446745008 7/134217728a_3$ $-1784665931871489658 5/33554432a_4+-3059836463847456491 7/134217728a_5-4903380422444758100 5/134217728a_6)y^2$
1	$(1448342736488180202 89/1073741824a_1-2717734021507543529 1/536870912a_2-6906651209500627567/268435456a_3$ $-335786885114830486657/1073741824a_4-2434251647314590110 21/1073741824a_5-1696764637056841597 07/536870912a_6)y$
0	$5084108308340531763 5/536870912a_1+4000065255742729721 3/1073741824a_2+3297366436634701777 5/536870912a_3$

$$g(z) = \bar{h}(z)$$

où la barre exprime l'action de la conjugaison complexe sur les coefficients.

Références

[1] N. M. Adrianov. Classification des groupes cartographiques primitifs des arbres plans, en Russe. *Fundamental'naya i prikladnaya matematika*, 3, 1997.

[2] N.M. Adrianov, Yu. Kotchetkov, and A.D. Souvorov. Arbres planaires avec des groupes cartographiques exceptionnels. *preprint en Russe*, 1997.

[3] C. Batut, K. Belabas, D. Bernardi, H. Cohen, and M. Olivier. *User's guide to PARI-GP*. Université de Bordeaux, 1996.

[4] Geo. D. Birkhoff and H. S. Vandiver. On the integral divisors of $a^n - b^n$. *Annals of Math.*, 5: 173–180, 1903.

[5] W. Bosma, J. Cannon, C. Playhost, and alii. *Magma reference manual*. http://www.maths.usyd.edu.au, 1997.

[6] W. Burnside. On simply transitive groups of prime degree. *Quart. J. Math.*, 37: 215–221, 1906.

[7] R.D. Carmichael. *Introduction to the theory of groups of finite order*. Ginn, Boston, 1937.

[8] J.W.S. Cassels. Factorization of polynomials in several variables. In *Proceedings of the 15th Scandinavian Congress, Oslo*, volume 118 of *Lecture Notes in Math.*, pages 1–17. Springer, 1968.

[9] B.W. Char, K.O. Geddes, G.H. Gonnet, B.L. Leong, M.B. Monagan, and S.M. Watt. *Maple V language reference manual*. Springer, 1991.

[10] Claude Chevalley. Thèses. *Faculté des sciences de l'Université de Paris*, 1934.

[11] J. Conway, R. Curtis, S. Norton, R. Parker, and R. Wilson. *Atlas of finite groups*. Clarendon Press, 1985.

[12] C.W. Curtis, W.M. Kantor, and G.M. Seitz. The 2-transitives permutations representations of the finite Chevalley groups. *Trans. Amer. Math. Soc.*, 218: 1–59, 1976.

[13] H. Davenport, D.J. Lewis, and A. Schinzel. Equations of the form $f(x) = g(y)$. *Quart. J. Math. Oxford*, 12: 304–312, 1961.

[14] H. Davenport and A. Schinzel. Two problems concerning polynomials. *J. Reine Angew Math.*, 214: 386–391, 1964.

[15] P. Dembowski. *Finite Geometries*. Springer, 1968.

[16] D. Dixon. *The structure of linear groups*. Van Nostrand Reinhold Company, 1971.

[17] Leila Schneps edt. *The theory of Grothendieck's dessins d'enfant*. Cambridge University Press, 1994.

[18] Walter Feit. Automorphisms of symmetric balanced incomplete block designs. *Math. Z.*, 118: 40–49, 1970.

[19] Walter Feit. On symmetric balanced incomplete block designs with doubly transitive automorphism groups. *Journal of Combinatorial Theory (A)*, 14: 221–247, 1973.

[20] Walter Feit. Some consequences of the classification of finite simple groups. *Proceedings of Symposia in Pure Math.*, 37: 175–181, 1980.

[21] Michael Fried. On a conjecture of Schur. *Michigan Math. J.*, 17: 41–55, 1970.

[22] Michael Fried. The field of definition of function fields and a problem in the reducibility of polynomials in two variables. *Illinois J. Math.*, 17: 128–146, 1973.

[23] Michael Fried. Exposition on an arithmetic-group theoretic connection via Riemann's existence theorem. *Proceedings of Symposia in Pure Math.*, 37: 571–602, 1980.

[24] Serge Lang. *Algebra, second edition.* Addison-Wesley, 1984.

[25] Jr. Marshall Hall. *The theory of Groups.* The Macmillan company, 1959.

[26] P. Müller. Primitive monodromy groups for polynomials. In M. Fried, editor, *Recent Developments in the Inverse Galois Problem*, volume 186 of *Contemporary Math.*, pages 385–401. AMS, 1995.

[27] Herbert John Ryser. *Combinatorial Mathematics.* John Wiley and Sons, 1963.

[28] I. Schur. Zur theorie der einfach transitiven permutationsgruppen. *Preuss. Akad. Wiss., Phys.-Math. Kl.*, pages 598–623, 1933.

[29] James Singer. A theorem in finite projective geometry and some applications to number theory. *Trans. Amer. Math. Soc.*, 43: 377–385, 1938.

[30] J. A. Todd. A combinatorial problem. *J. Math. Phys. Mass. Inst. Tech.*, 12: 321–333, 1933.