Graphes expanseurs

Laurent Demonet et Camille Wormser

sujet proposé par Yves Benoist

1er juillet 2002

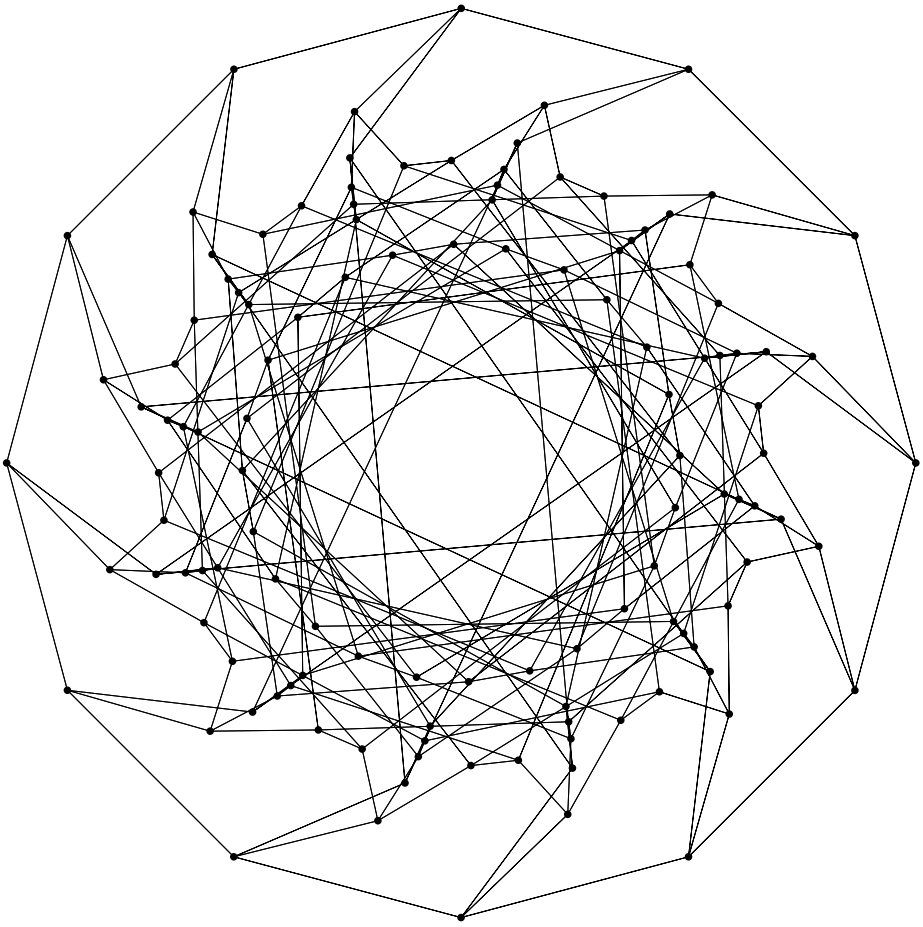

Table des matières

Introduction **3**

1 Graphes **3**
1.1 Graphes expanseurs 3
1.2 Graphes de Cayley 6

2 Sommes de deux carrés **6**

3 Représentations de groupes **8**

4 Étude de $\mathrm{PSL}_2(\mathbb{F}_q)$ **13**
4.1 Propriétés du groupe $\mathrm{PSL}_2(\mathbb{K})$ 13
4.2 Propriétés du groupe $\mathrm{PSL}_2(\mathbb{F}_q)$ 15
4.3 Représentations de $\mathrm{PSL}_2(\mathbb{F}_q)$ 18

5 Quaternions **20**
5.1 Définition des quaternions 20
5.2 Sommes de quatre carrés 21
5.3 Quaternions irréductibles 24
5.4 Groupe libre sur une famille de quaternions 25

6 Construction des graphes $Y_{p,q}$ **26**
6.1 Définitions 27
6.2 Estimations spectrales 29

L'illustration de la page précédente représente le graphe $Y_{3,5}$.

Introduction

Une famille de graphes expanseurs est une famille de graphes vérifiant asymptotiquement de bonnes propriétés de connexité, au sens exposé dans le paragraphe 1.1. Une de leurs applications éventuelles est l'organisation de réseaux en informatique.

On peut démontrer l'existence de telles familles par un argument de dénombrement (cf. [2], page 5).

Cet exposé présente, en suivant [1], une construction explicite d'une famille de graphes expanseurs. Cette question a été résolue successivement à l'aide de la propriété (T) de Kazhdan par Margulis (cf. [3]), puis grâce à l'étude de formes modulaires (cf. [4] et [5]) et enfin par les méthodes élémentaires présentées dans [1], que nous exposons.

1 Graphes

Soit G un graphe fini, et A sa matrice d'adjacence, telle que A_{ij} soit le nombre d'arêtes reliant les sommets i et j. Dans toute la suite, on ne considèrera que des graphes k-réguliers, i.e. tels que chaque sommet soit l'extrémité de k arêtes. De plus, les vecteurs sur lesquels la matrice agit seront représentés comme des fonctions de l'ensemble V des sommets dans $\mathbb{C}$. Posons donc $\ell^2(V) = \{f : V \to \mathbb{C}\}$, muni du produit scalaire hermitien usuel.

1.1 Graphes expanseurs

La matrice d'adjacence A est symétrique. Notons $\mu_0 \geqslant \mu_1 \geqslant \cdots \geqslant \mu_{n-1}$ ses valeurs propres, où n est le nombre de sommets du graphe.

Proposition 1 : *Si G est un graphe k-régulier à n sommets, alors*

(i) $\mu_0 = k$;

(ii) $|\mu_i| \leqslant k$ *si* $1 \leqslant i \leqslant n-1$;

(iii) μ_0 *est de multiplicité* 1 *si, et seulement si, G est connexe.*

Soit V l'ensemble des sommets de G, et E l'ensemble de ses arêtes. Si $F \subset V$, on notera ∂F le sous-ensemble de E composé des arêtes ayant une extrémité dans F et l'autre dans $V \setminus F$.

Définition : La *systole* de G est

$$g(G) = \text{longueur du plus court circuit dans } G,$$

où l'on appelle circuit tout lacet non trivial.

Proposition 2 : *Soit G un graphe k-régulier fini, et V l'ensemble de ses sommets. Si $k \geqslant 3$, on a*

$$g(G) < 2 + 2\log_{k-1}|V|.$$

Démonstration : Soit v_0 l'un des sommets de G, et B la boule de centre v_0 et de rayon $r = \lfloor (g(G)-1)/2 \rfloor$ (la « distance » entre deux sommets de G étant

la longueur du plus court chemin les reliant). Par définition de $g(G)$, B est une boule (en particulier connexe) qui ne comporte pas de cycle. Il s'agit donc en fait de la boule de rayon r de l'arbre k-régulier, dont on calcule facilement le cardinal :

$$|B| = 1 + k\frac{(k-1)^r - 1}{k-2}$$

En écrivant que $\log_{k-1}|V| \geqslant \log_{k-1}|B|$, on obtient $g(G) \leqslant 2 + 2\log_{k-1}|V|$. $\square$

Définition : La *constante isopérimétrique* de G est

$$h(G) = \inf\left\{\frac{|\partial F|}{\min\{|F|, |V \setminus F|\}} : F \subset V,\ 0 < |F| < +\infty\right\}.$$

Définition : Soit $(X_m)_{m\geqslant 1}$ une famille de graphes connexes k-réguliers telle que $|V_m| \to +\infty$ quand $m \to +\infty$. La famille $(X_m)_{m\geqslant 1}$ est une *famille d'expanseurs* s'il existe $\varepsilon > 0$ tel que $h(X_m) \geqslant \varepsilon$ pour tout $m \geqslant 1$.

Théorème 3 : *Soit $G = (V, E)$ un graphe fini, connexe, k-régulier et sans boucles. On a alors*

$$\frac{k - \mu_1}{2} \leqslant h(G) \leqslant \sqrt{2k(k-\mu_1)}.$$

Démonstration : Fixons arbitrairement une orientation de G. Si $f \in \ell^2(V)$, on définit $df \in \ell^2(E)$ par $df(e) = f(e^+) - f(e^-)$, où e^- et e^+ sont respectivement l'origine et l'extrémité de e. On note $d^* : \ell^2(E) \to \ell^2(V)$, l'adjoint de d pour les produits scalaires hermitiens, et $\Delta = d^*d$. On calcule alors que $\Delta = k\cdot\mathrm{Id} - A$. Si $f \in \ell^2(V)$ est orthogonale aux fonctions constantes, i.e. au premier sous-espace propre, on obtient, en décomposant dans une base de vecteurs propres

$$\|df\|^2 = (\Delta f | f) \geqslant (k - \mu_1)\|f\|^2.$$

Soit maintenant $F \subset V$. On définit alors f_F par

$$f_F(x) = \begin{cases} |V - F| & \text{si } x \in F\ ; \\ -|F| & \text{si } x \notin F. \end{cases}$$

Dès lors, f_F est orthogonale aux fonctions constantes, et comme

$$\|f_F\|^2 = |F|\,|V \setminus F|\,|V|$$
$$\|df_F\|^2 = |V|^2|\partial F|$$

on obtient, d'après l'inégalité précédente que

$$\frac{|\partial F|}{|F|} \geqslant (k - \mu_1)\frac{|V \setminus F|}{|V|}.$$

Enfin, par symétrie, on peut supposer que $|F| \leqslant |V|/2$, si bien que $|\partial F|/|F| \geqslant (k - \mu_1)/2$, et donc $h(G) \geqslant (k - \mu_1)/2$.

Pour démontrer la seconde inégalité, étant donné une fonction f positive, on définit

$$B_f = \sum_{e\in E} |f(e^+)^2 - f(e^-)^2|.$$

Notons alors $\beta_r > \beta_{r-1} > \cdots > \beta_1 > \beta_0$ les valeurs de f, posons $L_i = \{x \in V : f(x) \geqslant \beta_i\}$ pour $0 \leqslant i \leqslant r$ et $f(e^+) = \beta_{i_{e^+}}$, $f(e^-) = \beta_{i_{e^-}}$. On a alors les égalités suivantes :

$$\begin{aligned} B_f &= \sum_{e\in E} |f(e^+)^2 - f(e^-)^2| \\ &= \sum_{e\in E} \left(\sum_{k=i_{e^-}+1}^{i_{e^+}} ({\beta_k}^2 - {\beta_{k-1}}^2) \right) \\ &= \sum_{k=1}^{r} |\{e \in E : i_{e^-} < k \leqslant i_{e^+} + 1\}| ({\beta_k}^2 - {\beta_{k-1}}^2) \\ &= \sum_{k=1}^{r} |\partial L_k| ({\beta_k}^2 - {\beta_{k-1}}^2) \end{aligned}$$

De plus, l'inégalité de Cauchy-Schwarz appliquée deux fois donne

$$B_f = \sum_{e\in E} |f(e^+) + f(e^-)| \cdot |f(e^+) - f(e^-)| \leqslant \sqrt{2k}\|f\|\|df\|.$$

Soit maintenant une fonction f telle que $|\mathrm{supp}(f)| = |\{x \in V : f(x) \neq 0\}| \leqslant |V|/2$. On a alors $B_f \geqslant h(X)\|f\|^2$. En effet, une transformation d'Abel donne les inégalités suivantes :

$$\begin{aligned} B_f &\geqslant h(X) \sum_{i=1}^{r} |L_i| ({\beta_i}^2 - {\beta_{i-1}}^2) \\ &= h(X) \left(|L_r| {\beta_r}^2 + \sum_{i=1}^{r-1} (|L_i| - |L_{i+1}|) {\beta_i}^2 \right) \\ &= h(X)\|f\|^2 \end{aligned}$$

Enfin, soit g une fonction associée à la valeur propre $k - \mu_1$ de Δ, et $f = \max(g, 0)$. Quitte à changer g en $-g$, on peut supposer que $|\mathrm{supp}(f)| \leqslant |V|/2$ (cependant, f est non nulle, car g est orthogonale à la fonction constante égale à 1). On a les inégalités

$$h(X)\|f\|^2 \leqslant B_f \leqslant \sqrt{2k}\|f\|\|df\|.$$

Reste à calculer $\|df\|$. On a, si $g(x) > 0$

$$\begin{aligned} (\Delta f)(x) = kf(x) - \sum_{y\in V} A_{xy} f(y) &= kg(x) - \sum_{g(y)>0} A_{xy} g(y) \\ \leqslant kg(x) - \sum_{y\in V} A_{xy} g(y) &= (\Delta g)(x) = (k - \mu_1) g(x). \end{aligned}$$

D'où il vient $\|df\|^2 \leqslant (k-\mu_1)\|f\|^2$, si bien que l'encadrement de B_f donne $h(X) \leqslant \sqrt{2k(k-\mu_1)}$. □

Pour montrer qu'une famille de graphes est une famille d'expanseurs, nous étudierons donc le comportement asymptotique du *trou spectral* $k - \mu_1$.

1.2 Graphes de Cayley

Soit G un groupe et S une partie finie non-vide et symétrique (i.e. telle que $S = S^{-1}$) de G.

Définition : Le *graphe de Cayley* $\mathcal{G}(G,S)$ est le graphe dont les sommets sont les éléments de G et dont l'ensemble des arêtes est

$$E = \{\{x,y\} : x,y \in G; \exists s \in S : y = xs\}.$$

On a maintenant quelques propriétés élémentaires.

Proposition 4 : *Soit $\mathcal{G}(G,S)$ un graphe de Cayley. Posons $k = |S|$. On a alors*

(i) $\mathcal{G}(G,S)$ est un graphe k-régulier, sur les sommets duquel ses automorphismes agissent transitivement ;

(ii) $\mathcal{G}(G,S)$ est connexe si, et seulement si, S engendre G.

2 Sommes de deux carrés

Par la suite, $r_k(n)$ désignera le nombre de décompositions de n en somme de k carrés de nombres entiers *relatifs*.

Proposition 5 : *Un entier $n \in \mathbb{N}$ s'écrit comme somme de deux carrés (i.e. $r_2(n) > 0$) si, et seulement si, pour tout nombre premier p congru à 3 modulo 4, la p-valuation de n est paire.*

De façon plus générale, on a la proposition suivante sur les irréductibles de $\mathbb{Z}[i]$.

Proposition 6 : *Un nombre $\pi \in \mathbb{Z}[i]$ est irréductible si, et seulement s'il vérifie l'une des trois propriétés suivantes :*

(i) $N(\pi) = 2$;

(ii) $N(\pi) = p$, où p est premier, avec $p \equiv 1 \pmod 4$;

(iii) $\pi = \varepsilon q$, où ε est inversible et q premier, avec $q \equiv 3 \pmod 4$.

On notera $d_i(n)$ le nombre de diviseurs de n congrus à i modulo 4, et $d(n)$ le nombre de diviseurs de n.

Le théorème suivant est dû à Legendre.

Théorème 7 : *Si $n \in \mathbb{N}^*$, $r_2(n) = 4(d_1(n) - d_3(n))$.*

Démonstration : Soit $n > 0$. Posons $\delta(n) = d_1(n) - d_3(n)$. Dans un premier temps, on suppose n impair et on le décompose en $n = km$, avec

$$k = \prod_{h=1}^{a} {p_h}^{r_h} \quad p_h \text{ premier et } p_h \equiv 1 \pmod 4,$$

$$m = \prod_{j=1}^{b} {q_j}^{s_j} \quad q_j \text{ premier et } q_j \equiv 3 \pmod 4.$$

Il vient alors $\delta(n) = d(k)\delta(m)$. Or δ est donné par

$$\delta(m) = \begin{cases} 0 & \text{si au moins l'un des } s_j \text{ est impair ;} \\ 1 & \text{si } m \text{ est un carré.} \end{cases}$$

En effet, posons $m' = m/{q_1}^{s_1}$. Supposons que s_1 soit impair. On a alors

$$d_1(m) = \frac{s_1+1}{2} d_1(m') + \frac{s_1+1}{2} d_3(m') = d_3(m).$$

Si, en revanche, m est un carré,

$$d_1(m) = \left(\frac{s_1}{2}+1\right) d_1(m') + \frac{s_1}{2} d_3(m')$$

$$d_3(m) = \frac{s_1}{2} d_1(m') + \left(\frac{s_1}{2}+1\right) d_3(m'),$$

si bien que $\delta(m) = \delta(m')$, et comme $\delta(1) = 1$, $\delta(m) = 1$.
On obtient donc que

$$\delta(n) = \begin{cases} d(k) & \text{si } m \text{ est un carré} \\ 0 & \text{sinon} \end{cases}$$

Revenons maintenant au cas général. On écrit $n = 2^t N$, avec $N = km$ comme précédemment. On a alors $\delta(n) = \delta(N)$. Si m n'est pas un carré, le théorème est vrai d'après la proposition 5. Sinon, cette proposition donne que $r_2(n) > 0$. Dans ce cas, décomposons n en facteurs premiers dans $\mathbb{Z}[i]$ (rappelons que $\mathbb{Z}[i]$ est factoriel) :

$$n = (-i)^t (1+i)^{2t} \prod_{h=1}^{a} \pi_h^{r_h} \overline{\pi}_h^{r_h} \prod_{j=1}^{b} q_j^{s_j}$$

où π_h est un irréductible tel que $N(\pi_h) = p_h$. Comptons le nombre de factorisations de n sous la forme $n = (A+iB)(A-iB)$ en utilisant le fait que $\mathbb{Z}$ est factoriel. Si $n = (A+iB)(A-iB)$, on a nécessairement

$$A + iB = \varepsilon (1+i)^t \prod_{h=1}^{a} \pi_h^{t_h} \overline{\pi}_h^{u_h} \prod_{j=1}^{b} q_j^{\frac{s_j}{2}}$$

$$A - iB = \varepsilon' (1+i)^t \prod_{h=1}^{a} \pi_h^{u_h} \overline{\pi}_h^{t_h} \prod_{j=1}^{b} q_j^{\frac{s_j}{2}}$$

où ε et ε' sont des inversibles et $t_h + u_h = r_h$ pour $1 \leqslant h \leqslant a$. Le nombre de choix possibles de $A+iB$ est donc le nombre de choix de ε et des t_h. On a donc finalement

$$4 \prod_{h=1}^{a} (r_h + 1) = 4d(k) = 4\delta(N) = 4\delta(n).$$

□

Lemme 8 : *Pour tout* $\varepsilon > 0$,

$$d(n) = O(n^{\varepsilon}).$$

Démonstration : Si $n = \prod_{i=1}^{k} p_i^{\nu_i}$ où les p_i sont des nombres premiers distincts et les ν_i sont non nuls, alors :

$$d(n) = \prod_{i=1}^{k} (\nu_i + 1)$$

et, comme $\forall x > 0, \log(x+1) < \sqrt{x}$,

$$\frac{\log d(n)}{\log n} \leqslant \frac{\sum_{i=1}^{k} \sqrt{\nu_i}}{\sum_{i=1}^{k} \nu_i \log p_i}$$

Puis, en utilisant l'inégalité de Schwartz,

$$\frac{\log d(n)}{\log n} \leqslant \frac{\sum_{i=1}^{k} \sqrt{\nu_i}}{\frac{1}{k}\left(\sum_{i=1}^{k} \sqrt{\nu_i \log p_i}\right)^2} \leqslant \frac{k}{\sqrt{\log 2} \sum_{i=1}^{k} \sqrt{\nu_i \log p_i}}.$$

Soit $A > 0$, si

$$\frac{\sqrt{\log 2} \sum_{i=1}^{k} \sqrt{\nu_i \log p_i}}{k} < A$$

alors en particulier la moyenne des $\sqrt{\log p_i}$ est majorée et comme les p_i sont des nombres premiers tous différents, il existe $K \in \mathbb{N}$ qui ne dépend que de A tel que $k \leqslant K$; de même il existe P et ν ne dépendant que de A tels que tous les p_i soient majorés par P et tous les ν_i par ν. On en déduit que $n \leqslant P^{K\nu}$ donc $\log_n d(n)$ tend vers 0 quand n tend vers l'infini. Ceci achève la démonstration. □

Corollaire 9 : *Pour tout* $\varepsilon > 0$,

$$r_2(n) = O\left(n^{\varepsilon}\right).$$

Corollaire 10 : *Pour tout* $\varepsilon > 0$,

$$r_3(n) = O\left(n^{\frac{1}{2}+\varepsilon}\right).$$

3 Représentations de groupes

On présente ici des rappels de théorie des représentations.

Définition : Soit G un groupe. Une *représentation* de G est une paire (π, V), où V est un espace vectoriel complexe et π un morphisme de G dans $\mathrm{GL}(V)$. Le *degré* de (π, V) est la dimension de V.

Nous ne considérerons par la suite que des représentations de degré fini.

Définition : Soit (π, V) une représentation d'un groupe G. Un sous-espace W de V est *stable* par π si, pour tout $g \in G$, $\pi(g)W = W$.

Si W est un sous-espace de V stable par π, on dit que $(\pi|_W, W)$ est une *sous-représentation* de V. Les sous-espaces 0 et V de V sont trivialement stables par π.

Définition : Une représentation (π, V) est *irréductible* si elle n'admet pas de sous-espace stable non-trivial.

Définition : Soient (π, V) et (ρ, W) deux représentations de G. Un morphisme de représentations de π vers ρ est une application linéaire $T : V \to W$ telle que, pour tout $g \in G$, le diagramme suivant commute :

$$\begin{array}{ccc} V & \xrightarrow{T} & W \\ {\scriptstyle \pi(g)}\downarrow & & \downarrow{\scriptstyle \rho(g)} \\ V & \xrightarrow{T} & W \end{array}$$

L'espace vectoriel des morphismes de π vers ρ sera noté $\mathrm{Hom}_G(\pi, \rho)$. Deux représentations sont *équivalentes* s'il existe un isomorphisme de l'une vers l'autre.

On démontre facilement le lemme suivant.

Lemme 11 : *Soient (π, V) et (ρ, W) deux représentations irréductibles de G (de degré fini). Alors,*

$$\dim \mathrm{Hom}(\pi, \rho) = \begin{cases} 1 & \text{si } \pi \text{ et } \rho \text{ sont équivalentes ;} \\ 0 & \text{sinon.} \end{cases}$$

On définit naturellement la somme directe et le produit tensoriel de deux représentations. De plus, si (π, V) est une représentation, on note $V^* = \mathrm{Hom}(V, \mathbb{C})$ l'espace dual de V et on définit la représentation duale de (π, V), notée (π^*, V^*) par

$$(\pi^*(g)f)(x) = f(\pi(g^{-1})x) \quad (g \in G, x \in V, f \in V^*).$$

Soient maintenant (π, V) et (ρ, W) deux représentations de G. Considérons la représentation $(\sigma, \mathrm{Hom}(V, W))$ définie par

$$\sigma(g)T = \rho(g)T\pi(g^{-1}) \quad (g \in G, T \in \mathrm{Hom}(V, W)).$$

Proposition 12 : *La représentation σ est équivalente à la représentation $\rho \otimes \pi^*$.*

Démonstration : Si $f \in V^*$ et $w \in W$, on définit $\theta_{w,f} \in \mathrm{Hom}(V, W)$ par

$$\theta_{w,f}(v) = f(v)w \quad (v \in V).$$

L'application $(w, f) \mapsto \theta_{w,f}$ est bilinéaire, et induit donc $B : W \otimes V^* \to \mathrm{Hom}(V, W)$. Clairement, B est surjective. Par dimension, B est un isomorphisme. On a alors, pour $g \in G$, $w \in W$ et $f \in V^*$,

$$\sigma(g)\theta_{w,f} = \theta_{\rho(g)w, \pi^*(g)f} = B(\rho(g)w \otimes \pi^*(g)f).$$

Ainsi, $B \in \mathrm{Hom}(\rho \otimes \pi^*, \sigma)$ et B est un isomorphisme. □

Proposition 13 : *Soit (π, V) une représentation d'un groupe fini G. Alors,*

(i) il existe un produit scalaire hermitien sur V invariant sous l'action de G ;

(ii) tout sous-espace W invariant par π admet un supplémentaire invariant ;

(iii) si $V \neq 0$, π est équivalente à une somme directe de représentations irréductibles de G.

Démonstration : Soit $(\cdot|\cdot)$ un produit scalaire hermitien sur V. On définit

$$\langle v_1 | v_2 \rangle = \sum_{g \in G} (\pi(g)v_1 | \pi(g)v_2) \quad (v_1, v_2 \in V).$$

Le produit scalaire $\langle \cdot | \cdot \rangle$ convient. Le point (i) est démontré, et les deux autres en découlent. □

Si (π, V) une représentation d'un groupe G, on note V^G l'ensemble des points fixes sous l'action de G.

Proposition 14 : *Soit (π, V) une représentation d'un groupe fini G. On définit $P_\pi = \frac{1}{|G|} \sum_{g \in G} \pi(g)$. Alors,*

(i) P_π est un idempotent de $\mathrm{End}\, V$;

(ii) pour tout $g \in G$, $\pi(g)P_\pi = P_\pi \pi(g) = P_\pi$;

(iii) $\mathrm{Im}\, P_\pi = V^G$;

(iv) $\frac{1}{|G|} \sum_{g \in G} \mathrm{Tr}\, \pi(g) = \dim V^G$.

Démonstration :

(i) Le résultat résulte de la transitivité de la translation dans le groupe.

(ii) On démontre ce point de la même façon que le précédent.

(iii) Comme P_π est un idempotent, $\mathrm{Im}\, P_\pi = \{v \in V : P_\pi(v) = v\}$ et d'après le point précédent,
$$\mathrm{Im}\, P_\pi = V^G.$$

(iv) La trace d'un idempotent est égale à son rang, d'où le résultat. □

Définition : Soit (π, V) une représentation de G. Le *caractère* de π est la fonction $\chi_\pi : G \to \mathbb{C} : g \mapsto \mathrm{Tr}\, \pi(g)$.

Proposition 15 : *Soient (π, V) et (ρ, W) deux représentations de G. Alors,*

(i) $\chi_{\pi^*}(g) = \chi_\pi(g^{-1})$, pour tout $g \in G$;

(ii) $\chi_{\pi \oplus \rho} = \chi_\pi + \chi_\rho$;

(iii) $\chi_{\pi \otimes \rho} = \chi_\pi \chi_\rho$;

(iv) si π et ρ sont équivalentes, $\chi_\pi = \chi_\rho$.

Démonstration :

(i) Si B est une base de V et B^* sa base duale, la matrice de $\pi^*(g)$ dans la base B^* est la transposée de celle de $\pi(g^{-1})$ dans la base B.

(ii) Ce point est évident.

(iii) Si $(\pi(g)_{ik})_{1\leqslant i,k\leqslant m}$ et $(\rho(g)_{jl})_{1\leqslant j,l\leqslant n}$ sont les matrices de $\pi(g)$ et $\rho(g)$ dans les bases B et C respectivement, alors $(\pi(g)_{ik}\rho(g)_{jl})$ est la matrice de $\pi(g)\otimes\rho(g)$ dans la base $B\otimes C$. On a donc

$$\chi_{\pi\otimes\rho}(g) = \sum_{i=1}^{m}\sum_{j=1}^{n}\pi(g)_{ii}\rho(g)_{jj} = \left(\sum_{i=1}^{m}\pi(g)_{ii}\right)\left(\sum_{j=1}^{n}\rho(g)_{jj}\right) = \chi_\pi(g)\chi_\rho(g).$$

(iv) Soit $T\in\mathrm{Hom}(\pi,\rho)$ inversible. On a alors $\chi_\rho(g) = \mathrm{Tr}(T\pi(g)T^{-1}) = \mathrm{Tr}(\pi(g)) = \chi_\pi(g)$. □

Lemme 16 : *Soit (π,V) une représentation d'un groupe fini G. Alors,*

(i) $\chi_\pi(1) = \dim V$;

(ii) $\chi_\pi(g) = \overline{\chi_\pi(g^{-1})}$, *pour tout* $g\in G$;

(iii) $\chi_\pi(g) = \chi_\pi(hgh^{-1})$, *pour tous* $g,h\in G$.

Démonstration :

(i) C'est évident.

(ii) D'après la proposition 13, il existe un produit scalaire $\langle\cdot|\cdot\rangle$ invariant par π. Dès lors, si $(e_1,\ldots,e_n)$ est une base orthonormée pour ce produit scalaire, on a :

$$\chi_\pi(g^{-1}) = \sum_{i=1}^{n}\langle\pi(g^{-1})e_i|e_i\rangle = \sum_{i=1}^{n}\langle e_i|\pi(g)e_i\rangle = \sum_{i=1}^{n}\overline{\langle\pi(g)e_i|e_i\rangle} = \overline{\chi_\pi(g)}$$

(iii) Ce point résulte des propriétés de la trace. □

Définissons maintenant le produit scalaire de deux fonctions $f_1, f_2 : G\to\mathbb{C}$ par

$$\langle f_1|f_2\rangle_G = \frac{1}{|G|}\sum_{g\in G} f_1(g)\overline{f_2(g)}.$$

Théorème 17 : *Soient (π,V) et (ρ,W) deux représentations d'un groupe fini G. Alors, $\langle\chi_\rho|\chi_\pi\rangle_G = \dim\mathrm{Hom}(\pi,\rho)$.*

Démonstration : Calculons ce produit scalaire :

$$\begin{aligned}
\langle \chi_\rho | \chi_\pi \rangle_G &= \frac{1}{|G|} \sum_{g \in G} \chi_\rho(g) \overline{\chi_\pi(g)} \\
&= \frac{1}{|G|} \sum_{g \in G} \chi_\rho(g) \chi_\pi(g^{-1}) && \text{(d'après le lemme 16)} \\
&= \frac{1}{|G|} \sum_{g \in G} \chi_\rho(g) \chi_{\pi^*}(g) && \text{(d'après la proposition 15)} \\
&= \frac{1}{|G|} \sum_{g \in G} \chi_{\rho \otimes \pi^*}(g) && \text{(d'après la proposition 15)} \\
&= \frac{1}{|G|} \sum_{g \in G} \mathrm{Tr}(\rho \otimes \pi^*)(g) \\
&= \dim (W \otimes V^*)^G && \text{(d'après la proposition 14)}
\end{aligned}$$

D'après la proposition 12, la représentation $\rho \otimes \pi^*$ est équivalente à la représentation σ sur $\mathrm{Hom}(V, W)$ définie par

$$\sigma(g)(T) = \rho(g) T \pi(g^{-1}) \quad (T \in \mathrm{Hom}(V, W), g \in G).$$

Ainsi, $T \in \mathrm{Hom}(V, W)$ est un point fixe de G si, et seulement si, $T \in \mathrm{Hom}(\pi, \rho)$. On a donc

$$\dim (W \otimes V^*)^G = \dim \mathrm{Hom}(V, W)^G = \dim \mathrm{Hom}(\pi, \rho).$$

Cela démontre le théorème. □

Ce théorème admet quelques corollaires :

Proposition 18 : *Soit (π, V) une représentation d'un groupe fini G, et (ρ, W) une représentation irréductible fixée. Le nombre de représentations équivalentes à ρ dans une décomposition de π en somme de représentations irréductibles est égal à $\langle \chi_\pi | \chi_\rho \rangle$.*

Proposition 19 : *Soit (π, V) une représentation d'un groupe fini G, supposée non nulle. La représentation π est irréductible si, et seulement si, $\langle \chi_\pi | \chi_\pi \rangle = 1$.*

Proposition 20 : *Soit $(\rho_1, W_1), \ldots, (\rho_h, W_h)$ la liste des représentations irréductibles du groupe fini G. Notons $n_i = \dim W_i$ le degré de ρ_i. On a alors $|G| = \sum_{i=1}^h n_i^2$.*

Démonstration : Soit $\ell^2(G)$ l'espace vectoriel des fonctions sur G à valeurs dans $\mathbb{C}$. On note $(\lambda_G, \ell^2(G))$ la représentation définie par $(\lambda_G(g)f)(x) = f(g^{-1}x)$. En considérant la base $(\delta_g)_{g \in G}$ de $\ell^2(G)$, on obtient que $\chi_{\lambda_G} = |G| \delta_1$. On a donc

$$\langle \chi_{\lambda_G} | \chi_{\rho_i} \rangle_G = \frac{1}{|G|} \sum_{g \in G} |G| \delta_1(g) \overline{\mathrm{Tr}\, \rho_i(g)} = \overline{\mathrm{Tr}\, \rho_i(1)} = n_i.$$

Ainsi, $\chi_{\lambda_G} = \sum_{i=1}^h n_i \chi_{\rho_i}$. En évaluant cette égalité en l'identité, on obtient le résultat attendu. □

Soit X un ensemble fini et G un groupe fini agissant sur X. On note $\ell^2(X)$ l'espace vectoriel des fonctions sur X à valeurs dans $\mathbb{C}$. On note $(\lambda_X, \ell^2(X))$ la représentation définie par $(\lambda_X(g)f)(x) = f(g^{-1}x)$. Soit λ_X^0 la restriction au sous-espace de co-dimension 1

$$W_0 = \left\{ f \in \ell^2(X) : \sum_{x \in X} f(x) = 0 \right\}.$$

Proposition 21 : *Si G agit de façon 2-transitive sur X, alors λ_X^0 est une représentation irréductible de G.*

Démonstration : Par 2-transitivité, l'action de G sur X^2 a 2 orbites, la diagonale Δ et son complémentaire $X^2 \setminus \Delta$. Comme les éléments de $\ell^2(X^2)^G$ sont les fonctions constantes sur les orbites de G, on a

$$\begin{aligned} 2 &= \dim \ell^2(X^2)^G \\ &= \frac{1}{|G|} \sum_{g \in G} \chi_{\lambda_{X^2}}(g) \qquad \text{(d'après la proposition 14).} \end{aligned}$$

De plus, l'isomorphisme (par dimension et surjectivité) $\ell^2(X) \otimes \ell^2(X) \to \ell^2(X^2)$: $f_1 \otimes f_2 \mapsto f_1 f_2$ est un morphisme entre les représentations $\lambda_X \otimes \lambda_X$ et λ_{X^2}. Elles sont donc équivalentes, d'où $\chi_{\lambda_{X^2}} = \chi^2_{\lambda_X}$. Ainsi,

$$2 = \frac{1}{|G|} \sum_{g \in G} \chi^2_{\lambda_X}(g) = \langle \chi_{\lambda_X} | \chi_{\lambda_X} \rangle_G$$

car il est clair que χ_{λ_X} est à valeurs réelles. De plus, la représentation λ_X se décompose en somme directe de λ_X^0 et de la représentation de degré 1 sur les fonctions constantes sur X. On a donc $\chi_{\lambda_X} = \chi_{\lambda_X^0} + 1$. Si l'on injecte cela dans l'égalité précédente, on obtient

$$1 = 2\langle 1 | \chi_{\lambda_X^0} \rangle_G + \langle \chi_{\lambda_X^0} | \chi_{\lambda_X^0} \rangle_G.$$

D'où, nécessairement, $\langle \chi_{\lambda_X^0} | \chi_{\lambda_X^0} \rangle_G = 1$ et λ_X^0 est irréductible. □

4 Étude de $\mathrm{PSL}_2(\mathbb{F}_q)$

4.1 Propriétés du groupe $\mathrm{PSL}_2(\mathbb{K})$

Ce paragraphe a pour objet de montrer quelques propriétés de $\mathrm{PSL}_2(\mathbb{K})$, quand $\mathbb{K}$ est un corps commutatif quelconque.

Proposition 22 : $\mathrm{PSL}_2(\mathbb{K}) \triangleleft \mathrm{PGL}_2(\mathbb{K})$.

Démonstration : Si l'on note S le sous-groupe de $\mathbb{K}^\times$ composé des carrés, on a $\mathrm{PSL}_2(\mathbb{K}) = \ker(\det)$, où $\det : \mathrm{PGL}_2(\mathbb{K}) \to \mathbb{K}^\times/S$ est le morphisme induit par $\det : \mathrm{GL}\,2(\mathbb{K}) \to \mathbb{K}^\times$. □

En particulier, cela implique que tout changement de repère projectif de $\mathbb{P}^1(\mathbb{K})$ laisse $\mathrm{PSL}_2(\mathbb{K})$ invariant. Par la suite, on utilisera ce résultat de façon implicite.

Lemme 23 : *Soit $\mathbb{K}$ un corps, et a_1 et a_2 deux points de $\mathbb{P}^1(\mathbb{K})$. Si H est un sous-groupe de $\mathrm{PSL}_2(\mathbb{K})$ contenant tous les éléments de $\mathrm{PSL}_2(\mathbb{K})$ ayant a_1 ou a_2 pour unique point fixe, alors $H = \mathrm{PSL}_2(\mathbb{K})$.*

Démonstration : À un changement de repère projectif près, on peut supposer que $a_1 = 0$ et $a_2 = \infty$.
Soit $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}_2(\mathbb{K})$.
Si $c \neq 0$, $H \ni \begin{pmatrix} 1 & \frac{a-1}{c} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix} \begin{pmatrix} 1 & \frac{d-1}{c} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & \frac{ad-1}{c} \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.
Si $c = 0$ alors $d \neq 0$ et dans ce cas, d'après la ligne précédente, $\begin{pmatrix} a+b & b \\ d & d \end{pmatrix} \in H$
donc $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a+b & b \\ d & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \in H$. □

Théorème 24 : *Si $\mathbb{K}$ est un corps de cardinal 4 ou au moins égal à 6[†], alors $\mathrm{PSL}_2(\mathbb{K})$ est simple.*

Démonstration : Il suffit de montrer que tout sous-groupe distingué H de $\mathrm{SL}_2(\mathbb{K})$ non contenu dans $\{\pm \mathrm{Id}\}$ est égal à $\mathrm{SL}_2(\mathbb{K})$ tout entier.
Soit $A \in H \setminus \{\pm \mathrm{Id}\}$ et $v \in \mathbb{K}^2$ tel que (v, Av) soit une base de $\mathbb{K}^2$.
Dans cette base, A s'écrit $\begin{pmatrix} 0 & -1 \\ 1 & \alpha \end{pmatrix}$ car $\det A = 1$.
Comme $\mathbb{K} = \mathbb{F}_4$ ou $|\mathbb{K}| \geqslant 6$, il existe un élément β de $\mathbb{K}^*$ tel que $\beta^4 \neq 1$. Comme $H \triangleleft \mathrm{SL}_2(\mathbb{K})$,

$$H \ni \begin{pmatrix} \beta & 0 \\ 0 & \beta^{-1} \end{pmatrix}^{-1} A^{-1} \begin{pmatrix} \beta & 0 \\ 0 & \beta^{-1} \end{pmatrix} A = \begin{pmatrix} \beta^{-2} & \alpha(\beta^{-2}-1) \\ 0 & \beta^2 \end{pmatrix} = B$$

puis, pour $\mu \in \mathbb{K}$:

$$H \ni \begin{pmatrix} 1 & \frac{\mu}{\beta^4-1} \\ 0 & 1 \end{pmatrix}^{-1} B^{-1} \begin{pmatrix} 1 & \frac{\mu}{\beta^4-1} \\ 0 & 1 \end{pmatrix} B = \begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix}$$

Et ensuite :

$$H \ni \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & -\mu \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 \\ \mu & 1 \end{pmatrix}$$

Le lemme 23 permet de conclure. □

Proposition 25 : *Si $\mathbb{K}$ est un corps commutatif, tout élément de $\mathrm{PSL}_2(\mathbb{K})$ a un centralisateur abélien.*

[†]Cela se montre d'une façon similaire pour $\mathbb{F}_5$, mais ce résultat n'interviendra pas dans la suite.

Démonstration : Tout d'abord, remarquons que tout polynôme du second degré sur $\mathbb{K}$ se scinde sur $\overline{\mathbb{K}}$, clôture algébrique de $\mathbb{K}$[‡]. Soit donc A un élément de $\mathrm{PSL}_2(\mathbb{K})$. Dans $\mathbb{P}^1(\overline{\mathbb{K}})$, A a alors un ou deux points fixes. Dans les deux cas, on peut supposer que A fixe ∞.

- Si A n'a que ∞ comme point fixe, alors tous les éléments de son centralisateur dans $\mathrm{PSL}_2(\overline{\mathbb{K}})$ ont ∞ comme point fixe. Ainsi, A est une translation de $\overline{\mathbb{K}} \subset \mathbb{P}^1(\overline{\mathbb{K}})$ et son centralisateur dans $\mathrm{PSL}_2(\overline{\mathbb{K}})$ est composé d'applications affines de $\overline{\mathbb{K}}$. On en déduit facilement que le centralisateur de A dans $\mathrm{PSL}_2(\overline{\mathbb{K}})$ est le groupe des translations de $\overline{\mathbb{K}}$, qui est abélien. On conclut immédiatement car le centralisateur de A dans $\mathrm{PSL}_2(\mathbb{K})$ est un sous-groupe du centralisateur de A dans $\mathrm{PSL}_2(\overline{\mathbb{K}})$.
- Si A a un deuxième point fixe, on peut supposer, à changement de repère projectif près, que c'est 0 et par conséquent que A est une homothétie de $\overline{\mathbb{K}} \subset \mathbb{P}^1(\overline{\mathbb{K}})$. Si un élément du centralisateur de A dans $\mathbb{P}^1(\overline{\mathbb{K}})$ échangeait 0 et ∞, ce serait une inversion de centre 0, qui ne commuterait pas avec A. Donc les éléments du centralisateur de A dans $\mathbb{P}^1(\overline{\mathbb{K}})$ ont 0 et ∞ comme points fixes et ce sont les homothéties de $\mathbb{P}^1(\overline{\mathbb{K}})$ de déterminant 1 (i.e. celles de rapport carré) qui forment un groupe abélien. □

4.2 Propriétés du groupe $\mathrm{PSL}_2(\mathbb{F}_q)$

Dans ce paragraphe, on étudiera en particulier des propriétés des sous-groupes de $\mathrm{PSL}_2(\mathbb{F}_q)$, quand q est un nombre premier.

Lemme 26 : *Si q est premier, et $g \in \mathrm{PSL}_2(\mathbb{F}_q)$, les assertions suivantes sont équivalentes :*

i) g est d'ordre q ;

ii) g admet un unique point fixe ;

iii) dans un certain repère projectif, g est une translation de $\mathbb{F}_q \subset \mathbb{P}^1(\mathbb{F}_q)$.

Démonstration :

i) ⇒ ii) L'application g agit comme une permutation d'ordre premier q sur $\mathbb{P}^1(\mathbb{F}_q)$. Les orbites de cette permutation sont donc de longueur q ou 1. Comme $g \neq 1$, g a une orbite de longueur q et une orbite de longueur 1, ce qui montre le résultat.

ii) ⇒ iii) À un changement de repère près, le point fixe de g est ∞. Ainsi, g agit alors sur $\mathbb{F}_q \subset \mathbb{P}^1(\mathbb{F}_q)$ comme une application affine non constante et sans point fixe, c'est-à-dire une translation.

iii) ⇒ i) C'est évident. □

Lemme 27 : *Si G est un groupe fini et si le centralisateur de tout élément hors du centre Z de G est abélien, alors l'intersection de deux sous-groupes de G abéliens maximaux distincts est Z.*

Démonstration : Notons que tout sous-groupe abélien maximal de G contient

[‡]Si $\mathbb{K} = \mathbb{F}_q$ où q est une puissance d'un nombre premier, on peut remplacer $\overline{\mathbb{K}}$ par $\mathbb{F}_{q^2}$.

Z. Si J et K sont des sous-groupes abéliens maximaux et $J \cap K \neq Z$ et si $g \in (J \cap K) \setminus Z$, J et K sont tous deux inclus dans le centralisateur de g qui est par hypothèse abélien. Par maximalité, J et K sont égaux au centralisateur de g donc $J = K$. □

Lemme 28 : *Si q est un nombre premier impair et H un sous-groupe de $\mathrm{PSL}_2(\mathbb{F}_q)$ tel que $q \nmid |H|$ alors tout sous-groupe abélien maximal de H est d'indice au plus 2 dans son normalisateur.*

Démonstration : Soit J un sous-groupe abélien maximal de H.
On peut bien sûr supposer que H est non trivial et que $A \in J$ n'est pas l'identité. Comme pour la proposition 25, on regarde A comme élément de $\mathrm{PSL}_2(\mathbb{F}_{q^2})$. Dans $\mathbb{F}_{q^2}$, A admet alors un ou deux points fixes. On suppose que A fixe ∞. Si A avait un seul point fixe, ce serait une translation de $\mathbb{F}_{q^2} \subset \mathbb{P}^1(\mathbb{F}_{q^2})$ et q diviserait l'ordre de A, ce qui contredirait $q \nmid |H|$.
Donc A a un second point fixe, qui peut être envoyé par changement de repère projectif sur 0. Dès lors, A est une homothétie de $\mathbb{F}_{q^2} \subset \mathbb{P}^1(\mathbb{F}_{q^2})$. Comme J est abélien, tous ses éléments fixent $\{0, \infty\}$. Les éléments inversant 0 et ∞ sont des inversions qui ne commutent donc pas avec A. J ne contient donc que des homothéties de $\mathbb{F}_{q^2} \subset \mathbb{P}^1(\mathbb{F}_{q^2})$.
Pour tout élément B du normalisateur de J, $AB\{0,\infty\} = BB^{-1}AB\{0,\infty\} = B\{0,\infty\}$ car $B^{-1}AB \in J$ et donc $B(\{0,\infty\}) \subset \{0,\infty\}$ puis par cardinalité, $B\{0,\infty\} = \{0,\infty\}$. L'application canonique de $N_H(J)$ dans $\mathfrak{S}(\{0,\infty\})$ admet alors clairement J pour noyau (car J est abélien maximal), ce qui achève la démonstration. □

Définition : Un groupe G est dit *métabélien* s'il admet un sous-groupe distingué H tel que H et G/H soient abéliens. En particulier, un tel groupe est résoluble.

Proposition 29 : *Soit G un groupe. Les trois assertions suivantes sont équivalentes :*

i) G est métabélien ;

ii) Le groupe dérivé de G est abélien ;

iii) $\forall a, b, c, d \in G, [[a, b], [c, d]] = 1$[†]*.* □

Théorème 30 : *Si q est premier, les sous-groupes stricts de $\mathrm{PSL}_2(\mathbb{F}_q)$ possédant strictement plus de 60 éléments sont métabéliens*[‡]*.*

Démonstration : Soit H un sous groupe strict de $\mathrm{PSL}_2(\mathbb{F}_q)$ possédant strictement plus de 60 éléments.
Distinguons deux cas :
– Si $q \mid |H|$, alors H contient au moins un sous-groupe d'ordre q. Supposons par l'absurde qu'il en contienne plus d'un. Dans ce cas, d'après le lemme 26,

[†] $[x, y] = xyx^{-1}y^{-1}$

[‡] En réalité, les seuls sous-groupes stricts de $\mathrm{PSL}_2(\mathbb{F}_q)$ non métabéliens sont $\mathfrak{S}_4$ et $\mathfrak{A}_5$.

il existerait a_1 et a_2 dans $\mathrm{PSL}_2(\mathbb{F}_q)$ tels que H contienne tous les éléments ayant pour unique point fixe a_1 ou a_2, si bien que H serait $\mathrm{PSL}_2(\mathbb{F}_q)$ d'après le lemme 23.
Soit alors H_0 l'unique sous-groupe d'ordre q de H. À changement de repère projectif près, H_0 est le groupe des translations de $\mathbb{P}^1(\mathbb{F}_q)$ et a ∞ pour point fixe. Comme H_0 est distingué dans H, H fixe aussi ∞ et H est alors contenu dans le groupe des applications affines de $\mathbb{F}_q \subset \mathbb{P}^1(\mathbb{F}_q)$, qui est métabélien (son groupe dérivé est l'ensemble des translations de $\mathbb{F}_q$). Donc H est métabélien.

– Si $q \nmid |H|$ alors, par cardinalité, $q \geqslant 7$ et en particulier, q est impair. Soit $h = |H|$. Soient $C_1, \ldots, C_s$ les classes de conjugaison des sous-groupes abéliens maximaux de H égaux à leurs normalisateurs et $C_{s+1}, \ldots, C_{s+t}$ celles des sous-groupes abéliens maximaux de H d'indice 2 dans leurs normalisateurs (d'après le lemme 28, ce sont les seuls cas possibles). Soit enfin g_i le cardinal commun des éléments de C_i.
Tout $A \in H$ différent de l'identité est contenu dans exactement un sous-groupe abélien maximal d'après la proposition 25 et le lemme 27 et par conséquent,

$$|H| = 1 + \sum_{i=1}^{s+t} \sum_{J \in C_i} (|J| - 1).$$

Puis, en remarquant que si H agit sur C_i par conjugaison, $J \in C_i$ a pour orbite C_i et pour stabilisateur $N(J)$ et par conséquent que $\forall J \in C_i, |H| = |C_i||N(J)|$

$$\begin{aligned} 1 &= \frac{1}{|H|} + \sum_{i=1}^{s+t} \sum_{J \in C_i} \frac{|J|-1}{|H|} = \frac{1}{h} + \sum_{i=1}^{s+t} \sum_{J \in C_i} \frac{|J|-1}{|C_i||N(J)|} \\ &= \frac{1}{h} + \sum_{i=1}^{s+t} \sum_{J \in C_i} \frac{|J|-1}{|C_i||J|[N(J):J]} = \frac{1}{h} + \sum_{i=1}^{s} \frac{g_i - 1}{g_i} + \sum_{i=s+1}^{s+t} \frac{g_i - 1}{2g_i}. \end{aligned}$$

Donc,

$$1 = \frac{1}{h} + \sum_{i=1}^{s} \left(1 - \frac{1}{g_i}\right) + \frac{1}{2} \sum_{i=s+1}^{s+t} \left(1 - \frac{1}{g_i}\right) \geqslant \frac{1}{h} + \frac{s}{2} + \frac{t}{4}.$$

Il y a alors 5 possibilités :

1) Si $s = 1$ et $t = 0$, H est abélien, d'où le résultat.
2) Si $s = 1$ et $t = 1$, on peut écrire la relation précédente comme ceci :

$$1 = \frac{1}{h} + 1 - \frac{1}{g_1} + \frac{1}{2} - \frac{1}{2g_2}$$

D'où :

$$1 + \frac{2}{h} = \frac{2}{g_1} + \frac{1}{g_2}$$

Comme $g_1 < h$, $g_2 \geqslant 2$ et alors $\frac{1}{2} < \frac{2}{g_1}$. Donc $2 \leqslant g_1 \leqslant 3$. Si $g_1 = 3$, alors $\frac{1}{3} < \frac{1}{g_2}$ et $g_2 = 2$ puis $h = 12$, ce qui contredit $h > 60$. Donc $g_1 = 2$. Alors, comme $g_2 = \frac{h}{2}$, H admet un sous-groupe abélien d'indice 2, ce qui montre le résultat.

3) Si $s = 0$ et $t = 1$, la relation devient :

$$1 = \frac{1}{h} + \frac{1}{2}\left(1 - \frac{1}{g_1}\right)$$

Ceci contredit le fait que $h > 60$.

4) Si $s = 0$ et $t = 2$, alors :

$$1 = \frac{1}{h} + \frac{1}{2}\left(1 - \frac{1}{g_1} + 1 - \frac{1}{g_2}\right)$$

Ceci contredit le fait que $g_1 < h$ et $g_2 < h$.

5) Si $s = 0$ et $t = 3$, il vient que :

$$1 = \frac{1}{h} + \frac{1}{2}\left(1 - \frac{1}{g_1} + 1 - \frac{1}{g_2} + 1 - \frac{1}{g_3}\right)$$

Ou encore :

$$1 + \frac{2}{h} = \frac{1}{g_1} + \frac{1}{g_2} + \frac{1}{g_3}$$

Si on suppose que $g_1 \leqslant g_2 \leqslant g_3$, on obtient tout de suite que $g_1 = 2$ puis $2 \leqslant g_2 \leqslant 4$. Si $g_2 = 2$, $g_3 = \frac{h}{2}$ et H contient un sous-groupe abélien d'indice 2.

Si $g_2 = 3$, $\frac{1}{6} + \frac{2}{h} = \frac{1}{g_3}$, ce qui est impossible puisque $h > 60$ ($\frac{1}{6} < \frac{1}{g_3} < \frac{1}{6} + \frac{2}{60} = \frac{1}{5}$).

Si $g_2 = 4$, $\frac{1}{4} + \frac{2}{h} = \frac{1}{g_3}$, ce qui est aussi impossible puisque $h > 60$ ($\frac{1}{4} < \frac{1}{g_3} < \frac{1}{4} + \frac{2}{60} < \frac{1}{3}$).

Cela conclut la preuve. □

4.3 Représentations de $\mathrm{PSL}_2(\mathbb{F}_q)$

Soit $q \geqslant 7$[†] un nombre premier. Démontrons le théorème suivant.

Théorème 31 : *Le degré de toute représentation non triviale de* $\mathrm{PSL}_2(\mathbb{F}_q)$ *est au moins* $\frac{q-1}{2}$.

Notons B le groupe des transformations affines de $\mathbb{F}_q$, i.e. des $z \mapsto az + b$ pour $a \in \mathbb{F}_q^\times$ et $b \in \mathbb{F}_q$. On considère, comme dans la partie 3 (page 13), la représentation $\lambda_{\mathbb{F}_q}$ de B et sa sous-représentation $\lambda^0_{\mathbb{F}_q}$ sur

$$W_0 = \left\{ f \in \ell^2(\mathbb{F}_q) : \sum_{z \in \mathbb{F}_q} f(z) = 0 \right\}.$$

Lemme 32 : *La représentation* $\lambda^0_{\mathbb{F}_q}$ *est irréductible, de degré* $q - 1$.

Démonstration : D'après la proposition 21, il suffit de montrer que B agit de

[†] Le théorème est vrai dans le cas $q = 5$, mais il utilise le résultat de la proposition 24 pour $\mathbb{F}_5$, que l'on ne démontre pas, car on s'intéressera au comportement asymptotique, quand p est fixé et q devient grand.

façon 2-transitive sur $\mathbb{F}_q$. Cela revient à montrer qu'il existe une droite affine reliant deux points quelconques de $\mathbb{F}_q^2$, ce qui est évident. □

Soit maintenant B_0 le stabilisateur de ∞ dans $\mathrm{PSL}_2(\mathbb{F}_q)$, c'est-à-dire le sous-groupe de B composé des $z \mapsto az+b$ où a est un carré (non nul). Ainsi, B_0 est un sous-groupe d'indice 2 de B. Soit α le morphisme de groupe $(z \mapsto az+b) \mapsto a$.

La proposition suivante dresse la liste des représentations irréductibles de B_0.

Proposition 33 : *Le groupe B_0 admet $\frac{q+3}{2}$ représentations irréductibles, réparties en :*
– $\frac{q-1}{2}$ morphismes de B_0 dans $\mathbb{C}^\times$, factorisables par α ;
– 2 représentations ρ_+ et ρ_- de degré $\frac{q-1}{2}$.

Démonstration : Le groupe des carrés de $\mathbb{F}_q$ étant un groupe abélien, ses représentations irréductibles sont nécessairement de degré 1 (en utilisant l'existence de valeurs propres sur $\mathbb{C}$). D'après la proposition 20, il y en a exactement $\frac{q-1}{2}$. Comme α est surjective, on obtient, en les composant à droite par α, $\frac{q-1}{2}$ représentations distinctes irréductibles de B_0 dans $\mathbb{C}^\times$.
Soit $\omega = e^{2i\pi/q}$. On définit, pour tout $c \in \mathbb{F}_q$

$$e_c : \mathbb{F}_q \to \mathbb{C} : n \mapsto \omega^{cn}.$$

Les (e_c) sont orthogonaux au sens du produit scalaire sur $\ell^2(\mathbb{F}_q)$, et en forment donc une base. De plus, les (e_c) pour $c \in \mathbb{F}_q^\times$ forment une base de W_0, et l'on note W_+ et W_- les sous-espaces de W_0 engendrés respectivement par les (e_c) pour c carré, et les (e_c) pour c non carré. On vérifie facilement que W_+ et W_- sont stables sous l'action de B_0. Ces deux espaces sont de dimension $\frac{q-1}{2}$. On pose donc ρ_+ et ρ_- les restrictions de $\lambda^0_{\mathbb{F}_q}|_{B_0}$ à W_+ et W_-.
Si $g \in B \setminus B_0$, $\lambda^0_{\mathbb{F}_q}(g)$ échange W_+ et W_-. On en déduit que

$$\chi_{\lambda^0_{\mathbb{F}_q}}(g) = \begin{cases} \chi_{\rho_+}(g) + \chi_{\rho_-}(g) & \text{si } g \in B_0; \\ 0 & \text{sinon.} \end{cases}$$

Comme, d'après le lemme 32, $\lambda^0_{\mathbb{F}_q}$ est irréductible, on calcule que

$$1 = \langle \chi_{\lambda^0_{\mathbb{F}_q}} | \chi_{\lambda^0_{\mathbb{F}_q}} \rangle_B = \frac{1}{2}(\langle \chi_{\rho_+} | \chi_{\rho_+} \rangle_{B_0} + 2\,\mathrm{Re}\langle \chi_{\rho_+} | \chi_{\rho_-} \rangle_{B_0} + \langle \chi_{\rho_-} | \chi_{\rho_-} \rangle_{B_0}).$$

Or le théorème 17 assure que les nombres $\langle \chi_{\rho_+} | \chi_{\rho_+} \rangle_{B_0}$, $\langle \chi_{\rho_+} | \chi_{\rho_-} \rangle_{B_0}$ et $\langle \chi_{\rho_-} | \chi_{\rho_-} \rangle_{B_0}$ sont des entiers positifs, avec $\langle \chi_{\rho_+} | \chi_{\rho_+} \rangle_{B_0}$ et $\langle \chi_{\rho_-} | \chi_{\rho_-} \rangle_{B_0} > 0$. On a donc finalement $\langle \chi_{\rho_+} | \chi_{\rho_+} \rangle_{B_0} = \langle \chi_{\rho_-} | \chi_{\rho_-} \rangle_{B_0} = 1$ et $\langle \chi_{\rho_+} | \chi_{\rho_-} \rangle_{B_0} = 0$. Cela conclut la démonstration car la formule des degrés, établie dans la proposition 20, montre que l'on a ainsi trouvé toutes les représentations de B_0. □

Enfin, soit π une représentation non triviale de $\mathrm{PSL}_2(\mathbb{F}_q)$ de degré n. D'après la proposition 13, sa restriction à B_0 se décompose en somme de représentations irréductibles de B_0. De plus, comme $q \geqslant 7$, $\mathrm{PSL}_2(\mathbb{F}_q)$ est simple, par la proposition 24. La représentation $\pi|_{B_0}$ doit donc être fidèle. Or la liste établie dans le lemme 33 montre que toutes les représentations de degré 1 sont triviales sur le groupe dérivé de B_0, car elles sont factorisables par α. L'une au moins des deux

représentations irréductibles de B_0 de degré $\frac{q-1}{2}$ doit donc apparaître dans la décomposition de $\pi|_{B_0}$, si bien que $n \geqslant \frac{q-1}{2}$. Cela conclut la démonstration du théorème 31.

5 Quaternions

5.1 Définition des quaternions

Définition : Soit A un anneau. L'algèbre des *quaternions* sur A, notée $\mathbb{H}(A)$, est le A-module libre engendré par les quatre éléments 1, i, j et k, que l'on munit de la structure d'algèbre définie par :

(i) 1 est le neutre pour la multiplication ;

(ii) $i^2 = j^2 = k^2 = -1$;

(iii) $ij = -ji = k$, $jk = -kj = i$, $ki = -ik = j$.

On constate que la conjugaison n'est pas un automorphisme. En revanche, la *norme*, définie par $N(q) = q\overline{q}$, est multiplicative, ie. on a $N(q_1 q_2) = N(q_1)N(q_2)$.

Proposition 34 : *Soit A un anneau dans lequel 4 n'est pas un diviseur de zéro. S'il existe $x, y \in A$ tels que $x^2 + y^2 + 1 = 0$, alors $\mathbb{H}(A)$ est isomorphe à une sous-algèbre de $M_2(A)$.*

Démonstration : Posons

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, i = \begin{pmatrix} x & -y \\ -y & -x \end{pmatrix}, j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, k = \begin{pmatrix} y & x \\ x & -y \end{pmatrix}.$$

Ainsi, les propriétés (i), (ii) et (iii) de la définition précédente sont vérifiées. Reste à démontrer que le module est libre, i.e. que 1, i, j et k sont linéairement indépendantes. Cela revient à vérifier que le déterminant suivant est non nul dans le corps des fractions de A :

$$\begin{vmatrix} 1 & x & 0 & y \\ 0 & -y & 1 & x \\ 0 & -y & -1 & x \\ 1 & -x & 0 & -y \end{vmatrix} = -4(x^2 + y^2) = 4.$$

or on a justement supposé que 4 n'était pas un diviseur de zéro. Cela démontre l'injection attendue. □

Notons que dans le cas où l'injection est possible, la norme d'un quaternion est égale au déterminant de la matrice associée.

Proposition 35 : *Soit q une puissance d'un nombre premier impair. Alors il existe $x, y \in \mathbb{F}_q$ tels que $x^2 + y^2 + 1 = 0$.*

Démonstration : On note qu'il y a $(q+1)/2$ carrés dans $\mathbb{F}_q$. Dès lors, les deux ensembles

$$A_+ = \{x^2 + 1 : x \in \mathbb{F}_q\} \text{ et } A_- = \{-y^2 : y \in \mathbb{F}_q\}$$

ne sont pas disjoints, d'où le résultat. □

Nous utiliserons les quaternions sur l'anneau $\mathbb{Z}/n\mathbb{Z}$. Nous aurons donc besoin de la propriété suivante.

Proposition 36 : *Soit n un entier impair. Il existe $x, y \in \mathbb{N}$ tels que $x^2+y^2+1 \equiv 0 \pmod{n}$. En particulier, $\mathbb{H}(\mathbb{Z}/n\mathbb{Z})$ est isomorphe à l'algèbre $M_2(\mathbb{Z}/n\mathbb{Z})$.*

Démonstration : D'après le théorème des restes chinois, on peut se ramener au cas où $n = p^\alpha$, avec p premier et $\alpha \in \mathbb{N}^*$. Procédons par récurrence sur α.
Si $\alpha = 1$, la proposition précédente permet de conclure.
Supposons $\alpha > 1$. Par hypothèse de récurrence, il existe $x, y \in \mathbb{N}$ tels que $x^2 + y^2 + 1 \equiv 0 \pmod{p^{\alpha-1}}$. Quitte à échanger x et y, on peut supposer que $x \not\equiv 0 \pmod{p}$. Si l'on note $Q(X) = X^2 + y^2 + 1$, on a le développement de Taylor :

$$Q(x + \lambda p^{\alpha-1}) = Q(x) + \lambda p^{\alpha-1} Q'(x) + \frac{1}{2}\lambda^2 p^{2\alpha-2} Q''(x).$$

Le dernier terme est nécessairement entier et divisible par p^α, si bien que $Q(x + \lambda p^{\alpha-1}) \equiv Q(x) + \lambda p^{\alpha-1} Q'(x) \pmod{p^\alpha}$. Ainsi, on cherche λ tel que

$$Q(x) + \lambda p^{\alpha-1} Q'(x) \equiv 0 \pmod{p^\alpha}$$

$$\frac{Q(x)}{p^{\alpha-1}} + \lambda Q'(x) \equiv 0 \pmod{p}$$

Comme on a supposé $x \not\equiv 0 \pmod{p}$, et comme p est impair, $Q'(x)$ est inversible. On a ainsi trouvé un λ qui convienne, et il existe donc x tel que $Q(x) \equiv 0 \pmod{p^\alpha}$, ce qui était le résultat attendu.
Enfin, on sait que dans ces conditions, $\mathbb{H}(\mathbb{Z}/n\mathbb{Z})$ s'injecte dans $M_2(\mathbb{Z}/n\mathbb{Z})$. Ces deux algèbres, ayant même cardinal, sont isomorphes. □

Proposition 37 : *Tout quaternion $\alpha \in \mathbb{H}(\mathbb{Z})$ non inversible est produit de quaternions irréductibles.*

Démonstration : Soit $\alpha \in \mathbb{H}(\mathbb{Z})$. Démontrons le résultat par récurrence sur $N(\alpha)$. Si $N(\alpha) = 1$, α est inversible. Si maintenant α n'est pas irréductible, soit β et γ non inversibles tels que $\alpha = \beta\gamma$. Par hypothèse de récurrence, comme $N(\beta)$ et $N(\gamma)$ sont strictement inférieurs à $N(\alpha)$, on conclut que β et γ se décomposent en produit d'irréductibles, et donc α aussi. □

Il n'y a pas unicité de cette factorisation.

5.2 Sommes de quatre carrés

Soit p un nombre premier. On s'intéresse à l'équation $a_0^2 + a_1^2 + a_2^2 + a_3^2 = p$, avec $a_0, a_1, a_2, a_3 \in \mathbb{Z}$. D'après le théorème suivant, démontré par Jacobi, elle possède $8(p + 1)$ solutions.

Théorème 38 : *Soit n un entier impair positif. Alors, le nombre de solutions de $a_0^2 + a_1^2 + a_2^2 + a_3^2 = n$, avec $a_0, a_1, a_2, a_3 \in \mathbb{Z}$, est $8 \sum_{d|n} d$.*

Dans le cas des sommes de deux carrés, on utilise la factorialité de $\mathbb{Z}[i]$ pour obtenir que le nombre de décomposition d'un entier n strictement positif en somme de deux carrés (d'entiers *relatifs*) est égal à $4(d_1(n) - d_3(n))$, où $d_i(n)$ est le nombre de diviseurs de n congrus à i modulo 4. L'anneau $\mathbb{H}(\mathbb{Z})$ n'étant pas factoriel ; pour démontrer le théorème 38, on introduit un nouvel anneau.

Définition : On appelle *anneau des quaternions d'Hurwitz* l'ensemble

$$\widetilde{\mathbb{H}}(\mathbb{Z}) = \mathbb{H}(\mathbb{Z}) \cup \left(\frac{1+i+j+k}{2} + \mathbb{H}(\mathbb{Z}) \right).$$

Proposition 39 : *Les quaternions d'Hurwitz forment un anneau, qui est euclidien (à gauche comme à droite).*

Démonstration : On vérifie facilement que cet ensemble est un anneau. Montrons qu'il est euclidien. Si $z_1, z_2 \in \widetilde{\mathbb{H}}(\mathbb{Z})$, il s'agit de montrer que la distance de $q = z_1 {z_2}^{-1}$ (ou ${z_2}^{-1} z_1$) au réseau des points entiers ou demi-entiers de $\mathbb{R}^4$ est strictement inférieure à 1. Or la distance de q au réseau des points entiers de $\mathbb{R}^4$ est toujours inférieure à 1, et l'égalité n'est vérifiée que si q est demi-entier. Cela démontre que la distance de q au réseau des points entiers ou demi-entiers de $\mathbb{R}^4$ est strictement inférieure à 1. Ainsi, $\widetilde{\mathbb{H}}(\mathbb{Z})$ est euclidien à gauche comme à droite. □

On cherche le nombre de factorisations de n sous la forme $n = z\overline{z}$, avec $z \in \mathbb{H}(\mathbb{Z})$. Il y a deux fois plus de telles factorisations dans $\widetilde{\mathbb{H}}(\mathbb{Z})$. En effet, supposons que $n = z\overline{z}$, avec $z \in \widetilde{\mathbb{H}}(\mathbb{Z}) \setminus \mathbb{H}(\mathbb{Z})$. Si l'on note $\alpha = \frac{1+i+j+k}{2}$ et $z = \frac{a+ib+jc+kd}{2}$ on est dans l'un des deux cas suivants :

$$\begin{array}{ll} \alpha z \in \mathbb{H}(\mathbb{Z}) & \text{si, et seulement si,} \quad a-b-c-d \equiv 0 \pmod 4 ; \\ \overline{\alpha} z \in \mathbb{H}(\mathbb{Z}) & \text{si, et seulement si,} \quad a+b+c+d \equiv 0 \pmod 4. \end{array}$$

Cela résulte du fait que a, b, c et d sont impairs. Comme α est inversible, on a une bijection entre les solutions dans $\mathbb{H}(\mathbb{Z})$ et celles dans $\widetilde{\mathbb{H}}(\mathbb{Z}) \setminus \mathbb{H}(\mathbb{Z})$. Il s'agit donc de montrer qu'il y a $16 \sum_{d|n} d$ telles factorisations dans $\widetilde{\mathbb{H}}(\mathbb{Z})$.

Cela revient à compter les idéaux à droite de norme n^2, où la norme d'un idéal I d'un anneau A est définie comme suit.

Proposition 40 : *Si I est un idéal d'un anneau A, la norme de I est $N(I) = |A/I|$. Dans le cas de $\widetilde{\mathbb{H}}(\mathbb{Z})$, qui est principal à droite, si $I = (z) = z\widetilde{\mathbb{H}}(\mathbb{Z})$, on a*

$$N(I) = N(z)^2.$$

Démonstration : $\widetilde{\mathbb{H}}(\mathbb{Z})$ est un $\mathbb{Z}$-module libre de dimension 4 dont une base est (α, i, j, k). Pour calculer la norme de l'idéal I, on utilise les résultats sur les modules sur les anneaux principaux. On a donc

$$N(I) = \det(x \mapsto zx).$$

Ce déterminant est le même que celui de l'application $x \mapsto zx$ sur $\mathbb{H}(\mathbb{R})$, car une base de $\widetilde{\mathbb{H}}(\mathbb{Z})$ en est une de $\mathbb{H}(\mathbb{R})$, si bien que l'on peut calculer ce déterminant dans la base $(1, i, j, k)$. Ainsi, si $z = a + ib + jc + kd$,

$$N(I) = \begin{vmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{vmatrix} = \left(a^2 + b^2 + c^2 + d^2\right)^2 = N(z)^2.$$

□

On notera J_n l'ensemble des idéaux à droite de norme n^2. Comme il y a 16 inversibles dans $\widetilde{\mathbb{H}}(\mathbb{Z})$ (l'ensemble des éléments de norme 1, à savoir 1, i, j, k, α, $i\alpha$, $j\alpha$, $k\alpha$ et leurs opposés), il y a 16 fois plus d'éléments de norme n que d'idéaux dans J_n. Montrons donc que $|J_n| = \sum_{d|n} d$. Dans la suite, les idéaux considérés seront toujours des idéaux à droite.

Clairement, la norme des idéaux est invariante par passage au quotient, et comme les idéaux de $\widetilde{\mathbb{H}}(\mathbb{Z})$ contenant n sont en bijection avec ceux de $\widetilde{\mathbb{H}}(\mathbb{Z})/(n)$, on est ramené au cas des idéaux de $\widetilde{\mathbb{H}}(\mathbb{Z})/(n) = \widetilde{\mathbb{H}}(\mathbb{Z}/n\mathbb{Z}) = \mathbb{H}(\mathbb{Z}/n\mathbb{Z})$, cette égalité découlant du fait que 2 est inversible dans $\mathbb{Z}/n\mathbb{Z}$. Finalement, d'après la proposition 36, il s'agit de dénombrer les idéaux de $M_2(\mathbb{Z}/n\mathbb{Z})$ de norme n^2, donc les idéaux de $M_2(\mathbb{Z})$ contenant $n\,\mathrm{Id}$ et de norme n^2.

La proposition suivante donne une caractérisation des idéaux à droite de $M_2(\mathbb{Z})$.

Proposition 41 : *Les idéaux à droite de $M_2(\mathbb{Z})$ sont en bijection avec les réseaux de $\mathbb{Z}^2$, par l'application qui, à un idéal I de $M_2(\mathbb{Z})$, associe le réseau*

$$\mathrm{Im}(I) = \{M(x) : M \in I, x \in \mathbb{Z}^2\}$$

où (e_1, e_2) est la base canonique de $\mathbb{Z}^2$. De plus, on a alors que $N(I) = \mathrm{vol}(\mathrm{Im}(I))^2$.

Démonstration : Cette application est bien surjective, car l'application $R \mapsto \{M \in M_2(\mathbb{Z}) : \mathrm{Im}(M) \subset R\}$ en est clairement une réciproque à droite. Reste à montrer l'injectivité. Soit I un idéal de $M_2(\mathbb{Z})$, et $M \in M_2(\mathbb{Z})$ telle que $\mathrm{Im}(M) \subset \mathrm{Im}(I)$. Par définition, il existe $A, B \in I$ tels que $A(e_1) = M(e_1)$ et $B(e_2) = M(e_2)$. Dès lors, on a

$$M = A\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + B\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \in I.$$

Ainsi, on a montré que $M \in I \Leftrightarrow \mathrm{Im}(M) \subset \mathrm{Im}(I)$, d'où l'injectivité.
Enfin, comme $M_2(\mathbb{Z})$ s'identifie à $\left(\mathbb{Z}^2\right)^2$, et comme, d'après le raisonnement précédent, cette identification envoie I sur $\mathrm{Im}(I)^2$, $M_2(\mathbb{Z})/I$ s'identifie à $\left(\mathbb{Z}^2/\mathrm{Im}(I)\right)^2$, si bien que $N(I) = \mathrm{vol}(\mathrm{Im}(I))^2$. □

D'après cette caractérisation, on doit dénombrer les réseaux de $\mathbb{Z}^2$ de volume n et qui contiennent $(n, 0)$ et $(0, n)$. Mais si les vecteurs α et β engendrent un réseau R de volume n, en multipliant la matrice $(\alpha\ \beta)$ par la transposée de sa comatrice, on obtient que $(n, 0)$ et $(0, n)$ sont dans R.

Proposition 42 : *Dans $\mathbb{Z}^2$, le nombre de réseaux de volume n est $\sum_{d|n} d$.*

Démonstration : Soit R un réseau de $\mathbb{Z}^2$ de volume n, et $\alpha = (\alpha_1, \alpha_2)$ et $\beta = (\beta_1, \beta_2)$ deux vecteurs engendrant R. Soit $d = \alpha_1 \wedge \beta_1$, et $u, v \in \mathbb{Z}$ tels que $u\alpha + v\beta = d$. On a alors :

$$\begin{pmatrix} \alpha_1 & \beta_1 \\ \alpha_2 & \beta_2 \end{pmatrix} \begin{pmatrix} u & -\beta_1/d \\ v & \alpha_1/d \end{pmatrix} = \begin{pmatrix} d & 0 \\ * & n/d \end{pmatrix}$$

La seconde matrice est inversible, si bien que tout réseau R est engendré par une matrice de la forme

$$\begin{pmatrix} d & 0 \\ x & n/d \end{pmatrix}$$

où $x \in \mathbb{Z}$. Mais, quitte à effectuer une division euclidienne, on peut supposer que $x \in [0, n/d - 1]$, auquel cas il est clair que les réseaux définis sont deux-à-deux distincts. Ainsi, il y a $\sum_{d|n} n/d = \sum_{d|n} d$ réseaux de volume n dans $\mathbb{Z}^2$. □

Ceci conclut la démonstration du théorème 38.

5.3 Quaternions irréductibles

Utilisons les quaternions d'Hurwitz introduits précédemment pour caractériser les quaternions irréductibles.

Définition : Un quaternion $z \in \mathbb{H}(\mathbb{Z})$ est dit *pair* si la somme de ses coefficients l'est, et *impair* sinon.

Notons que le produit de deux quaternions impairs est impair, le produit de deux quaternions pairs est pair, celui d'un pair et d'un impair est pair.

On note toujours $\alpha = \frac{1+i+j+k}{2} \in \widetilde{\mathbb{H}}(\mathbb{Z})$. Remarquons que si $z \in \mathbb{H}(\mathbb{Z})$, z et $\alpha z \overline{\alpha}$ ont la même parité. En effet, la conjugaison par α opère une permutation circulaire de i, j et k.

Lemme 43 : *Soit $z \in \mathbb{H}(\mathbb{Z})$ un quaternion. On a alors les équivalences suivantes :*

$$z \text{ est pair} \Leftrightarrow \alpha z \in \mathbb{H}(\mathbb{Z}) \Leftrightarrow \overline{\alpha} z \in \mathbb{H}(\mathbb{Z})$$

La proposition suivante est une caractérisation utile des quaternions irréductibles.

Proposition 44 : *$\delta \in \mathbb{H}(\mathbb{Z})$ est irréductible si, et seulement si, $N(\delta)$ est premier dans $\mathbb{Z}$.*

Démonstration : Montrons d'abord le résultat sur $\widetilde{\mathbb{H}}(\mathbb{Z})$.

Soit donc $x \in \widetilde{\mathbb{H}}(\mathbb{Z})$, tel que $N(x) = pb$, avec p premier et b non inversible. Montrons que x n'est pas irréductible. Comme $\widetilde{\mathbb{H}}(\mathbb{Z})$ est principal à gauche, il existe β tel que $(\alpha, p) = (\beta)$. Comme tous les éléments de (α, p) ont leur norme divisible par p, β n'est pas inversible. Il existe q tel que $p = \beta q$, et l'on a alors $p^2 = N(\beta)N(q)$. Si q est inversible, p divise x, et le résultat est démontré. Sinon, on a nécessairement $N(\beta) = N(q) = p$. Il existe donc k tel que $\alpha = \beta k$, $N(\beta) = p$ et $N(k) = b$. Ainsi, x n'est pas irréductible.

Traitons maintenant le cas de $\mathbb{H}(\mathbb{Z})$. Soit $x \in \mathbb{H}(\mathbb{Z})$, dont la norme n'est pas première dans $\mathbb{Z}$. On a montré que dans ce cas, x se factorise sur $\widetilde{\mathbb{H}}(\mathbb{Z})$ en deux quaternions non inversibles : $x = ab$. Quitte à modifier a, on peut supposer que $b \in \mathbb{H}(\mathbb{Z})$. Alors, si $a \in \mathbb{H}(\mathbb{Z})$, la preuve est terminée. Sinon, $\alpha a \in \mathbb{H}(\mathbb{Z})$ ou $\overline{\alpha}a \in \mathbb{H}(\mathbb{Z})$. Supposons par exemple que $\overline{\alpha}a \in \mathbb{H}(\mathbb{Z})$. On a alors $x = \alpha(\overline{\alpha}a)b$. Comme $x \in \mathbb{H}(\mathbb{Z})$, d'après le lemme précédent, $\overline{\alpha}a$ ou b sont pairs. Comme $a \notin \mathbb{H}(\mathbb{Z})$, $\overline{\alpha}a$ est impair et b est pair. On a donc $x = (a\overline{\alpha})(\alpha b)$. On a vu que $\mathbb{H}(\mathbb{Z})$ est stable par conjugaison par α, si bien que $a\overline{\alpha} \in \mathbb{H}(\mathbb{Z})$, et d'après le lemme précédent, $\alpha b \in \mathbb{H}(\mathbb{Z})$. Ainsi, x n'est pas irréductible sur $\mathbb{H}(\mathbb{Z})$. □

5.4 Groupe libre sur une famille de quaternions

Considérons les $8(p+1)$ solutions de l'équation $a_0^2 + a_1^2 + a_2^2 + a_3^2 = p$, avec $a_0, a_1, a_2, a_3 \in \mathbb{Z}$ et p premier. En réduisant l'équation modulo 4, il vient que si $\alpha = a_0 + a_1 i + a_2 j + a_3 k$ est solution on a :

– si $p \equiv 1 \pmod 4$, l'un des a_i est impair et les autres sont pairs ;

– si $p \equiv 3 \pmod 4$, l'un des a_i est pair et les autres sont impairs.

En tout cas, notons a_i^0 cet élément distingué. Parmi les 8 éléments associés à α, on en distingue un qui admette $|a_i^0|$ pour partie réelle. Il est unique si $a_0 \neq 0$, mais l'on doit choisir arbitrairement l'un des deux possibles si $p \equiv 3 \pmod 4$ et $a_0 = 0$.

Notons S_p l'ensemble de ces $p+1$ solutions distinguées. Si $\alpha = a_0 + a_1 i + a_2 j + a_3 k \in S_p$, $\overline{\alpha} \in S_p$ si, et seulement si, $a_0 > 0$. Ainsi, on écrit S_p sous la forme

$$S_p = \{\alpha_1, \overline{\alpha_1}, \ldots, \alpha_s, \overline{\alpha_s}, \beta_1, \ldots, \beta_t\}$$

où les α_i ont une partie réelle strictement positive, tandis que celle des β_i est nulle. Remarquons que si $p \equiv 1 \pmod 4$, les β_i sont absents.

Définition : Un *mot réduit* sur S_p est un mot sur l'alphabet S_p ne contenant aucun facteur de la forme $\alpha_i\overline{\alpha_i}$, $\overline{\alpha_i}\alpha_i$ ou β_i^2.

On note alors $G = \langle x_1, \ldots, x_s, y_1, \ldots, y_t \mid y_i = y_i^{-1} : 1 \leqslant i \leqslant t \rangle$. Remarquons que le graphe de Cayley associé à cette présentation du groupe G est l'arbre $(2s+t)$-régulier, c'est-à-dire $(p+1)$-régulier.

Considérons alors le monoïde

$$\Lambda' = \{\alpha \in \mathbb{H}(\mathbb{Z}) : \alpha \equiv 1 \pmod 2 \text{ ou } \alpha \equiv i+j+k \pmod 2, \exists k \in \mathbb{N},\ N(\alpha) = p^k\}.$$

On définit sur Λ' la relation d'équivalence $\sim$ telle que $\alpha \sim \beta \Leftrightarrow (\exists a, b \in \mathbb{N})(p^a\alpha = \pm p^b\beta)$.

Théorème 45 : *Le groupe G est isomorphe à $\Lambda = \Lambda'/\sim$, et $\mathcal{G}(\Lambda, \widetilde{S_p})$ est un arbre $(p+1)$-régulier.*

Ce théorème découle du résultat suivant :

Lemme 46 : *Soit $k \in \mathbb{N}$ et $\alpha \in \mathbb{H}(\mathbb{Z})$ tels que $N(\alpha) = p^k$. Alors, α admet une unique factorisation de la forme $\alpha = \varepsilon p^r w_m$, où ε est un inversible de $\mathbb{H}(\mathbb{Z})$ et w_m un mot réduit sur S_p de longueur m, avec $k = 2r + m$.*

Démonstration : Soit $\alpha \in \mathbb{H}(\mathbb{Z})$ tel que $N(\alpha) = p^k$. D'après la proposition 37, α s'écrit comme produit d'irréductibles, i.e. $\alpha = \delta_1 \dots \delta_n$. De plus, la proposition 44 entraîne que, pour tout $i \in \{1, \dots, n\}$, $N(\delta_i) = p$ et que $n = k$. De ce fait, il existe ε_i et $\gamma_i \in S_p$ tels que $\delta_i = \varepsilon_i \gamma_i$.
Les quaternions ne commutent pas. Cependant, il est clair que, pour tout $\gamma \in S_p$ et tout ε inversible, il existe $\gamma' \in S_p$ et ε' inversible tels que $\gamma\varepsilon = \varepsilon'\gamma'$. On peut donc factoriser α en $\alpha = \varepsilon\gamma_1 \dots \gamma_k$, avec toujours ε inversible et $\gamma_i \in S_p$. On réduit alors le mot $\gamma_1 \dots \gamma_k$, ce qui fait apparaître un terme p^r.
Cela montre l'existence de la factorisation attendue.
Pour établir l'unicité de cette factorisation, montrons qu'il y a autant de quaternions de norme p^k que de factorisations possibles. On calcule facilement que le nombre de mots réduits de longueur m est

$$\begin{cases} 1 & \text{si} \quad m = 0\,; \\ (p+1)p^{m-1} & \text{si} \quad m \geqslant 1. \end{cases}$$

On en déduit que le nombre d'expressions de la forme $\varepsilon p^r w_m$, avec ε inversible, w_m un mot réduit de longueur m et $2r + m = k$, est

$$\begin{cases} 8\left(1 + \displaystyle\sum_{r=0}^{\frac{k}{2}-1} (p+1)p^{k-2r-1}\right) & \text{si } k \text{ est pair}\,; \\ 8\displaystyle\sum_{r=0}^{\frac{k-1}{2}} (p+1)p^{k-2r-1} & \text{si } k \text{ est impair.} \end{cases}$$

En simplifiant ces expressions, on obtient que le nombre de telles expressions est $8\left(\frac{p^{k+1}-1}{p-1}\right)$ quel que soit k. Enfin, le théorème 38 assure que le nombre de quaternions de norme p^k est

$$8\sum_{i=0}^{k} p^i = 8\left(\frac{p^{k+1}-1}{p-1}\right).$$

L'unicité est ainsi démontrée. □

L'existence de la factorisation, énoncée dans le lemme, assure que $\mathcal{G}(\Lambda, \widetilde{S_p})$ est connexe. S'il existait un circuit dans ce graphe, le mot réduit associé contredirait l'unicité de la factorisation de p^n. Ainsi, $\mathcal{G}(\Lambda, \widetilde{S_p})$ est un arbre, l'isomorphisme entre G et Λ est évident et le théorème 45 est démontré.

6 Construction des graphes $Y_{p,q}$

Soit q un nombre premier distinct de p. Nous allons définir les graphes $Y_{p,q}$ comme quotients de l'arbre $(p+1)$-régulier, qui est le graphe de Cayley $\mathcal{G}(\Lambda, \widetilde{S_p})$, où $\widetilde{S_p}$ est l'ensemble des classes des éléments de S_p pour la relation $\sim$. Ces quotients seront induits par une réduction des quaternions modulo q.

6.1 Définitions

Soit $\tau_q : \mathbb{H}(\mathbb{Z}) \to \mathbb{H}(\mathbb{F}_q)$ la surjection canonique. Clairement, $\tau_q : \Lambda' \to \mathbb{H}(\mathbb{F}_q)$ induit un morphisme $\Pi_q : \Lambda \to \mathbb{H}(\mathbb{F}_q)^\times / Z_q$, où $Z_q = \{\alpha \in \mathbb{H}(\mathbb{F}_q) : \alpha = \overline{\alpha}\}$. En termes matriciels (cf. proposition 36), Π_q est un morphisme de groupes de Λ dans $\mathrm{PGL}_2(\mathbb{F}_q)$.

Notons $\Lambda(q)$ son noyau et posons $S_{p,q} = \Pi_q(\widetilde{S_p})$.

Lemme 47 : *Si q est assez grand ($q > 2\sqrt{p}$ suffit), on a $|S_{p,q}| = |S_p| = p+1$.*

Démonstration : Supposons que $q > 2\sqrt{p}$, et montrons que cette majoration est suffisante. Soient $\alpha = a_0 + ia_1 + ja_2 + ka_3$ et $\beta = b_0 + ib_1 + jb_2 + kb_3$ deux éléments de S_p distincts. Comme $N(\alpha) = N(\beta) = p$, pour tout $j \in \{0,1,2,3\}$, $a_j, b_j \in [-\sqrt{p}, \sqrt{p}]$, si bien que $\tau_q(\alpha) \neq \tau_q(\beta)$. Notons π la projection de $\mathbb{H}(\mathbb{F}_q)^\times$ dans $\mathbb{H}(\mathbb{F}_q)^\times / Z_q$. Supposons que l'on ait $\pi \circ \tau_q(\alpha) = \pi \circ \tau_q(\beta)$. Il existerait alors $\lambda \in \mathbb{F}_q^\times$ tel que $\tau_q(\alpha) = \lambda \tau_q(\beta)$. En prenant la norme, on obtient que $p = \lambda^2 p$, d'où $\lambda = -1$. Mais comme, par hypothèse, $a_0, b_0 \geqslant 0$, on a en fait $a_0 = b_0 = 0$, et donc $\beta = \overline{\alpha}$. Ceci est impossible par construction de S_p. □

On supposera par la suite cette condition remplie. On peut alors définir les $Y_{p,q}$:

$$Y_{p,q} = \mathcal{G}(\Lambda / \Lambda(q), S_{p,q})$$

En tant que quotient d'un arbre, $Y_{p,q}$ est connexe et, d'après le lemme 47, $Y_{p,q}$ est $(p+1)$-régulier. Pour établir des propriétés spectrales de la famille $Y_{p,q}$, il faut identifier le sous-groupe $\Lambda/\Lambda(q)$ de $\mathrm{PGL}_2(\mathbb{F}_q)$.

On utilisera implicitement la commutativité du diagramme suivant.

$$\begin{array}{ccccc} S_p \subset \Lambda' & \xrightarrow{\tau_q} & \mathbb{H}(\mathbb{F}_q)^\times & = & \mathrm{GL}\,2(\mathbb{F}_q) \\ \downarrow & & \downarrow & & \downarrow \\ \widetilde{S_p} \subset \Lambda & \xrightarrow{\Pi_q} & \mathbb{H}(\mathbb{F}_q)^\times / Z_q & = & \mathrm{PGL}_2(\mathbb{F}_q) \end{array}$$

Lemme 48 :

$$\Lambda(q) = \{\widetilde{\alpha} \in \Lambda : \alpha = \overline{\alpha} \ (\mathrm{mod.}\, q)\}$$

Démonstration : Cela résulte du fait que p et q sont des nombres premiers distincts. □

La systole du graphe $Y_{p,q}$ est liée à la longueur minimale des relations définissant le quotient $\Lambda/\Lambda(q)$. La minoration établie dans la proposition suivante permettra d'établir que certains éléments du quotient sont non triviaux.

Proposition 49 : *On a la minoration $g(Y_{p,q}) \geqslant 2\log_p q$. Si de plus $\left(\frac{p}{q}\right) = -1$, on a même $g(Y_{p,q}) \geqslant 4\log_p q - \log_p 4$.*

Démonstration : Soit $g = g(Y_{p,q})$, et $x_0, \ldots, x_{g-1}, x_g = x_0$ les sommets d'un cycle de longueur g. Par transitivité, on peut supposer que $x_0 = x_g = 1$. Soient alors $t_1, \ldots, t_g \in S_{p,q}$ tels que $x_i = t_i x_{i-1}$ pour $1 \leqslant i \leqslant g$, et soit γ_i l'unique

antécédent de t_i par Π_q. On note $\alpha = \gamma_1 \dots \gamma_g \in \Lambda'$, et $\alpha = a_0 + a_1 i + a_2 j + a_3 k$. Dès lors, α est un mot réduit sur S_p, car sinon, $\widetilde{\alpha} \in \Lambda$ ne serait pas réduit (en tant que chemin du graphe), ce qui contredirait sa minimalité. De ce fait, d'après le théorème 45, $\alpha \not\sim 1$ dans Λ'.
Cela entraîne que l'un des nombres a_1, a_2, a_3 au moins est non nul. De plus, par construction, $\widetilde{\alpha} \in \Lambda(q)$. D'après le lemme 48, les nombres a_1, a_2, a_3 sont donc divisibles par q, si bien que

$$p^g = N(\alpha) \geqslant q^2.$$

En prenant le logarithme, on obtient le résultat.
Si maintenant $\left(\frac{p}{q}\right) = -1$, comme $p^g \equiv a_0^2 \pmod{q}$, on a

$$1 = \left(\frac{p^g}{q}\right) = \left(\frac{p}{q}\right)^g = (-1)^g.$$

Ainsi, g est pair. Notons donc $g = 2h$. En particulier,

$$p^{2h} \equiv a_0^2 \pmod{q^2}.$$

Comme p n'est pas divisible par q, on en déduit que l'on a

$$p^h \equiv \pm a_0 \pmod{q^2}.$$

De plus, comme $a_0^2 \leqslant p^g$, $|a_0| \leqslant p^h$. Dès lors, si l'on suppose $p^h < q^2/2$, on a nécessairement $p^h = \pm a_0$, et donc $p^g = N(\alpha) = a_0^2$. Cela implique que $a_1 = a_2 = a_3 = 0$, ce qui est impossible car $\alpha \not\sim 1$. Ainsi, on a l'inégalité $p^h \geqslant q^2/2$, ce qui donne le résultat en prenant le logarithme. □

La proposition 2, associée à la proposition précédente, permet de déduire le résultat suivant.

Proposition 50 : *Si $p \geqslant 3$, on a l'inégalité*

$$|Y_{p,q}| \geqslant \frac{q}{p}.$$

Si de plus $\left(\frac{p}{q}\right) = -1$, on a même

$$|Y_{p,q}| \geqslant \frac{q^2}{2p}.$$

Théorème 51 : *Supposons que $p \geqslant 3$. Si $q > p^8$, on peut identifier $\Lambda/\Lambda(q)$:*

$$\Lambda/\Lambda(q) = \begin{cases} \mathrm{PSL}_2(\mathbb{F}_q) & si \quad \left(\frac{p}{q}\right) = 1 \ ; \\ \mathrm{PGL}_2(\mathbb{F}_q) & si \quad \left(\frac{p}{q}\right) = -1. \end{cases}$$

Démonstration : Notons d'abord que dans le premier cas, on a $S_{p,q} \subset \mathrm{PSL}_2(\mathbb{F}_q)$, tandis que dans le deuxième, $S_{p,q} \subset \mathrm{PGL}_2(\mathbb{F}_q) \setminus \mathrm{PSL}_2(\mathbb{F}_q)$. En effet, si $A \in$

$\mathrm{GL}\,2(\mathbb{F}_q)$, $[A] \in \mathrm{PSL}_2(\mathbb{F}_q)$ si, et seulement si, $\det(A)$ est un carré dans $\mathbb{F}_q$. Or si $\alpha \in S_p$ et si $A \in \mathrm{GL}\,2(\mathbb{F}_q)$ est la matrice associée, $p = N(\alpha) = \det(A)$.
Ainsi, si l'on note $H_{p,q} = \mathrm{PSL}_2(\mathbb{F}_q) \cap (\Lambda/\Lambda(q))$, il suffit dans tous les cas de montrer que $H_{p,q} = \mathrm{PSL}_2(\mathbb{F}_q)$. D'après le théorème 30, il suffit de montrer que $|H_{p,q}| > 60$ et que $H_{p,q}$ n'est pas métabélien.
Comme $q > p^8$ et $p > 3$, on a, d'après la proposition 50

$$|\Lambda/\Lambda(q)| \geqslant \frac{q}{p} > 120,$$

d'où $|H_{p,q}| > 60$.
Reste à montrer que $H_{p,q}$ n'est pas métabélien, ce qui revient, d'après la proposition 29, à trouver $g_1, g_2, g_3, g_4 \in H_{p,q}$ tels que $[[g_1, g_2], [g_3, g_4]] \neq 1$.

- Si $\left(\frac{p}{q}\right) = 1$, soit $g_1 = g_3 \in S_{p,q}$, $g_2 \in S_{p,q} \setminus \{g_1^{\pm 1}\}$ et $g_4 \in S_{p,q} \setminus \{g_1^{\pm 1}, g_2^{\pm 1}\}$. Alors, $[[g_1, g_2], [g_3, g_4]]$ est un mot réduit de longueur 16 sur $S_{p,q}$. Or on a vu (cf. proposition 49) que $g(Y_{p,q}) \geqslant 2\log_p q > 16$. Ainsi, $[[g_1, g_2], [g_3, g_4]] \neq 1$.
- Si $\left(\frac{p}{q}\right) = -1$, les éléments de $S_{p,q}$ ne sont pas dans $H_{p,q}$, mais le produit de deux d'entre eux y est. Soit donc $h_1 \in S_{p,q}$, $h_2 \in S_{p,q} \setminus \{h_1^{\pm 1}\}$ et $h_3 \in S_{p,q} \setminus \{h_1^{\pm 1}, h_2^{\pm 1}\}$. On pose alors $g_1 = h_1 h_3$, $g_2 = h_2 h_3$, $g_3 = h_1 h_2$ et $g_4 = h_3 h_2$. On vérifie ensuite que $[[g_1, g_2], [g_3, g_4]]$ est un mot réduit de longueur 24 sur $S_{p,q}$. Or on sait que dans ce cas, $g(Y_{p,q}) \geqslant 4\log_p q - \log_p 4 > 24$. Ainsi, $[[g_1, g_2], [g_3, g_4]] \neq 1$.

Cela conclut la démonstration du théorème. □

6.2 Estimations spectrales

Le but de ce paragraphe est de minorer asymptotiquement le trou spectral des graphes $Y_{p,q}$, ce qui donnera en particulier le fait que ces graphes sont expanseurs.

Dans un premier temps, on considère que l'on se trouve dans un graphe simple k-régulier X non orienté quelconque.

Définition : Dans un graphe, on dira qu'un chemin est réduit s'il ne passe jamais deux fois de suite par la même arête.
On notera $F_\ell(a, b)$ l'ensemble des chemins réduits de longueur ℓ de a à b et A_ℓ la matrice formée des cardinaux des $F_\ell(a, b)$. Notons que A_1 est la matrice d'adjacence du graphe X.

Définition : Le $m^{\text{ième}}$ polynôme de seconde espèce de Tchebychev est le pôlynôme U_m vérifiant

$$\forall \theta \in \mathbb{C}, U_m(\cos\theta) = \frac{\sin(m+1)\theta}{\sin\theta}.$$

Proposition 52 : *Les polynômes de seconde espèce de Tchebychev existent et vérifient :*

- $U_0 = 1$;
- $U_1 = 2X$;
- $\forall m \geqslant 1, U_{m+1} = 2XU_m - U_{m-1}$.

Démonstration : C'est évident. □

Lemme 53 : *Les matrices A_ℓ vérifient la relation de récurrence suivante :*

$$\forall \ell \geqslant 1, A_{\ell+1} = A_1 A_\ell - (k - \mathbb{1}_{\ell \neq 1})\, A_{\ell-1}.$$

Démonstration : $A_1 A_\ell$ est la matrice des nombres de chemins de longueur $\ell+1$ qui sauf peut-être au tout début ne passent pas deux fois de suite par la même arête.
$(k - \mathbb{1}_{\ell\neq 1})\, A_{\ell-1}$ est la matrice des nombres de chemins de longueur $\ell+1$ passant deux fois par la même arête au début puis qui ne passent plus jamais deux fois de suite par la même arête (on choisit un chemin de longueur $\ell-1$ puis un voisin du sommet de départ différent du second sommet atteint par le chemin choisi).
Ceci achève la démonstration. □

Théorème 54 : *Pour tout m entier naturel, on a l'égalité suivante :*

$$\sum_{0 \leqslant \ell \leqslant \frac{m}{2}} A_{m-2\ell} = (k-1)^{\frac{m}{2}} U_m \left(\frac{A_1}{2\sqrt{k-1}} \right).$$

Démonstration : Procédons par récurrence sur m :
– Si $m = 0$, c'est évident.
– Si $m > 0$,

$$\sum_{0 \leqslant \ell \leqslant \frac{m}{2}} A_{m-2\ell} = \sum_{0 \leqslant \ell \leqslant \frac{m}{2}-1} (A_1 A_{m-2\ell-1} - (k - \mathbb{1}_{m-2\ell\neq 2}) A_{m-2\ell-2}) + A_{m-2\left[\frac{m}{2}\right]}.$$

Or, par hypothèse de récurrence,

$$A_1 \sum_{0 \leqslant \ell \leqslant \frac{m}{2}-1} A_{m-2\ell-1} = A_1 (k-1)^{\frac{m-1}{2}} U_{m-1} \left(\frac{A_1}{2\sqrt{k-1}} \right) - \mathbb{1}_{2\nmid m} A_1$$

et,

$$\sum_{0 \leqslant \ell \leqslant \frac{m}{2}-1} (k - \mathbb{1}_{m-2\ell\neq 2}) A_{m-2\ell-2} = (k-1)^{\frac{m}{2}} U_{m-2} \left(\frac{A_1}{2\sqrt{k-1}} \right) + \mathbb{1}_{2|m}\, \mathrm{Id}\,.$$

Donc finalement,

$$\begin{aligned}
\sum_{0 \leqslant \ell \leqslant \frac{m}{2}} A_{m-2\ell} &= A_1 (k-1)^{\frac{m-1}{2}} U_{m-1} \left(\frac{A_1}{2\sqrt{k-1}} \right) - (k-1)^{\frac{m}{2}} U_{m-2} \left(\frac{A_1}{2\sqrt{k-1}} \right) \\
&= (k-1)^{\frac{m}{2}} \left(\frac{A_1}{\sqrt{k-1}} U_{m-1} \left(\frac{A_1}{2\sqrt{k-1}} \right) - U_{m-2} \left(\frac{A_1}{2\sqrt{k-1}} \right) \right) \\
&= (k-1)^{\frac{m}{2}} U_m \left(\frac{A_1}{2\sqrt{k-1}} \right).
\end{aligned}$$

□

Si le graphe X a n sommets et si $(\mu_j)_{0\leqslant j\leqslant n-1}$ désigne la suite de ses valeurs propres, on a :

Corollaire 55 : *Formule de la trace :*

$$\sum_{x\in X}\sum_{0\leqslant r\leqslant\frac{m}{2}}(A_{m-2r})_{(x,x)} = (k-1)^{\frac{m}{2}}\sum_{j=0}^{n-1}U_m\left(\frac{\mu_j}{2\sqrt{k-1}}\right).$$

Démonstration : C'est le passage à la trace de l'égalité du théorème précédent (ceci est évident car la matrice d'adjacence de X est symétrique donc diagonalisable). □

Revenons au cas du graphe $Y_{p,q}$. C'est un graphe de Caley donc ses automorphismes agissent transitivement sur ses sommets (le passage d'un sommet g_1 à un sommet g_2 se fait par le morphisme de multiplication à gauche par $g_2g_1^{-1}$). Si l'on note pour simplifier $F_\ell = F_\ell(x,x)$ et $f_\ell = |F_\ell| = A_\ell(x,x)$, la formule de la trace devient donc :

$$\sum_{0\leqslant r\leqslant\frac{m}{2}} f_{m-2r} = \frac{p^{\frac{m}{2}}}{n}\sum_{j=0}^{n-1}U_m\left(\frac{\mu_j}{2\sqrt{p}}\right)$$

Définition : Pour m un entier naturel, on notera :

$$S_q(m) = \{\alpha\in\Lambda' : N(\alpha) = p^m, \alpha\equiv\overline{\alpha}[q]\}$$

$$s_q(m) = |S_q(m)|$$

Lemme 56 : *Si m est un entier naturel,*

$$s_q(m) = 2\sum_{0\leqslant r\leqslant\frac{m}{2}} f_{m-2r}$$

Démonstration : Tout d'abord, pour tout $\ell\in\mathbb{N}$, on a une bijection φ de F_ℓ dans l'ensemble des éléments de $\Lambda(q)$ s'écrivant comme mots réduits de longueur ℓ sur $\widetilde{S_p}$. En effet, si on a un circuit réduit de longueur ℓ dans $Y_{p,q}$, on lui associe naturellement un mot réduit w de longueur ℓ sur $\widetilde{S_p}$. Cette application est bien sûr injective. Comme c'est un circuit, $\Pi_q(w) = 1$ et $w\in\Lambda(q)$; réciproquement il clair que tout mot réduit de longueur ℓ sur $\widetilde{S_q}$ qui est dans $\Lambda(q)$ forme un circuit de longueur ℓ sans retour en arrière.
Les éléments de $S_q(m)$ sont exactement ceux de $\Lambda(q)$ qui s'écrivent $\pm p^\ell w_{m-2\ell}$ où $w_{m-2\ell}$ est un mot réduit de longueur $m-2\ell$ sur $\widetilde{S_p}$ (voir lemmes 46 et 48) d'où le résultat. □

Lemme 57 : *Toute valeur propre μ de $Y_{p,q}$ de module strictement inférieur à $p+1$ a une multiplicité supérieure à $\frac{q-1}{2}$.*

Démonstration : Notons G le sous-groupe de $\mathrm{PGL}_2(\mathbb{F}_q)$ engendré par $S_{p,q}$, c'est-à-dire $\mathrm{PSL}_2(\mathbb{F}_q)$ si p est un carré modulo q et $\mathrm{PGL}_2(\mathbb{F}_q)$ sinon.

Notons, pour $g \in \mathrm{PSL}_2(\mathbb{F}_q)$, $\gamma_g : G \to G$ la multiplication à gauche par g.
$\mathrm{PSL}_2(\mathbb{F}_q)$ agit linéairement à gauche sur $\ell^2(G)$ par l'application suivante : $(g, f) \mapsto f \circ \gamma_{g^{-1}}$. Comme $Y_{p,q}$ est un graphe de Cayley de G, sa matrice agit naturellement sur $\ell^2(G)$ et son action commute avec l'action de $\mathrm{PSL}_2(\mathbb{F}_q)$. Si V_μ est le sous-espace propre de $Y_{p,q}$ associé à μ, V_μ est alors invariant par l'action de $\mathrm{PSL}_2(\mathbb{F}_q)$ donc $\mathrm{PSL}_2(\mathbb{F}_q)$ agit sur V_μ.
Si cette action était triviale, c'est-à-dire si $\forall (g, f) \in \mathrm{PSL}_2(\mathbb{F}_q) \times V_\mu, f \circ \gamma_{g^{-1}} = f$, les éléments de V_μ seraient constants sur $\mathrm{PSL}_2(\mathbb{F}_q)$ et sur $G \setminus \mathrm{PSL}_2(\mathbb{F}_q)$. Soit f non nulle dans V_μ, x dans G où f ne s'annule pas :

$$\mu^2 f(x) = (Y_{p,q}^2 f)(x) = \sum_{(s_1,s_2) \in S_{p,q}^2} f(s_1 s_2 x)$$

puis, comme $\forall (s_1, s_2) \in S_{p,q}^2, s_1 s_2 \in \mathrm{PSL}_2(\mathbb{F}_q)$,

$$\mu^2 f(x) = |S_{p,q}^2| f(x) = (p+1)^2 f(x).$$

Comme $f(x) \neq 0$, $|\mu| = p + 1$ ce qui est absurde.
Finalement, l'action de $\mathrm{PSL}_2(\mathbb{F}_q)$ sur V_μ est non trivial ; comme toute représentation non triviale de $\mathrm{PSL}_2(\mathbb{F}_q)$ est de dimension supérieure à $\frac{q-1}{2}$ (voir le théorème 31), $\dim V_\mu \geqslant \frac{q-1}{2}$. □

Lemme 58 : *Pour tout $\varepsilon > 0$ et quand m est pair,*

$$s_q(m) = O\left(\frac{p^{m(1+\varepsilon)}}{q^3} + \frac{p^{\frac{m}{2}(1+2\varepsilon)}}{q}\right).$$

Démonstration : $s_q(m)$ est le nombre de solutions entières de $x_1^2 + q^2(x_2^2 + x_3^2 + x_4^2) = p^m$.
Cette équation implique $q^2 \mid \left(x_1 - p^{\frac{m}{2}}\right)\left(x_1 + p^{\frac{m}{2}}\right)$ donc $x_1 \equiv \pm p^{\frac{m}{2}} [q^2]$ (car q ne peut pas diviser les deux facteurs en même temps) ce qui nous donne au plus $2\left(\frac{p^{\frac{m}{2}}}{q^2} + 1\right)$ choix pour x_1.
Il s'agit maintenant de former $\frac{p^m - x_1^2}{q^2}$ comme somme de trois carrés, ce qui nous donne (d'après le corollaire 10) $O\left(\left(\frac{p^m}{q^2}\right)^{\frac{1}{2}+\varepsilon}\right)$ possibilités.
Ceci finit la preuve. □

Proposition 59 : *Si U_m désigne le m-ième polynôme de Tchebychev,*

i) $\forall x \in \mathbb{R}, U_m(\cosh x) = \frac{\sinh(m+1)x}{\sinh x}$;

ii) $\forall x \in \mathbb{R}, U_m(-\cosh x) = (-1)^m \frac{\sinh(m+1)x}{\sinh x}$;

iii) si m est pair, $\forall x \in \mathbb{R}, U_m(x) \geqslant -(m+1)$.

Démonstration :

i) Soit $x \in \mathbb{R}$:

$$U_m(\cosh x) = U_m(\cos ix) = \frac{\sin(m+1)ix}{\sin ix} = \frac{\sinh(m+1)x}{\sinh x}.$$

ii) Soit $x \in \mathbb{R}$:

$$U_m(-\cosh x) = U_m(\cos(\pi + ix)) = \frac{\sin(m+1)(\pi+ix)}{\sin(\pi+ix)}$$
$$= (-1)^m \frac{\sinh(m+1)x}{\sinh x}.$$

iii) Soit $x \in \mathbb{R}$:
Si $x \in [-1,1]$, notons $x = \cos\theta$; on a alors

$$U_m(x) = \frac{\sin(m+1)\theta}{\sin\theta} \geqslant -(m+1).$$

Sinon, les résultats précédents nous indiquent, comme m est pair que si $\psi = \operatorname{arccosh}|x|$, $U_m(x) = \frac{\sinh(m+1)\psi}{\sinh\psi} \geqslant 0$.

□

Théorème 60 : *Pour tout $\varepsilon \in \left]0, \frac{1}{6}\right]$, quand q tend vers l'infini, toute valeur propre μ de $Y_{p,q}$ de module différent de $p+1$ vérifie :*

$$|\mu| \leqslant p^{\frac{5}{6}+\varepsilon} + p^{\frac{1}{6}-\varepsilon}.$$

Cela implique en particulier, comme les $Y_{p,q}$ sont connexes, qu'ils forment une famille de graphes expanseurs.

Démonstration : Grâce au lemme 56, la formule de la trace devient :

$$s_q(m) = \frac{2}{n} p^{\frac{m}{2}} \sum_{j=0}^{n-1} U_m\left(\frac{\mu_j}{2\sqrt{p}}\right)$$

Désormais, on supposera que m est pair.
Si μ_q est une valeur propre de $Y_{p,q}$ de plus grand module différent de $p+1$ (en particulier, $|\mu_q| > 2\sqrt{p}$), notons $\psi_q = \operatorname{arccosh}\frac{|\mu_q|}{2\sqrt{p}}$; d'après le lemme 57 et la proposition 59, on a alors :

$$s_q(m) \geqslant \frac{2}{n} p^{\frac{m}{2}} \frac{q-1}{2} \frac{\sinh(m+1)\psi_q}{\sinh\psi_q} - 2p^{\frac{m}{2}}(m+1).$$

Puis par le lemme 58,

$$\frac{q-1}{2n} \frac{\sinh(m+1)\psi_q}{\sinh\psi_q} = O\left(\frac{p^{m(\frac{1}{2}+\varepsilon)}}{q^3} + \frac{p^{m\varepsilon}}{q}\right) + (m+1)$$

ce qui implique, comme $n \leqslant q^3$, que

$$\frac{q-1}{2} \frac{\sinh(m+1)\psi_q}{\sinh\psi_q} = O\left(p^{m(\frac{1}{2}+\varepsilon)} + q^2 p^{m\varepsilon}\right) + q^3(m+1).$$

Choisissons maintenant pour m le plus grand entier pair tel que $p^{\frac{m}{2}} \leqslant q^3$, c'est-à-dire $m = 2\left[3\log_p q\right]$; on a alors :

$$\frac{q-1}{2} \sinh(m+1)\psi_q = O\left(q^{3+6\varepsilon}\right)$$

car $\sinh \psi_q < \cosh \psi_q < p+1$.
Supposons maintenant par l'absurde qu'il existe une suite strictement croissante $(q_j)_{j\in\mathbb{N}}$ d'entiers naturels telle que pour tout $j \in \mathbb{N}$, $|\mu_{q_j}| > p^{\frac{5}{6}+\varepsilon} + p^{\frac{1}{6}-\varepsilon}$ c'est-à-dire, pour tout $j \in \mathbb{N}$, $\psi_{q_j} > \left(\frac{1}{3}+\varepsilon\right)\log p$.
Comme m tend vers l'infini en même temps que j, pour tout j assez grand,

$$\sinh(m+1)\psi_{q_j} \geqslant \frac{e^{(m+1)\psi_{q_j}}}{3} \geqslant \frac{e^{(-1+6\log_p q_j)\psi_{q_j}}}{3} \geqslant \frac{e^{6\log_p q_j \psi_{q_j}}}{3\sqrt{p}}.$$

Cela donne alors :

$$\frac{q_j - 1}{2} = O\left(q_j^{3+6\varepsilon-\frac{6\psi_{q_j}}{\log p}}\right)$$

donc quand j devient grand, $\psi_{q_j} \leqslant \left(\frac{1}{3}+\varepsilon\right)\log p$ ce qui contredit l'hypothèse faite ci-dessus. □

Références

[1] G. Davidoff, P. Sarnak, A. Valette, *An elementary construction of Ramanujan graphs*, prépublication.

[2] A. Lubotzky, *Discrete groups, expanding graphs and invariant measures*, Progress in Mathematics **125**, Birkhäuser, 1994.

[3] G. A. Margulis, *Explicit construction of concentrators*, Problems Inform. Transmission **9** (1973), 325-332.

[4] A. Lubotzky, R. Phillips and P. Sarnak, *Ramanujan conjectures and explicit construction of expanders*, Proc. Symp. on Theo. of Comp. Sci., **86** (1986), 240-246.

[5] A. Lubotzky, R. Phillips and P. Sarnak, *Ramanujan graphs*, Combinatorica **8** (1988), 261-277.