Présentation Proséminaire : Construction d'une famille de graphes à large maille $\mathcal{G}(SL_2(q)), S_q)$.

Matthieu Karlen
matthieu.karlen@unifr.ch
supervisé par Dr. Ciobotaru Corina

20 décembre 2016

Table des matières

1 Rappels

1.1 Definition 0.12

Soit $(X_m)_{m\geq 1}$ une famille de graphes finis, connexes et k-réguliers, avec $|V_m| \to \infty$ quand $m \to \infty$, où V_m est l'ensemble des sommets de X_m. On dit que cette famille a une **large maille** si pour une constante $C > 0$, on a que la maille $g(X_m)$ du graphe X_m satisfait la condition $g(X_m) \geq (C + o(1))\log_{k-1}|V_m|$, où $o(1)$ est une quantité tendant vers 0 lorsque $m \to \infty$.

1.2 Definition 4.1.1

Soit G un groupe et S un sous-ensemble non vide, fini de G. On suppose que $S = S^{-1}$ est symétrique. Le **graphe de Cayley** $\mathcal{G}(G, S)$ est le graphe composé de l'ensemble de sommets $V = G$ et de l'ensemble d'arêtes

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

1.3 Proposition 3.1.1

Soit q un nombre premier impair. Alors $|SL_2(q)| = q(q^2 - 1)$.

1.4 Lemma 3.2.1

Pour tout corps K, le groupe $SL_2(K)$ est engendré par les 2 sous-groupes suivants :

$$\left\{ \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} : \lambda \in K \right\} \text{ et } \left\{ \begin{pmatrix} 1 & 0 \\ \mu & 1 \end{pmatrix} : \mu \in K \right\}.$$

1.5 Proposition 4.1.2

Soit $\mathcal{G}(G, S)$ un graphe de Cayley. On pose $k = |S|$.
a) $\mathcal{G}(G, S)$ est un graphe simple, k-regulier et sommet-transitif.
b) $\mathcal{G}(G, S)$ n'a pas de boucle si et seulement si $1 \notin S$.
c) $\mathcal{G}(G, S)$ est connexe si et seulement si S engendre G.

1.6 Le groupe libre

Le **groupe libre** $\mathbb{L}_2$ à deux générateurs (engendré par $S = \{a, \ b\}$) est l'ensemble des mots réduits composés d'éléments de $S' = \{a, \ a^{-1}, \ b, \ b^{-1}\}$, muni de la loi de

concaténation. Un mot est dit **réduit** s'il ne contient aucun des séquences suivantes :

$$aa^{-1},\ a^{-1}a,\ bb^{-1},\ b^{-1}b.$$

2 Préambule

Le but de cette présentation est de construire une famille de graphes 4-réguliers à large maille et de donner une borne inférieure explicite à la taille de la maille (constante C dans la définition 0.12). Nous allons travailler avec des graphes de Cayley de $SL_2(q)$, où q est un nombre premier impair.

2.1 Notation

Nous dénoterons par :

$$\tau_q : SL_2(\mathbb{Z}) \to SL_2(q)$$

la réduction modulo q.

2.2 Notation

Nous considérerons les 2 matrices suivantes :

$$A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \in SL_2(\mathbb{Z}) \quad \text{et} \quad B = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \in SL_2(\mathbb{Z}).$$

Notons encore :

$$A_q = \tau_q(A) = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \in SL_2(q) \quad \text{et} \quad B_q = \tau_q(B) = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \in SL_2(q).$$

Comme ces matrices sont dans le groupe spécial linéaire, elle sont inversibles. Nous pouvons donc créer un sous-ensemble non-vide, fini et symétrique de $SL_2(q)$:

$$S_q = \left\{A_q,\ A_q^{-1},\ B_q,\ B_q^{-1}\right\}.$$

On se rappelle que $SL_2(q)$, muni de la multiplication matricielle est un groupe. On peut donc construire le graphe de Cayley suivant :

$$X_q := \mathcal{G}(SL_2(q), S_q).$$

C'est ce graphe qui nous intéressera lors de toute cette présentation.

3 Lemme A.1

Soit q un nombre premier impair et X_q le graphe défini ci-dessus. Alors X_q est 4-regulier et connexe et il possède $q(q^2-1)$ sommets.

Preuve

X_q est 4-régulier car S_q est formé de 4 matrices deux à deux différentes.

X_q possède $|SL_2(q)|$ sommets par définition d'un graphe de Cayley. Par la proposition 3.1.1 b), on a le résultat.

Par la proposition 4.1.2 c), X_q est connexe si et seulement si S_q engendre $SL_2(q)$.

Par le lemme 3.2.1, on sait que $SL_2(q)$ est engendré par les 2 sous-groupes :

$$\left\{ \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} : \lambda \in \mathbb{F}_q \right\} \quad \text{et} \quad \left\{ \begin{pmatrix} 1 & 0 \\ \mu & 1 \end{pmatrix} : \mu \in \mathbb{F}_q \right\}.$$

Montrons que A_q génère ce premier ensemble :

$A_q^l = \tau_q(A^l)\ \forall l \in \mathbb{N}$ car τ_q est un morphisme de groupes. Or :

$$A^l = \begin{pmatrix} 1 & 2l \\ 0 & 1 \end{pmatrix}.$$

Comme q est premier impair, pour tout $\lambda \in \mathbb{F}_q$, il existe $l \in \mathbb{N}$ tel que $\lambda = 2l \bmod q$, et donc :

$$\left\{ \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} : \lambda \in \mathbb{F}_q \right\} =< A_q > .$$

De manière similaire, on montre que :

$$\left\{ \begin{pmatrix} 1 & 0 \\ \mu & 1 \end{pmatrix} : \mu \in \mathbb{F}_q \right\} =< B_q > .$$

Ainsi, S_q génère $SL_2(q)$ et donc X_q est connexe.

□

Comme dans les présentations précédentes, on doit avoir des informations sur le graphe $\mathcal{G}(SL_2(\mathbb{Z}), S)$ où $S = \{A,\ B,\ A^{-1},\ B^{-1}\}$ afin de pouvoir calculer la maille de X_q.

Soit H le sous-ensemble de $SL_2(\mathbb{Z})$ engendré par A et B.

4 Proposition A.2

H est isomorphe au groupe libre $\mathbb{L}_2$ à deux générateurs.

Preuve

H est l'ensemble des mots réduits sur l'alphabet $\{A,\ A^{-1},\ B,\ B^{-1}\}$. En effet,

$$AA^{-1} = A^{-1}A = 1_{SL_2(\mathbb{Z})} \quad \text{et} \quad BB^{-1} = B^{-1}B = 1_{SL_2(\mathbb{Z})}.$$

Tout élément $C \in H$ est d'une des formes suivantes :

— Mot commençant et finissant par une puissance de A :

$$C_{AA} = A^{k_1}B^{l_1}A^{k_2}\dots B^{l_r}A^{k_{r+1}} \text{ où } k_i, l_i \in \mathbb{Z}\setminus\{0\}\ \forall i, j.$$

— Mot commençant et finissant par une puissance de B :

$$C_{BB} = B^{k_1}A^{l_1}B^{k_2}\dots A^{l_r}B^{k_{r+1}} \text{ où } k_i, l_i \in \mathbb{Z}\setminus\{0\}\ \forall i, j.$$

— Mot commençant par une puissance de A et finissant par une puissance de B :

$$C_{AB} = A^{k_1}B^{l_1}A^{k_2}\dots A^{k_r}B^{l_r} \text{ où } k_i, l_i \in \mathbb{Z}\setminus\{0\}\ \forall i, j.$$

— Mot commençant par une puissance de B et finissant par une puissance de A :

$$C_{BA} = B^{k_1}A^{l_1}B^{k_2}\dots B^{k_r}A^{l_r} \text{ où } k_i, l_i \in \mathbb{Z}\setminus\{0\}\ \forall i, j.$$

Nous allons montrer que l'application suivante est une bijection de H dans $\mathbb{L}_2$:

$$\begin{array}{rccc} \psi & : & \mathbb{L}_2 & \to & H \\ & & a & \mapsto & A \\ & & b & \mapsto & B. \end{array}$$

D'après les remarques précédentes, il est évident que ψ est bien définie et est un morphisme de groupes. Par construction, la surjectivité est vérifiée. Pour vérifier l'injectivité, il faut montrer que tout mot non vide est différent de l'identité dans H, ainsi le noyau de ψ sera $\{1_{\mathbb{L}_2}\}$. Pour ce faire, nous allons utiliser le lemme du ping-pong.

Laissons agir $SL_2(\mathbb{Z})$ sur $\mathbb{R}^2$ par la multiplication matrice-vecteur usuelle. Définissons deux sous-ensembles de $\mathbb{R}^2$ de la façon suivante :

— $E = \{(x,\ y) \in \mathbb{R}^2 : |y| > |x|\}$.

— $F = \{(x,\ y) \in \mathbb{R}^2 : |x| > |y|\}$.

Pour $k \in \mathbb{Z}^\star$ et $(x,\ y) \in \mathbb{R}^2$, on a que :

$$A^k(z) = \begin{pmatrix} 1 & 2k \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x + 2ky \\ y \end{pmatrix} \qquad B^k(z) = \begin{pmatrix} 1 & 0 \\ 2k & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ y - 2kx \end{pmatrix}.$$

En séparant les différents cas, on voit que $A^k(E) \subset F$ et $B^k(F) \subset E,\ \forall k \in \mathbb{Z}^\star$.

Prenons maintenant un mot du type C_{AA} et appliquons le à E :

$$\begin{aligned} A^{k_{r+1}}(E) &\subset F \\ B^{l_r}A^{k_{r+1}}(E) &\subset E \\ A^{k_r}B^{l_r}A^{k_{r+1}}(E) &\subset F \\ &\vdots \\ C_{AA}(E) = A^{k_1}B^{l_1}A^{k_2}\dots B^{l_r}A^{k_{r+1}}(E) &\subset F \end{aligned}$$

Comme $E \cap F = \emptyset$, on a que $C_{AA} \neq 1_{SL_2(\mathbb{Z})}$.

Pour traiter les mots du troisième type, C_{AB}, utilisons une petite astuce. Choisissons $k \in \mathbb{Z},\ k \neq k_1$. Alors $A^{-k}C_{AB}A^k$ est un mot du type C_{AA} et n'est donc pas la matrice identité. Ceci implique directement que C_{AB} n'est pas non plus l'identité.

Les 2 cas restants sont similaires.

Ainsi, tout mot non vide de H n'est pas égal à l'élément neutre. On a donc : $\mathrm{Ker}(\psi) = \{1_{\mathbb{L}_2}\}$. ψ est donc injectif.

On a ainsi montré que ψ est un isomorphisme entre H et $\mathbb{L}_2$.

□

Définition

Soit $||.||_v$ la norme euclidienne sur $\mathbb{R}^2$. La **norme d'opérateur** d'une matrice $T \in M_2(\mathbb{R})$ est définie comme :

$$||T|| = \sup\left\{ \frac{||Tv||_v}{||v||_v} : v \in \mathbb{R}^2 \setminus \{(0,\ 0)\} \right\}.$$

5 Lemme A.3

Soit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Notons A^T sa transposée. Alors

1. $||A|| = \left|\left|A^T\right|\right|$.
2. $||A|| = \left|\left|A^T A\right|\right|^{\frac{1}{2}}$.

3. $||A|| \geq \max\{|a|,\ |b|,\ |c|,\ |d|\}$.
4. Si A est symétrique avec valeurs propres $\lambda_1,\ \lambda_2 \in \mathbb{R}$, alors $||A|| = \max\{|\lambda_1|,\ |\lambda_2|\}$.

Sans démonstration (voir lemme A.3 dans le livre.) □

6 Calcul préparatoire

Afin de préparer le résultat du théorème suivant, calculons la norme d'opérateur des matrices A et B définies en debut de présentation et de leur inverses.

$$A^T A = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 2 & 5 \end{pmatrix}.$$

Le polynôme caractéristique de $A^T A$ est donc $(1-t)(5-t) - 4 = 1 - 6t + t^2$, dont les racines sont $3 \pm 2\sqrt{2}$.

Comme $A^T A$ est symétrique, on a que $\left|\left|A^T A\right|\right| = 3 + 2\sqrt{2}$ par le lemme A.3.4.

Par le lemme A.3.2, on a directement $||A|| = \sqrt{3 + 2\sqrt{2}} = \sqrt{1 + 2\sqrt{2} + (\sqrt{2})^2} = 1 + \sqrt{2}$.

7 Théorème

Les graphes X_q, pour q premier impair, satisfont :

$$\liminf_{q \to \infty} \frac{g(X_q)}{\log_3 |X_q|} \geq \frac{1}{3\log_3(1+\sqrt{2})} = \frac{\log(3)}{3\log(1+\sqrt{2})} = 0.41549\ldots$$

8 Preuve

Soit q un nombre premier impair fixé. Notons $g = g(X_q)$. Par sommet-transitivité (prop. 4.1.2 a)), X_q possède un circuit sans retour en arrière de longueur g commençant et finissant en $1_{SL_2(q)}$.

Numérotons ce circuit :

$$1_{SL_2(q)} = x_0,\ x_1, \ldots,\ x_{g-1},\ x_g = 1_{SL_2(q)}.$$

X_q étant un graphe de Cayley, on sait qu'il existe $\alpha_i \in S_q,\ i = 0,\ 1, \ldots,\ g-1$ tels que :

$$x_{i+1} = x_i \alpha_i,\ \forall i \in \{0,\ 1, \ldots,\ g-1\}.$$

La réduction modulo q restreinte à S $\tau_{q\,|S} : S \to S_q$ est bijective. Il existe donc une seule préimage de chacun des $\alpha_i,\ i = 0,\ 1, \ldots,\ g-1$ dans $\{A,\ A^{-1},\ B,\ B^{-1}\}$. Nommons ces éléments $\tilde{\alpha_i}$.

Alors $\tilde{\alpha_0}\tilde{\alpha_1}\ldots\tilde{\alpha}_{g-2}\tilde{\alpha}_{g-1} \in H$ est un mot réduit, car le circuit correspondant ne possède pas de retour en arrière. D'après la proposition A.2, on a donc :

$$\tilde{\alpha_0}\tilde{\alpha_1}\ldots\tilde{\alpha}_{g-2}\tilde{\alpha}_{g-1} \neq 1_{SL_2(\mathbb{Z})}.$$

D'autre part, nous avons que $\tau_q(\tilde{\alpha_0}\tilde{\alpha_1}\ldots\tilde{\alpha}_{g-2}\tilde{\alpha}_{g-1}) = \alpha_0\alpha_1\ldots\alpha_{g-2}\alpha_{g-1} = 1_{SL_2(q)}$. En d'autre mots :

$$\tilde{\alpha_0}\tilde{\alpha_1}\ldots\tilde{\alpha}_{g-2}\tilde{\alpha}_{g-1} \in \mathrm{Ker}(\tau_q).$$

Ainsi tous les coefficients de la matrice $\left(\tilde{\alpha_0}\tilde{\alpha_1}\ldots\tilde{\alpha}_{g-2}\tilde{\alpha}_{g-1} - 1_{SL_2(\mathbb{Z})}\right)$ sont divisibles par q.

Comme cette matrice n'est pas identiquement nulle, on en déduit qu'au moins un des coefficients est plus grand ou égal à q.

Par le lemme A.3.3 :

$$\left|\left|\tilde{\alpha_0}\tilde{\alpha_1}\ldots\tilde{\alpha}_{g-2}\tilde{\alpha}_{g-1} - 1_{SL_2(\mathbb{Z})}\right|\right| \geq q.$$

Par inégalité triangulaire de la norme (et sachant que $\left|\left|1_{SL_2(\mathbb{Z})}\right|\right| = 1$), on a :

$$||\tilde{\alpha_0}\tilde{\alpha_1}\ldots\tilde{\alpha}_{g-2}\tilde{\alpha}_{g-1}|| \geq q-1.$$

D'autre part, par la sous-multiplicativité de la norme, on a :

$$||\tilde{\alpha_0}\tilde{\alpha_1}\ldots\tilde{\alpha}_{g-2}\tilde{\alpha}_{g-1}|| \leq \underbrace{||\tilde{\alpha_0}||}_{=1+\sqrt{2}} \cdot \underbrace{||\tilde{\alpha_1}||}_{=1+\sqrt{2}} \cdot \ldots \cdot \underbrace{||\tilde{\alpha}_{g-1}||}_{=1+\sqrt{2}} = \left(1+\sqrt{2}\right)^g.$$

On obtient donc :

$$q-1 \leq \left(1+\sqrt{2}\right)^g.$$

Or, d'après le lemme A.1, $|X_p| = q(q^2-1) = (q-1)^3 \cdot \frac{q\cdot(q+1)}{(q-1)^2}$.

En prenant le logarithme en base 3, on obtient :

$$\log_3\left(|X_q|\right) = \log_3\left((q-1)^3\right) + \underbrace{\log_3\left(\underbrace{\frac{(q+1)\cdot q}{(q-1)^2}}_{<1}\right)}_{<0}$$

Ainsi :

$$\log_3(|X_q|) \leq \log_3\left((q-1)^3\right) \leq 3 \cdot \log_3\left((1+\sqrt{2})^g\right) \leq 3 \cdot g \cdot \log_3\left(1+\sqrt{2}\right)$$

Et donc finalement :

$$g \geq \frac{\log_3(|X_q|)}{3 \cdot \log_3\left(1+\sqrt{2}\right)}.$$

□

9 Exercices

Exercice 1

Enoncé

Pour $T \in M_2(\mathbb{R})$, montrer que $||T||$ est finie. Vérifier que $T \to ||T||$ est bien une norme sur $M_2(\mathbb{R})$.

Résolution

Pour contrôler que $T \to ||T||$ est bien une norme sur $M_2(\mathbb{R})$, il faut vérifier les points suivants :

1. homogénéité : $\forall A \in M_2(\mathbb{R}), \lambda \in \mathbb{R},$ on a $||\lambda A|| = |\lambda| \cdot ||A||$.
2. définie positive : $\forall A \in M_2(\mathbb{R})$ tel que $A \neq 0_{M_2(\mathbb{R})},\ ||A|| > 0_{\mathbb{R}}$.
3. sous-additivité (inégalité triangulaire) : $\forall A,\ B \in M_2(\mathbb{R}),$ on a $||A+B|| \leq ||A|| + ||B||$.
4. compatibilité avec la norme vectorielle : $||Av||_v \leq ||A|| \cdot ||v||_v$
5. sous-multiplicativité : $\forall A,\ B \in M_2(\mathbb{R}),$ on a $||A \cdot B|| \leq ||A|| \cdot ||B||$.

Soient $A,\ B \in M_2(\mathbb{R})$, $A, B \neq 0_{M_2(\mathbb{R})}$, $v \neq 0_{\mathbb{R}^2} \in \mathbb{R}^2$ et $\lambda \neq 0_{\mathbb{R}} \in \mathbb{R}$, $||.||$ la norme d'opérateur dans $M_2(\mathbb{R})$ et $||.||_v$ la norme euclidienne dans $\mathbb{R}^2$.

1.

$$\begin{aligned} ||\lambda \cdot A|| &= \sup\left\{\frac{||\lambda \cdot Av||_v}{||v||_v} : v \in \mathbb{R}^2 \setminus \{(0,\ 0)\}\right\} \\ &= \sup\left\{\lambda \cdot \frac{||Av||_v}{||v||_v} : v \in \mathbb{R}^2 \setminus \{(0,\ 0)\}\right\} \\ &= \lambda \cdot \sup\left\{\frac{||Av||_v}{||v||_v} : v \in \mathbb{R}^2 \setminus \{(0,\ 0)\}\right\} \\ &= \lambda \cdot ||A||. \end{aligned}$$

2. Soit $||A|| = 0$. C'est à dire $\sup\left\{\frac{||Av||_v}{||v||_v} : v \in \mathbb{R}^2 \setminus \{(0,\ 0)\}\right\} = 0$.

   Et donc $\forall v \in \mathbb{R}^2,\ ||Av||_v = 0_{\mathbb{R}}$. Par les propriétés de la norme Euclidienne, on a donc forcément $Av = 0_{\mathbb{R}^2}, \forall v \in \mathbb{R}^2$. v étant arbitraire, on obtient $A = 0_{M_2(\mathbb{R})}$.

3.

$$\begin{aligned}
||A+B|| &= \sup\left\{\frac{||(A+B)v||_v}{||v||_v} : v \in \mathbb{R}^2 \setminus \{(0,\ 0)\}\right\} \\
&= \sup\left\{\frac{||Av+Bv||_v}{||v||_v} : v \in \mathbb{R}^2 \setminus \{(0,\ 0)\}\right\} \\
&\leq \sup\left\{\frac{||Av||_v+||Bv||_v}{||v||_v} : v \in \mathbb{R}^2 \setminus \{(0,\ 0)\}\right\} \\
&= \sup\left\{\frac{||Av||_v}{||v||_v} + \frac{||Bv||_v}{||v||_v} : v \in \mathbb{R}^2 \setminus \{(0,\ 0)\}\right\} \\
&\leq \sup\left\{\frac{||Av||_v}{||v||_v} : v \in \mathbb{R}^2 \setminus \{(0,\ 0)\}\right\} + \sup\left\{\frac{||Bv||_v}{||v||_v} : v \in \mathbb{R}^2 \setminus \{(0,\ 0)\}\right\} \\
&= ||A|| + ||B||\,.
\end{aligned}$$

4. $\frac{||Av||_v}{||v||_v} \leq ||A||$ par définition du suprémum.

5.

$$\begin{aligned}
||AB|| &= \sup\left\{\frac{||(AB)v||_v}{||v||_v} : v \in \mathbb{R}^2 \setminus \{(0,\ 0)\}\right\} \\
&\leq \sup\left\{\frac{||A||\cdot||Bv||_v}{||v||_v} : v \in \mathbb{R}^2 \setminus \{(0,\ 0)\}\right\} \\
&\leq \sup\left\{\frac{||A||\cdot||B||\cdot||v||_v}{||v||_v} : v \in \mathbb{R}^2 \setminus \{(0,\ 0)\}\right\} \\
&= \sup\{||A|| \cdot ||B||\} \\
&= ||A|| \cdot ||B||\,.
\end{aligned}$$

Ainsi, l'application $A \to ||A||$ est bien une norme sur $M_2(\mathbb{R})$.

□

On remarque maintenant

$$||A|| = \sup\left\{\frac{||Av||_v}{||v||_v} : v \in \mathbb{R}^2 \setminus \{(0,\ 0)\}\right\} = \sup\left\{||Av||_v : v \in S_1 = \left\{x \in \mathbb{R}^2 : ||x|| = 1\right\}\right\}.$$

S_1 est compact dans $\mathbb{R}^2$ et toute matrice $A \in M_2(\mathbb{R})$ peut être identifiée à une application linéaire, donc continue. La norme euclidienne est également continue.

L'image d'un compact par une application continue est aussi un compact. Ainsi, $\forall A \in M_2(\mathbb{R}),\ \{Av : v \in S_1\}$ est un compact. L'application $||.||_v$ étant continue, elle y prend donc son maximum. Notons ce maximum M.

Alors $||A|| = \sup\{||Av||_v : v \in S_1\} = M < \infty$.

Ayant choisi une matrice $A \in M_2(\mathbb{R})$ arbitraire, on conclut finalement que $||A||$ est finie $\forall A \in M_2(\mathbb{R})$.

9.1 Exercice 2

9.1.1 Enoncé

Montrer que le théorème A.4 peut être amélioré :

$$\liminf_{q\to\infty} \frac{g(X_q)}{\log_3|X_q|} \geq \frac{2}{3\log_3(1+\sqrt{2})}.$$

9.1.2 Résolution

Au lieu de travailler avec la matrice $\left(\tilde{\alpha}_0 \dots \tilde{\alpha}_{g-1} - 1_{SL_2(\mathbb{Z})}\right)$, on utilise la matrice $\left(\tilde{\alpha}_0 \dots \tilde{\alpha}_{\frac{g-1}{2}} - \tilde{\alpha}_{g-1}^{-1} \dots \tilde{\alpha}_{\frac{g+1}{2}}^{-1}\right)$.

Cela revient à faire la moitié du circuit dans un sens, et l'autre moitié dans l'autre sens. Ainsi, par chacun des deux côtés, on arrive sur le même élément et cette matrice est identiquement nulle dans $SL_2(q)$.

Par les mêmes considérations que dans la preuve du théorème, cette matrice n'est pas nulle dans $SL_2(\mathbb{Z})$.

Ainsi tous ses coefficients sont divisibles par q et au moins l'un d'entre eux est non nul dans $\mathbb{Z}$.

Posons :

$$\left(\tilde{\alpha}_0 \dots \tilde{\alpha}_{\frac{g-1}{2}}\right) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ et } \left(\tilde{\alpha}_{g-1}^{-1} \dots \tilde{\alpha}_{\frac{g+1}{2}}^{-1}\right) = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}.$$

Comme au moins un coefficient de la matrice $\left(\tilde{\alpha}_0 \dots \tilde{\alpha}_{\frac{g-1}{2}} - \tilde{\alpha}_{g-1}^{-1} \dots \tilde{\alpha}_{\frac{g+1}{2}}^{-1}\right)$ est non nul et divisible par q, on a :

$$|x - x'| \geq q, \text{ pour } x \in \{a,\ b,\ c,\ d\}.$$

Alors on a $|x| \geq \frac{q}{2}$ ou $|x'| \geq \frac{q}{2}$.

Par le lemme A.3, on en déduit que la norme d'une des deux matrices est plus grande que $\frac{q}{2}$.

Sans restreindre la généralité, supposons que $\left|\left|\tilde{\alpha}_0 \dots \tilde{\alpha}_{\frac{g-1}{2}}\right|\right| \geq \frac{q}{2}$. (Dans le cas contraire, on considère le circuit dans le sens inverse, et on retombe sur ce résultat.)

Comme dans la preuve du théorème, on peut écrire :

$$\frac{|X_q|}{2^3} \leq \left(\frac{q}{2}\right)^3 \leq \left(\left|\left|\tilde{\alpha}_0 \dots \tilde{\alpha}_{\frac{g-1}{2}}\right|\right|\right)^3 \leq \left(1+\sqrt{2}\right)^{3\cdot\frac{g+1}{2}}.$$

En prenant le logarithme des deux côtés, on obtient :

$$\log_3\left(\frac{|X_q|}{2^3}\right) \leq \log_3\left(\left(1+\sqrt{2}\right)^{3\cdot\frac{g+1}{2}}\right)$$

$$\log_3(|X_q|) - 3\log_3(2) \leq 3\cdot\frac{g+1}{2}\cdot\log_3\left(1+\sqrt{2}\right)$$

$$\log_3(|X_q|) \leq 3\cdot\frac{g+1}{2}\cdot\log_3\left(1+\sqrt{2}\right) + 3\log_3(2)$$

En divisant pas le terme de gauche :

$$1 \leq 3\cdot\frac{g}{2\cdot\log_3(|X_q|)}\cdot\log_3\left(1+\sqrt{2}\right) + \underbrace{3\cdot\frac{1}{2\cdot\log_3(|X_q|)}\cdot\log_3\left(1+\sqrt{2}\right) + \frac{3\log_3(2)}{\log_3(|X_q|)}}_{O\left(\frac{1}{q^2}\right)}$$

Ainsi en prenant la limite :

$$\liminf_{q\to\infty}\frac{g(X_q)}{\log_3(|X_q|)} \geq \frac{2}{3\cdot\log_3(1+\sqrt{2})}.$$

Bibliographie

1. Giuliana Davidoff, Peter Sarnak and Alain Valette , *Elementary Number Theory, Group Theory and Ramanujan Graphs*, London Mathematical Society Student Texts, Appendix A.