Le mémoire est sur le livre [1]. La partie du livre que je écris est la seconde moitié du chapitre 1, chapitre 3 total et la première moitié du chapitre 4.

1 Théorie des graphes

1.1 Comportement asymptotique des valeurs propres

On discutera les valeurs propres associées à un graphe. On suppose que tous les graphes n'ont pas de lacets.

D'abord, pour le comportement asymptotique de μ_1, on a le théorème suivant.

Théorème 1.1. *Soit $(X_m)_{m\geq 1}$ une famille des graphes connexes, k-réguliers, finis et $|X_m| \to \infty$ quand $m \to \infty$. Alors*

$$\liminf_{m\to\infty} \mu_1(X_m) \geq 2\sqrt{k-1}.$$

Pour le comportement asymptotique de la valeur propre minimale, il y a un théorème similaire.

Définition 1.2. *La maille d'un graphe connexe X, dénotée $g(X)$, est la longueur minimale d'un cycle de X. Si X est un arbre, on dit que $g(X) = +\infty$.*

Théorème 1.3. *Soit $(X_m)_{m\geq 1}$ une famille des graphes connexes, k-réguliers, finis, et $g(X_m) \to \infty$ quand $m \to \infty$. Alors,*

$$\limsup_{m\to\infty} \mu(X_m) \leq -2\sqrt{k-1},$$

où $\mu(X)$ est la valeur propre minimale de X.

Cela nous inspire de faire la définition suivante.

Définition 1.4. *Un graphe fini connexe k-régulier X est un graphe de Ramanujan, si pour quelconque valeur propre μ de X, on a $|\mu| \leq 2\sqrt{k-1}$.*

1.2 Preuve de comportement asymptotique

On démontrera les théorème et on définira aussi quelques quantités d'un graphe.

Définition 1.5. *Soit X un graphe, Un chemin et X de longueur r et sans retour est une suite $x_0, \cdots, x_r$ des sommets telle que pour tout $1 \leq i \leq r-1$, $x_{i-1} \neq x_{i+1}$. On définit la matrice A_r par*

$(A_r)_{xy}$ = *le nombre des chemins de longueur r, sans retour, et $x_0 = x, x_r = y$.*

En particulier, $A_0 = I$ et A_1 est la matrice d'adjacence A. On peut calculer la fonction génératrice de (A_r).

Proposition 1.6. *Les matrices A_n satisfont les relations récursives suivantes.*

- $A_1^2 = A_2 + kI$.
- *Pour* $r \geq 2$, $A_1 A_r = A_r A_1 = A_{r+1} + (k-1)A_{r-1}$.

Donc la fonction génératrice est le suivant:

$$\sum_{i=0}^{\infty} A_t t^r = \frac{1-t^2}{1-At+(k-1)t^2}.$$

On peut aussi définir les matrices (T_r) par le suivant.

Définition 1.7.

$$T_m = \sum_{0 \leq r \leq \frac{m}{2}} A_{m-2r}.$$

Alors la fonction génératrice de T_m *est*

$$\sum_{m=0}^{\infty} T_m t^m = \frac{1}{1-At+(k-1)t^2}.$$

On trouve que la fonction génératrice est similaire avec celle du polynôme de Tchebychev $U_m(\cos x) = \frac{sin(m+1)x}{\sin x}$:

$$\sum_{m=1}^{\infty} U_m(x) t^m = \frac{1}{1-2xt+t^2}.$$

Donc on a la proposition suivant.

Proposition 1.8. *Pour* $m \in \mathbb{N}$,

$$T_m = (k-1)^{\frac{m}{2}} U_m(\frac{A}{2\sqrt{k-1}}).$$

Par calculer les traces des deux côtés, on a le suivant.

Proposition 1.9.

$$\sum_{x \in V} \sum_{0 \leq r \leq \frac{m}{2}} (A_{m-2r})_{xx} = (k-1)^{\frac{m}{2}} \sum_{j=0}^{n-1} U_m(\frac{A}{2\sqrt{k-1}})$$

On retourne la preuve des théorèmes. Pour simplicité, on démontrera seulement une version faible, i.e., on suppose aussi $g(X_n) \to \infty$ dans 1.1.

On considère la mesure

$$\nu_n = \frac{1}{|X_n|} \sum_{j=1}^{|X_n|-1} \delta_{\frac{\mu_j(X_n)}{\sqrt{k-1}}}$$

Les mesures (v_n) ont le comportement asymptotique suivant.

Proposition 1.10. *Soit $(X_n)_{n\geq 1}$ une famille des graphes connexes, k-réguliers, finis, et $g(X_n) \to \infty$ quand $n \to \infty$. Alors pour tout fonction continue f sur $[-\frac{k}{\sqrt{k-1}}, \frac{k}{k-1}]$,*

$$\lim_{n\to\infty} \int_{[-\frac{k}{\sqrt{k-1}}, \frac{k}{k-1}]} f(x) d\nu_n(x) = \int_{[-2,2]} f(x) \frac{k\sqrt{1-x^2/4}dx}{\pi((k-1)^{1/2} + (k-1)^{-1/2}) - x^2}.$$

Démonstration. La proposition peut être démontrée par montrer le cas $f = U_m$ car les (U_m) engendrent l'espace de Banach $C([-\frac{k}{\sqrt{k-1}}, \frac{k}{k-1}])$. Le cas $f(x) = U_m(\frac{x}{2})$ suit des calculations directes. Par proposition 1.9,

$$\int_{[-\frac{k}{\sqrt{k-1}}, \frac{k}{k-1}]} f(x) d\nu_n(x) = \frac{1}{|X_m|}(k-1)^{-\frac{m}{2}} \sum_{x\in V} \sum_{0\leq r\leq \frac{m}{2}} (A_{m-2r})_{xx}$$

car $(A_{m-2r})_{xx} = 0$ pour n suffisament grand, le droite côté égale à 0 si m est impair et 1 si $(k-1)^{-\frac{m}{2}}$ est impair. Le résultat coïncide avec le résultat du droite côté. □

Alors, en prenant f une fonction qui est zéro sur $[2, 2-\epsilon]$ et qui est 1 sur $[2-\frac{\epsilon}{2}, 2]$ et qui est linéaire sur $[2-\epsilon, 2-\frac{\epsilon}{2}]$, on peut montrer que pour tout $\epsilon > 0$, il existe $C > 0$ tel que le nombre des valeurs propres dans l'intervalle $[(2-\epsilon)\sqrt{k-1}, k]$ soit plus que $|X_n|$ quand $n \to \infty$. Donc 1.1 suit. 1.3 suit par un argument similaire.

1.3 La taille maximale d'un stable et le nombre chromatique

On définira deux invariants d'un graphe: la taille maximale d'un stable d'un graphe, et le nombre chromatique d'un graphe.

Définition 1.11. *Soit X un graphe.*

- *Le nombre chromatique de X, dénoté $\chi(X)$, est le nombre minimale $m \in \mathbb{N}$, satisfaisant qu'il existe une partition $X = X_1 \cup X_2 \cdots \cup X_m$, telle que pour tout i, les sommets dans X_i soient deux à deux non-adjacents.*
- *Un stable de X est un sous-ensemble S de X, tel que les sommets de S soient deux à deux non-adjacents. La taille maximale d'un stable est dénotée $i(X)$.*

Il est clair que $|X| \leq i(X)\chi(X)$ par définition. Des deux invariants sont liées aux valeurs propres.

Proposition 1.12. *Soit X un graphe fini, connexe, k-régulier et $|X| = n$. Alors*

$$i(X) \leq \frac{n}{k} \max\{|\mu_1|, |\mu_{n-1}|\}.$$

Donc

$$\chi(X) \geq \frac{k}{\max\{|\mu_1|, |\mu_{n-1}|\}}.$$

En particulier, si X est un graphe de Ramanujan non-biparti, $\chi(X) \geq \frac{k}{2\sqrt{k-1}}$.

Il y a une tension de la maille $g(X)$ et le nombre chromatique $\chi(X)$. Si le nombre des arêtes croît, $g(X)$ décroît et $\chi(X)$ croît et vice versa. Mais on peut montrer que pour toute paire de nombre (m, n), il existe un graphe X tel que $g(X) \geq m$ et $\chi(X) \geq n$. Il y a une preuve probabilistique d'Erdős mais on donnera explicitement les graphes $X^{p,q}$ dans section 4, qui satisferont cette condition.

2 Le groupe $\mathrm{PSL}(2, q)$

2.1 Propriétés élementaires de $\mathrm{PSL}(2, q)$

On discutera les propriétés de $\mathrm{PSL}(2, q)$ dans cette section. D'abord on définit le groupe $\mathrm{PSL}(2, q)$.

Définition 2.1. *Soit K un corps commutatif. Rappelons le groupe linéaire général $\mathrm{GL}(2, K)$ et le groupe linéaire spécial $\mathrm{SL}(2, K)$. Le groupe $\mathrm{PGL}(2, K)$ est le quotient*

$$\mathrm{PGL}(2, K) = \mathrm{GL}(2, K)/\{\lambda I \mid \lambda \in K^\times\}.$$

$$\mathrm{PSL}(2, K) = \mathrm{SL}(2, K)/\{\lambda I \mid \lambda = \pm 1\}.$$

Le morphisme de quotient $\mathrm{GL}(2, K) \to \mathrm{PGL}(2, K)$ est dénoté par ϕ. Quand K est le corps fini $\mathbb{F}_q$, les groupes sont dénotés $\mathrm{GL}(2, q)$, $\mathrm{SL}(2, q)$, $\mathrm{PGL}(2, q)$, $\mathrm{PSL}(2, q)$ respectivement.

Le groupe $\mathrm{GL}(2, K)$ agit sur l'espace projectif $P^1(K)$, par $Az = \frac{a_{11}z+a_{12}}{a_{21}z+a_{22}}$ si $A = (a_{ij})$. L'action peut descendre à $\mathrm{PGL}(2, K)$.

La première propriété essentielle de $\mathrm{PSL}(2, K)$ est la simplicité.

Théorème 2.2. *Si $|K| > 4$, $\mathrm{PSL}(2, K)$ est un groupe simple.*

La preuve utilise le lemme suivant.

Lemme 2.3. *Pour tout corps commutatif K, le groupe $\mathrm{SL}(2, K)$ est engendré par les éléments de la forme*

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \text{ ou } \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix}$$

Maintenant on peut montrer le théorème.

Démonstration. Pour un sous-groupe normal non-trivial de N, choisissons une matrice non-scalaire A de ϕ^N. Il existe ainsi un vecteur v tel que $\{v, Av\}$ soit une base de K^2. A est représentée par (i.e. conjuguée à) la matrice

$$\begin{pmatrix} 0 & -1 \\ 1 & d \end{pmatrix}$$

sous cette base. Notons que pour tout $U \in \phi^{-1}N$ et $V \in \mathrm{SL}(2, K)$, le commutateur $[U, V]$ est dans N. Donc le commutateur $[B, [C, A^{-1}]^{-1}] \in N$ pour

$$B = \begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix}, C = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix}.$$

On peut calculer que le commutateur égale à

$$\begin{pmatrix} 1 & \mu(\alpha^4 - 1) \\ 0 & 1 \end{pmatrix}.$$

Pour $|K| = 4$ ou $|K| > 5$, il existe $\alpha \in K^\times$ tel que $\alpha \neq 0$. Donc tous les éléments de la forme

$$\begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix}$$

est dans $\phi^{-1}(N)$. Par conjugaison et 2.3, $\phi^{-1}(N)$ doit être égal à $\mathrm{SL}(2, K)$. Le cas que $q = 5$ est démontré par le fait que $\mathrm{PSL}(2, \mathbb{F}_5)$ est isomorphe au groupe alterné A_5. □

La deuxième propriété concerne les sous-groupes de $\mathrm{PSL}(2, q)$.

Définition 2.4. *Un groupe G est métabélien s'il existe un sous-groupe distingué N de G tel que N et G/N soient abéliens.*

Théorème 2.5. *Soit q un nombre premier. Si H est un propre sous-groupe de $\mathrm{PSL}(2, q)$ et $|H| > 60$, alors H est métabélien.*

Le théorème se divise à deux propositions suivantes.

Proposition 2.6. *Si H est un propre sous-groupe de $\mathrm{PSL}(2, q)$ et $p \mid |H|$, alors H est métabélien.*

Démonstration. Par le théorème de Sylow, il existe un sous-groupe L de H de ordre p. S'il existe deux sous-groupes différents d'ordre p de H, par le théorème de Jordan (ou par considérer l'action de $\mathrm{PSL}(2, q)$ sur $P^1(q)$), il existe une base de $\mathrm{PSL}(2, q)$ tel que des générateurs des deux groupes soient conjugués à

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \text{ et } \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix}$$

alors par le lemme 2.3, $H = \mathrm{PSL}(2, q)$, une contradiction. Donc il y a un unique sous-groupe L de H d'ordre p. En particulier, le groupe est normal. Le groupe L est conjugué au groupe

$$U = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \mid a \in \mathbb{F}_q \right\}.$$

Le normalisateur du groupe est donc

$$B := \left\{ \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \mid a \in \mathbb{F}_q^\times, b \in \mathbb{F}_q \right\}.$$

Donc une conjugaison de H est dans B. La proposition suit que B/U et U sont abéliens. □

Proposition 2.7. *Si $|H| > 60$ et q ne divise pas $|H|$, alors H a un sous-groupe d'indice 2.*

La preuve utilise les deux lemmes suivant.

Lemme 2.8. *Soit G un groupe fini et Z est dans le centre de G. Supposons que pour tout $g \in G - Z$, le centralisateur de g $C_G(g)$ est abélien. Alors pour deux sous-groupes abéliens maximaux J, K de G, soit $J = K$, soit $J \cap K = Z$.*

Le cas que $G = \mathrm{SL}(2, q)$, Z est le groupe des matrices scalaires satisfait la condition.

Démonstration. Il est clair que $J \cap K \supset Z$, Si $J \cap K \neq Z$, choisissons $g \in J \cap K - Z$. Alors $C_G(g)$ est abélien et il contient J et K. Par la maximalité, $C_G(g) = J = K$. □

Lemme 2.9. *Soit H un sous-groupe de $\mathrm{SL}(2, q)$ et q ne divise pas H. Soit J un sous-groupe abélien maximal de H. Alors J a indice au plus 2 dans son normalisateur $N_H(J)$.*

Démonstration. Si $J \subset \{\pm 1\}$, par maximalité $H = J$. Sinon, il existe un élément $g \in \mathrm{SL}(2, q)$ dont les deux valeurs propres sont différentes. Donc l'action de g sur $P^1(q^2)$ a deux points fixés, a, b. Les éléments de J peuvent être simultanément diagonalisés. Donc les éléments de J fixent les deux points. Les éléments de $N_H(J)$ fixent l'ensemble a, b. Donc il y a un homomorphisme $N_H(J) \to \mathfrak{S}_2$ dont noyau contient J. Donc $[N_H(J) : J] \leq 2$. □

On peut maintenant démontrer la proposition et alors on finira la preuve du théorème 2.4.

Démonstration. Pour tel H, on dénote $\tilde{H} = \phi^{-1}(H)$, $h = |H|$. (ϕ: SL $\to$ PSL). Alors $|\tilde{H}| = 2h$. Soit $C_1, \cdots, C_s, C_{s+1}, \cdots, C_{s+t}$ les classes de conjugaison des sous-groupes abéliens maximaux de $\tilde{H}$ telles que un quelconque représentatif J_i de C_i satisfasse satisfaisant $[N_{\tilde{H}}(J_i) : J_i] = 1$ pour $i \leq s$ et $[N_{\tilde{H}}(J_i) : J_i] = 2$ pour $i \geq s$. On dénote $|J_i| = 2g_i$.

Notons que par 2.8, l'intersection de quelconques deux différents sous-groupes sont le groupe des scalaires $\{\pm 1\}$. On déduit l'équation suivante:

$$\begin{aligned} 2h - 2 &= \sum_{J \text{ maximal}} (|J| - 2) = \sum_{i=1}^{s+t} (|J_i| - 2) \frac{|\tilde{H}|}{|N_{\tilde{H}}(J_i)|} \\ &= \sum_{i=1}^{s} \frac{(g_i - 1)2h}{g_i} + \sum_{i=s+1}^{s+t} \frac{(g_i - 1)2h}{g_i}. \end{aligned}$$

De l'équation on déduit que

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

On peut résoudre l'équation par discuter tous les cas et montrer qu'il existe i tel que $h = g_i$ ou $h = 2g_i$, qui démontre le théorème. □

2.2 Théorie des représentations de groupe $\mathrm{PSL}(2, q)$

On montrera le théorème suivant sur les représentations de $\mathrm{PSL}(2, q)$.

Théorème 2.10. *Soit $q > 5$ un nombre premier. Alors le degré de quelconque représentation non-triviale est au moins $\frac{q-1}{2}$.*

D'abord, on rappelle quelques notions et conséquences élémentaires dans la théorie des représentations sans preuve. On suppose que tous les espaces vectoriels sont sur $\mathbb{C}$ et de dimension finie.

Définition 2.11. *On fixe un groupe fini G.*

- *Une représentation de G est une action ρ de G sur un espace vectoriel V.*
- *Une sous-représentation de V est une sous-espace W de V tel que $g(W) \in W$.*
- *Une représentation irréductible est une représentation $V \neq 0$ dont sous-représentation est soit 0 soit V.*
- *Une représentation semi-simple est une somme directe des représentations irréductibles. On peut montrer que tous les représentations sont semi-simples.*
- *On peut définir un homomorphisme de deux représentation naturellement.*
- *Il y a quelques opérations sur la catégorie des représentations: somme directe, produit tensoriel, homomorphisme internel, dual, etc.*

Pour un ensemble X avec G-action, l'espace $\mathbb{C}X$ des fonctions $X \to \mathbb{C}$ a une structure naturelle de G-représentation.

Un outil de la théorie des représentations est le caractère.

Définition 2.12. *Pour une représentation (V, ρ) de G, le caractère χ_V et la fonction $G \to \mathbb{C}$ définite par*

$$\chi_V(g) = \mathrm{tr}\ (\mathrm{g}).$$

Il y a une notion de produit scalaire des représentations.

$$\langle \pi, \rho \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_\rho(g) \overline{\chi_\pi(g)}$$

Les caractères satisfont les propriétés suivantes.

Proposition 2.13. *On fixe un groupe fini G et deux représentations (V, π), (W, ρ).*

- $\chi_{\pi\oplus\rho} = \chi_\pi + \chi_\rho$, $\chi_{\pi\oplus\rho} = \chi_\pi + \chi_\rho$, $\chi_{\pi^*} = \bar{\chi}_\pi$.
- $\dim \hom_G(\pi, \rho) = \langle \pi, \rho \rangle$.
- *Une représentation est irréductible si et seulement si le produit scalaire de son caractère et lui-même et* 1.
- *Les caractères des représentations irréductibles sont orthogonales.*

On utilisera les conséquences suivantes dans la preuve du théorème.

Proposition 2.14. *Soit $V_1, \cdots, V_n$ tous les représentations irréductibles de G (au sens d'isomorphisme). Alors il y a une identité*

$$\sum_{i=1}^{n} (\dim V_i)^2 = |G|.$$

Proposition 2.15. *Soit X un ensemble avec G-action. On définit le sous-espace*

$$W_0 := \{f \colon X \to \mathbb{C} \mid \sum_{x\in X} f(x) = 0\} \subset \mathbb{C}X$$

qui a une structure de G-représentation. Si l'action de G sur X est 2-transitive, la représentation W_0 est irréductible.

Maintenant on peut démontrer le théorème.

Démonstration. D'abord, on considère le groupe $ax + b$, i.e., le groupe B des transformations affines de $\mathbb{F}_q$. L'action est 2-transitive. Donc la représentation correspondante W_0 est irréductible. On a $\dim_{W_0} = q - 1$.

Alors on considère le sous-groupe B_0 de $\mathrm{PSL}(2, q)$ des matrices triangulaires supérieures. B_0 agit naturellement sur $\mathbb{F}_q$ et s'identifie avec le sous-groupe des $a^2x + b$, un sous-groupe de B d'indice 2.

Le groupe des matrices diagonales est un quotient de B_0, qui est un groupe abélien de cardinalité $\frac{q-1}{2}$. Donc B_0 a $\frac{q-1}{2}$ représentations de dimension 1. La représentation de B_0 sur W_0 se décompose à deux sous-représentations:

$$\begin{aligned} W_+ &= \langle e_c \mid c \in \mathbb{F}_q^2 \rangle \\ W_- &= \langle e_c \mid c \in \mathbb{F}_q - \mathbb{F}_q^2 \rangle \end{aligned}$$

où $e_c \colon \mathbb{F}_q \to \mathbb{C}$ est donnée par $e_c(x) = \exp(\frac{2\pi i c x}{q})$. Les B_0-représentations sont irréductibles car la B-représentation W_0 est irréductible et $[B : B_0] = 2$. Les deux représentations sont de dimension $\frac{q-1}{2}$. La somme des carrés des tous les B_0-représentations au-dessus sont $\frac{q(q-1)}{2}$, la cardinalité de B_0. Donc les représentations sont tous les représentations irréductibles de B_0.

On retourne vers le théorème. Pour une représentation non-triviale V, Car le groupe $\mathrm{PSL}(2,q)$ est simple, l'homomorphisme correspondant $\mathrm{PSL}(2,q) \to \mathrm{GL}(V)$ est injectif. Donc sa réstriction $B_0 \to \mathrm{GL}(V)$ est injectif. On note que tous les représentations de dimension 1 de B_0 annulent $U_0 \in B_0$ (U_0 est le sous-groupe des matrices triangulaires supérieures avec les éléments diagonaux 1). Donc V doit contenir une représentation de dimension $\frac{q-1}{2}$. Donc $\dim V \geq \frac{q-1}{2}$. □

3 Le graphe $X^{p,q}$

Dans cette section on construira le graphe $X^{p,q}$ mentionné dans la première section. Le graphe sera construit comme un groupe de Cayley.

On rappelle quelques définitions propriétés élémentaires de graphe de Cayley.

Définition 3.1. *Soit G un graphe et $S \in G$ un sous-ensemble fini symétrique de G (i.e. $S = S^{-1}$). Le graphe de Cayley $\mathcal{G}(G,S)$ a:*

- *Sommets: les éléments de G.*
- *Arêtes: deux éléments g, h sont liés s'il existe $sinS$ tel que $gs = h$.*

Définition 3.2. *Soit $\mathcal{G}(G,S)$ un graphe de Cayley.*

- *$CG(G,S)$ est simple, transitif aux sommets, $|S|$-régulier.*
- *$\mathcal{G}$ n'a pas de lacets si et seulement si $1 \notin S$.*
- *$\mathcal{G}$ est connexe si et seulement si S engendre G.*
- *Si $\mathcal{G}$ est connexe, $\mathcal{G}$ est biparti si et seulement s'il existe un homomorphisme $G \to \{\pm 1\}$ tel que l'image de S est $\{-1\}$.*

Soit p, q deux nombres premiers impairs différents dans le suivant. Rappelons que dans la théorie des quaternions, on a définit l'ensemble

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

Il a un sous-ensemble

$$S_p = \{\alpha_1, \cdots, \alpha_s, \bar{\alpha}_1, \cdots, \bar{\alpha}_s, \beta_1, \cdots, \beta_t\}$$

des quaternions de norme p et de cardinalité $p+1$, tel que tous les éléments de Λ' peuvent être uniquement écrits comme un produit réduit $\pm p^n s_1 \cdots s_m$ où $s_1, \cdots, s_n \in S_p$.

Définition 3.3. *L'ensemble Λ' est le quotient $\Lambda'/\sim$, où la relation $\sim$ est définit par*

$$x \sim y \iff \exists n \in \mathbb{Z}, x = \pm p^n y.$$

On dénote $Q \colon \Lambda' \to \Lambda$ le quotient.

On a le diagramme commutatif:

$$\begin{array}{ccccccc} & & S_p \in \Lambda' & \xrightarrow{\tau_q} & \mathbb{H}(\mathbb{F}_q)^\times & \xrightarrow{\psi_q} & \mathrm{GL}(2,q) \\ & & \downarrow Q & & \downarrow & & \downarrow \phi_q \\ \Lambda(q) & \longrightarrow & \Lambda & \xrightarrow{\Pi_q} & \mathbb{H}(\mathbb{F}_q)^\times/\mathbb{F}_q^\times & \xrightarrow{\beta} & \mathrm{PGL}(2,q). \end{array}$$

où τ_q est induite par le quotient $\mathbb{H}(\mathbb{Z}) \to \mathbb{H}(\mathbb{F}_q)$, Π_q est le quotient de τ_q, $\Lambda(q)$ est le noyau de Π_q, ψ_q est un isomorphisme entre les deux groupes et β est le quotient de ψ_q.

On suppose $q > 2\sqrt{p}$ dans le reste de la section. Dans ce cas, $\Pi_q \circ Q$ est injective car tous les éléments de S_p a coordonné dans $[-\sqrt{p}, \sqrt{p}]$. En notant que l'isomorphisme ψ_q identifie la norme avec le déterminant, les éléments dans $\psi_q \circ \tau_q$ ont déterminants p. Donc $S_{p,q} := \phi_q \circ \psi_q \circ \tau_q(S_p)$ est dans $\mathrm{PSL}(2,q)$ si et seulement si p est un résidu quadractique modulo p. Donc on fait la définition suivante.

Définition 3.4. *Le graphe $X^{p,q}$ est le groupe de Cayley $\mathcal{G}(G, S_{p,q})$ (la conjugaison dans $\mathbb{H}$ donne $S = S^{-1}$), où*

$$G = \begin{cases} \mathrm{PSL}(2,q) & \left(\frac{p}{q}\right) = 1 \\ \mathrm{PGL}(2,q) & \left(\frac{p}{q}\right) = -1. \end{cases}$$

Il n'est pas clair que $X^{p,q}$ est connexe. On considérera un autre graphe $Y^{p,q}$ pour démontrer cela le processus de preuve donnera aussi une estimation de maille de $X^{p,q}$. Rappelons les notations dans le diagramme commutatif.

Proposition 3.5. *Λ a une structure d'un groupe libre et $\mathcal{G}(\Lambda, Q(S_p))$ est un arbre $p+1$-régulier.*

Démonstration. En notant que la relation $\sim$ est multiplicative, la multiplication sur Λ' induit une multiplication sur Λ. L'identité est $Q(1)$ et l'inversion est induite par la conjugaison de $\mathbb{H}$. La liberté de Λ et le fait que $\mathcal{G}$ est un arbre est justement une interprétation du fait d'unique factorisation. □

Définition 3.6. *Le graphe $Y^{p,q}$ est le graphe de Cayley $\mathcal{G}(\Lambda/\Lambda(q), T^{p,q})$ où $T_{p,q} := \Pi_q \circ Q(\Lambda)$.*

Alors $Y^{p,q}$ est connexe et β identifie $Y^{p,q}$ comme un composant de $X^{p,q}$. Par la transitivité aux sommets, la maille de $Y^{p,q}$ est la même de la maille de $X^{p,q}$. On énonce la proposition suivante sur la maille, qui sera utilisée dans la preuve de $X^{p,q} = Y^{p,q}$.

Proposition 3.7. *On a $g(Y^{p,q}) \geq 2\log_p q$. Si p n'est pas un résidu quadractique de q, on a $g(Y^{p,q}) \geq 4\log_p q - \log_p 4$.*

Démonstration. Supposons que $x_0, x_1, \cdots, x_g = x_0$ se forment un cycle. Par définition du graphe de Cayley, il existe les éléments $s_0, \cdots, s_{g-1} \in S$ tels que $x_{n+1} = x_n \Pi_q \circ Q(s_n)$. Donc le produit $s_0 s_1 \cdots s_{g-1} \in \Lambda(q)$. Par la définition de $\Lambda(q)$, un élément $\alpha = a_0 + a_1 i + a_2 j + a_3 k$ est contenu dans $\Lambda(q)$ si et seulement si $q \mid a_1, a_2, a_3$. Par le fait d'unique factorisation, $(a_1, a_2, a_3) \neq (0, 0, 0)$. Donc la norme du produit $s_0 s_1 \cdots s_{g-1} \in \Lambda(q)$ est au moin q^2. Car la norme de s_n est p, on a $g \geq 2 \log_p q$.

Quand $(\frac{p}{q}) = -1$, écrivons $s_0 s_1 \cdots s_{g-1} = a_0 + a_1 i + a_2 j + a_3 k$. Calculer la norme des deux côtés montre que $p^g \equiv a_0^2 \pmod{q}^2$. Donc $g = 2h$ est pair et $p^h \equiv \pm a_0 \pmod{q}^2$. Supposons que $g < 4 \log_p q - \log_p 4$, alors $p^h < \frac{q^2}{2}$. En notant que $a_0 \leq |a_0 + a_1 i + a_2 j + a_3 k| = p^h$, $|p^h \pm a_0| < q^2$. Donc $p^h = \pm a_0$. Donc $a_1 = a_2 = a_3 = 0$, on a une contradiction. □

Maintenant on peut montrer le théorème suivant.

Théorème 3.8. *Supposons que $p > 5$, $q > p^8$. Le graphe $X^{p,q}$ est connexe. donc les graphes $Y^{p,q}$ et $X^{p,q}$ sont isomorphes.*

Démonstration. Il suffit de démontrer que $S_{p,q}$ engendre $\mathrm{PGL}(2, q)$ si $(\frac{p}{q}) = -1$ et $S_{p,q}$ engendre $\mathrm{PSL}(2, q)$ si $(\frac{p}{q}) = 1$. En tous les deux cas, il suffit de montrer que l'intersection H du groupe engendré par $S_{p,q}$ et du groupe $\mathrm{PSL}(2, q)$ est $\mathrm{PSL}(2, q)$.

Le groupe H a cardinalité plus de 60 (par e.g. le fait que pour tout graphe X, $k+1$-régulier, $g(X) \leq 2 + 2 \log_k |X|$). Donc soit $H = \mathrm{PSL}(2, q)$, soit H est métabélien. Il suffit de démontrer que le dernier cas n'a pas de lieu. Ppur cela, il est équivalent de trouver quatre éléments g_1, g_2, g_3, g_4 de H, tels que le commutateur $[[g_1, g_2], [g_3, g_4]]$ n'est pas 1.

Si $(\frac{p}{q}) = 1$, on prend arbitrairement $g_1 \in S_{p,q}$, g_2 distinct de $g_1^{\pm 1}$, $g_3 = g_1$ et g_4 distinct de $g_1^{\pm 1}, g_2^{\pm 1}$. Alors le commutateur définit un chemin sans retour dans le graphe $X^{p,q}$ de longueur 16. Par la proposition au-dessus sur la maille de $X^{p,q}$, le chemin ne peut pas former un cycle. Donc la valeur du commutateur n'est pas 1.

Le cas $(\frac{p}{q}) = -1$ est similaire. On prend $h_1 \in S_{p,q}$ arbitrairement, h_2 est distinct de $h_1^{\pm 1}$, h_3 distinct de $h_1^{\pm 1}, h_2^{\pm 1}$. Alors on prend $g_1 = h_1 h_3$, $g_2 = h_2 h_3$, $g_3 = h_1 h_2$, $g_4 = h_3 h_2$. On peut montrer que $[[g_1, g_2], [g_3, g_4]]$ définit un chemin de longueur 24 et sans retour. Donc la valeur du commutateur n'est pas 1 par l'argument de maille. □

Référence

[1] G. Davidoff, P. Sarnak, and A. Valette. *Elementary Number Theory, Group Theory and Ramanujan Graphs.* London Mathematical Society Student Texts. Cambridge University Press, 2003.