Résumé
– Structures de sous-groupes –

Aurelio Privitera

Contact: aurelio.privitera@unifr.ch
Responsable: Dr. Corina Ciobotaru

29.11.2016

Pour établir la propriété de connexité dans les graphes de Ramanujan $X^{p,q}$ on doit d'abord comprendre quelques structures de sous-groupes de $\mathrm{PSL}_2(q)$.

1 Structures de sous-groupes

Rappel. Soient un ensemble X et σ une permutation de X. Pour $x \in X$, l'orbite de x sur σ est l'ensemble $\Omega_x = \{\sigma^k(x) : k \in \mathbb{Z}\}$.

Lemme 1.1. *Soit σ une permutation d'un ensemble X. Si σ est d'ordre p avec p nombre premier, alors chaque orbite σ de X possède soit un élément soit p éléments.*

Preuve. On pose H le sous-groupe engendré par σ dans $\mathrm{Sym}(X)$. La preuve du lemme c'est une aplication directe de la formule suivante:

$$|H| = |\Omega_x| \cdot |H_x|, \text{ où } |H| = p.$$

□

Une première application de ce lemme est le théorème de Cauchy. Ce théorème donne une condition pour l'existence des éléments d'ordre premier dans un groupe fini.

Théorème 1.2 (Théorème de Cauchy)**.** *Soit G un groupe fini, et soit p un nombre premier. Si p divise $|G|$, alors G contient un élément d'ordre p.*

Idée de la preuve. Application du lemme 1.1. □

Pour étudier et comprendre le but principal de notre section on doit d'abord introduire une nouvelle définition.

Définition 1.3. Un groupe G est *métabélien* s'il admet un sous-groupe normal N tel que N et G/N soient abélien.

But. En 1901, le mathématicien américain Dickson a donné une liste des tous les sous-groupes de $\mathrm{PSL}_2(q)$, où q est un nombre premier. En regardant la liste de Dickson, on a remarqué que tous les sous-groupes propres de $\mathrm{PSL}_2(q)$ sont métabéliens, avec deux exceptions:

- Sym(4), d'ordre 24
- Alt(5), d'ordre 60

Notre but est de donner une preuve directe de ce fait. Avec le théorème suivant on peut donner une spiegation à ces deux exceptions trouver par Dickson.

Théorème 1.4. *Soit q un nombre premier. Soit H un sous-groupe propre de $\mathrm{PSL}_2(q)$, tel que $|H| > 60$. Alors H est métabélien.*

Le Théorème 1.4 suit immédiatement des deux résultats suivants.

Proposition 1.5. *Soit q un nombre premier, et soit H un sous-groupe propre de $\mathrm{PSL}_2(q)$. Si q divise $|H|$, alors H est métabélien.*

Proposition 1.6. *Soit q un nombre premier, et soit H un sous-groupe propre de* $\mathrm{PSL}_2(q)$. *Si $|H| > 60$ et q ne divise pas $|H|$, alors H possède un sous-groupe abélien d'indice au plus 2; en particulier H est métabélien.*

Pour prouver les deux Propositions 1.5 et 1.6 on va d'abord donner une description des éléments d'ordre q dans $\mathrm{PSL}_2(q)$.
Rappel. $\varphi : \mathrm{SL}_2(q) \to \mathrm{PSL}_2(q)$ définie par $\varphi(A) = \varphi_A$ désigne la transformation linéaire fractionnaire (transformation de Möbius). En plus on rappelle que $P^1(\mathbb{F}_q) = \mathbb{F}_q \cup \{\infty\}$ est la droite projective sur $\mathbb{F}_q$, c'est-à-dire l'espace projectife sur $\mathbb{F}_q$ de dimension 1 où $\mathbb{F}_q$ est un corps fini avec q éléments tel que $q = p^l$, avec p nombre premier (p est la caractéristique de $\mathbb{F}_q$).

Lemme 1.7. *Soit q un nombre premier. Pour $A \in \mathrm{SL}_2(q)$, les propriétés suivantes sont équivalentes:*

i) φ_A est d'ordre q;

ii) il existe un unique sous-espace unidimensionel D dans $\mathbb{F}_q^2$ tel que A ou $-A$ fixe D point par point;

iii) φ_A est conjugué dans $PGL_2(q)$ à un certain φ_{C_b} avec $b \in \mathbb{F}_q^\times$ et $C_b = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$.

Preuve. On vas donner la preuve rigoureuse de la prémière direction, afin de fournir une description claire des éléments d'ordre q dans $\mathrm{PSL}_2(q)$.
i) $\Rightarrow$ ii) φ_A est la transformation linéaire fractionnaire sur $P^1(\mathbb{F}_q)$.
$\Rightarrow |P^1(\mathbb{F}_q)| = q + 1$ et φ_A est d'ordre q par hypothèse. $\mathbb{F}_q \cup \{\infty\} = \bigsqcup_{x \in P^1(\mathbb{F}_q)} < \varphi_A > x$, où $< \varphi_A >$ est le sous-groupe engendré par φ_A, i.e. $< \varphi_A >= \{\varphi_A^n : n \in \mathbb{Z}\}$. Par le Lemme 1.1 soit $|< \varphi_A > x| = 1$, soit $|< \varphi_A > x| = q$. Supposons toutes les orbites sont d'ordre 1, donc $\forall x \in P^1(\mathbb{F}_q)$ $|< \varphi_A > x| = 1$,

$$\Rightarrow < \varphi_A > x = x \ \forall x \in P^1(\mathbb{F}_q)$$

$\Rightarrow \varphi_A = id$ dans $\mathrm{PSL}_2(q)$, ce qui est une contradiction car φ_A est d'ordre q.

Alors $\exists x \in P^1(\mathbb{F}_q)$ tel que $|< \varphi_A > x| = q$

$$\Rightarrow \exists\ y \notin < \varphi_A > x \text{ tel que } < \varphi_A > y = y$$

$\Rightarrow \varphi_A$ possède un unique point fixe dans $P^1(\mathbb{F}_q)$, ce qui correspond à un sous-espace unidimensionnel D dans $\mathbb{F}_q^2$ qui est globalement invariant sous A (peut seulement faire une dilatation des points sur la droite D). L'application

$$\varphi : \mathrm{SL}_2(q) \to \mathrm{PSL}_2(q)$$

a pour noyau $\left\{\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}\right\}$, donc A peut être ou simplement A, qui est d'ordre q ou $A\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}$, qui est d'ordre $2q$. On analyse ces deux cas:

a) A est d'ordre q. Vu que A agit sur la droite D avec au moins un point fixe (notamment (0,0)), et vu que $|D| = q$, par le Lemme 1.1 A fixe D point par point.

b) A est d'ordre $2q$, alors par la définition de l'ordre on a que $A^{2q} = \mathrm{id}$. On veut montrer que $-A(x) = x\ \forall x \in D$ donc que $-A$ fixe D point par point. On suppose que $A(x) = x\ \forall x \in D$

$$\Rightarrow A = \varphi_A\begin{pmatrix}\lambda & 0\\ 0 & \lambda\end{pmatrix},\ \varphi_A\Big(\begin{pmatrix}\lambda & 0\\ 0 & \lambda\end{pmatrix}x\Big) = x$$

$$\Rightarrow \begin{pmatrix}\lambda & 0\\ 0 & \lambda\end{pmatrix}x = x \Rightarrow \lambda = 1 \Rightarrow \varphi_A = A,$$ ce qui est une contradiction (φ_A est d'ordre q).

Alors A agit sur D par $x \to -x$ et donc $-A$ fixe D point par point.

ii) $\Rightarrow$ iii) **Idée**. Choisir une base $\{e_1, e_2\}$ en $\mathbb{F}_q^2$, avec $e_1 \in D$ et $e_2 \in \mathbb{F}_q^2 \backslash D$ et appliquer la formule de changement de base.

iii) $\Rightarrow$ i) Cette implication est immédiate car φ_{C_b} est d'ordre q. □

Grâce à ce lemme on a donc donné une description des éléments d'ordre q dans $\mathrm{PSL}_2(q)$, en effet on peut affirmer la suivante chose:

Soient A,$B \in \mathrm{SL}_2(q)$ tels que φ_A et φ_B sont d'ordre q. Si A,B fixent globalement la même ligne D dans $\mathbb{F}_q^2$, alors φ_A et φ_B génèrent le même sous-groupe d'ordre q dans $\mathrm{PSL}_2(q)$.

Preuve de la Proposition 1.5. Puisque q divise $|H|$, par le théoreme de Cauchy 1.2 on sait que H contient au moins un sous-groupe d'ordre q.

Assertion. H contient un unique sous-groupe C d'ordre q. **Idée de la preuve**: faire une preuve par contradiction en supposant qu'il y a deux sous-groupes distincts C_1 et C_2 d'ordre q et appliquer le Lemme 1.7.

Soit

$$C = \varphi\left\{\begin{pmatrix}1 & \lambda\\ 0 & 1\end{pmatrix} : \lambda \in \mathbb{F}_q\right\}$$ l'unique sous-groupe dans H (donc normal).

L'action de C sur la ligne projective $P^1(\mathbb{F}_q)$ est une translation: $z \mapsto z + \lambda$. L'unique point fixe de C dans $P^1(\mathbb{F}_q)$ est ∞. Pour tout $\varphi_A \in C$, $\varphi_B \in H$:

$$\varphi_A(\varphi_B(\infty)) = \varphi_B(\varphi_{B^{-1}AB}(\infty)) = \varphi_B(\infty) \text{ car } \varphi_{B^{-1}AB}(\infty) = \infty\ .$$

$\Rightarrow \varphi_B(\infty)$ est fixé par C. Ainsi $\varphi_B(\infty) = \infty$ pour tout $\varphi_B \in H$ (car $C \triangleleft H$), ce qui signifie que H est contenu dans le stabilisateur de ∞ dans $\mathrm{PSL}_2(q)$. Mais cela n'est rien d'autre que le sous-groupe

$$B_0 = \varphi\left\{ \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} : a \in \mathbb{F}_q^{\times} \ , \ b \in \mathbb{F}_q \right\}$$

En prenant comme sous-groupe normal de B_0, le groupe $N = \varphi\left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{F}_q \right\}$, on peut verifier que B_0 est métabélien, alors aussi H vu que $H \subset B_0$. □

Pour prouver la proposition 1.6, nous avons besoin de rappeler une terminologie (définition 1.8) et d'illustrer trois lemmes (1.9, 1.10 et 1.11).

Définition 1.8. Soit G un groupe; soient $J \subseteq H \subseteq G$ deux sous-groupes et soit $g \in G$.

a) Le centralisateur $C_H(g)$ de g dans H est le sous-groupe $C_H(g) = \{h \in H\colon hg = gh\ \}$.

b) Le normalisateur $N_H(J)$ de J dans H est le sous-groupe $N_H(J) = \{h \in H\colon hJh^{-1} = J\}$.

Lemme 1.9. *Soit G un groupe fini, et soit Z un sous-groupe central de G. Supposons que, pour tout $g \in G - Z$, le centralisateur $C_G(g)$ est abélien. Soient J, K deux sous-groupes maximaux abéliens de G. Si $J \neq K$, alors $J \cap K = Z$.*

Idée de la preuve. Prouver d'abord que:

1. Chaque sous-groupe abélien maximal J de G doit contenir Z.

2. Pour tout $g \in G - Z$, le centralisateur $C_G(g)$ est un sous-groupe maximal abélien de G.

Aplliquer les deux points ci-dessus aux hypothèses du lemme. □

Lemme 1.10. *Soit q un nombre premier. Chaque matrice non-scalaire de* $\mathrm{SL}_2(q)$ *possède un centre abélien.*

Idées de la preuve. (assez technique)
• considérer la transformation linéaire fractionnaire (transformation de Möbius) φ_A dans $P^1(\mathbb{F}_{q^2})$ pour trouver des point fixes.
• en sachant que φ_A possède une ou deux solutions dans $P^1(\mathbb{F}_{q^2})$, analyser les deux différentes solutions:

a) φ_A possède un unique point fixe dénoté ∞

b) φ_A possède deux points fixes dénotés 0 et ∞

□

Lemme 1.11. *Soit q un nombre premier impair. Soit H un sous-groupe de $\mathrm{SL}_2(q)$, contenant les matrices scalaires, tel que q ne divise pas $|H|$. Si J est un sous-groupe maximal abélien de H, alors $[N_H(J) : J] \leq 2$.*

Preuve. **Note**: le résultat est trivial quand H est le sous-groupe de matrices scalaires dans $\mathrm{SL}_2(q)$ comme $N_H(H) = H$ et donc $[N_H(H) : H] = [H : H] = 1$.
Idée. Supposer que H, et donc aussi J, contient une certaine matrice non-scalaire A et considérer la transformation linéaire fractionnaire φ_A dans $P^1(\mathbb{F}_{q^2})$. Prouver d'abord par contradiciton que φ_A possède deux points fixes dans $P^1(\mathbb{F}_{q^2})$.

Supposer après que les points fixe de φ_A sont $\{0, \infty\}$. J est abélien et $J \subset N_H(J)$, donc $J \subseteq C_L(A) =$ "fixe $\{0, \infty\}$" avec $L = \mathrm{SL}_2(q^2)$, où

$$C_L(A) = \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} : a \in \mathbb{F}_{q^2}^{\times} \right\}.$$

Pour $g \in J$, $n \in N_H(J)$ et $z \in \{0, \infty\}$, on a

$$g(n(z)) = n(n^{-1}gn(z)) = n(z)$$

car $n^{-1}gn \in J$. $n(z)$ est fixé par J et ceci montre que chaque élément dans $N_H(J)$ agit comme une permutation sur $\{0, \infty\}$. On définit donc un homomorphisme

$$\omega : N_H(J) \to \mathrm{Sym}\ \{0, \infty\}.$$

$\Rightarrow Ker(\omega) \subseteq C_L(A)$ (donc abélien)
$\Rightarrow J \subseteq Ker(\omega)$.
Par maximalité de J on a que $Ker(\omega) = J$. Par le premier théorème d'isomorphisme on a

$$[N_H(J) : J] = [N_H(J)/J] \leq 2 = |\mathrm{Sym}\{0, \infty\}|.$$

□

Preuve de la Proposition 1.6. Soit H un sous-groupe de $\mathrm{PSL}_2(q)$, avec $|H| > 60$, tel que q ne divise pas $|H|$. Par la formule d'ordre de $\mathrm{PSL}_2(q)$ on doit avoir que $q \geq 7$, de plus q est impaire.

La transformation de Möbius $\varphi : \mathrm{SL}_2(q) \to \mathrm{PSL}_2(q)$ a le noyau d'ordre 2.

Pour faire la preuve on a besoin des nouvelles notations. Soit $\tilde{H} = \varphi^{-1}(H)$. En prenant le sous-groupe $P = \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$ dans $\mathrm{SL}_2(q)$, on a par la formule d'indice que $|\tilde{H}| = [\tilde{H} : P] \cdot |P|$, donc si on pose $[\tilde{H} : P] = h$ on a que $|\tilde{H}| = 2h$.
Par le Lemme 1.11 on peut dénoter par $C_1, ..., C_s$ les classes de conjugaison des sous-groupes abéliens maximaux J de $\tilde{H}$ avec $[N_{\tilde{H}}(J) : J] = 1$, et par $C_{s+1}, ..., C_t$ les classes de conjugaison des sous-groupes abéliens maximaux J de $\tilde{H}$ avec $[N_{\tilde{H}}(J) : J] = 2$ ($s + t \geq 1$ car $\tilde{H}$ contient au moins un sous-groupe maximal abélien). Si on prend encore une fois le

sous-groupe $P = \left\{ \pm\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$, alors pour un représentant J_i de C_i, la formule d'indice donne $|J_i| = [J_i : P] \cdot |P| = 2g_i$ avec $g_i = [J_i : P]$.

Assertion. Pour tout matrice non-scalaire $A \in \tilde{H}$, il existe un unique index i $(1 \leq i \leq s+t)$ tel que A est conjugé dans $\tilde{H}$ à un certain élément de J_i.
Idée de la preuve. Prouver l'existense (trivial) et l'unicité par contradiction en supposant que A est conjugué à un élément de J_i et à un élément de J_j et en utilisant le Lemmes 1.10 et 1.9.

Pour un i fixe, le nombre de matrices non-scalire dans $\tilde{H}$ qui sont conjuguées à un certain élément de J_i est $(|J_i|$ - 2)$\cdot |C_i|$ ("-2" à cause du noyau). $Stab_{\tilde{H}}(J_i) = N_{\tilde{H}}(J_i)$, donc par la formule de l'indice on a que $|\tilde{H}| = [\tilde{H} : N_{\tilde{H}}(J_i)] \cdot |N_{\tilde{H}}(J_i)|$.
$[\tilde{H} : N_{\tilde{H}}(J_i)] = |C_i| = \dfrac{|\ \tilde{H}\ |}{|\ N_{\tilde{H}}(J_i)\ |} = \dfrac{|\ \tilde{H}\ |}{|\ J_i\ |\ [N_{\tilde{H}}(J_i) : J_i]}$ et donc $(|J_i|$ - 2$)|C_i| = \frac{(g_i-1)2h}{g_i[N_{\tilde{H}}(J_i):J_i]}$.

$$\Rightarrow 2h \text{ - } 2 = \sum_{i=1}^{s} \frac{(g_i - 1)2h}{g_i} + \sum_{j=s+1}^{s+t} \frac{(g_j - 1)2h}{2g_j},$$

ceci conduit à la **relation de base**: $1 = \dfrac{1}{h} + \sum\limits_{i=1}^{s} \left(1 - \dfrac{1}{g_i}\right) + \sum\limits_{j=s+1}^{s+t} \dfrac{1}{2}\left(1 - \dfrac{1}{g_j}\right)$.
$g_i, g_j \geq 2$, par conséquent 1 - $\dfrac{1}{g_i} \geq \dfrac{1}{2}$ et donc

$$1 \geq \frac{1}{h} + \frac{s}{2} + \frac{t}{4} > \frac{s}{2} + \frac{t}{4}.$$

L'inégalité $1 > \dfrac{s}{2} + \dfrac{t}{4}$ possède exactement cinq solutions entières avec $s \geq 0$, $t \geq 0$ et $s + t \geq 1$. Nous examinons maintentant les cinq solutions cas par cas.

a) **Cas s = 1, t = 0**. La relation de base donne $1 = \dfrac{1}{h} + 1 - \dfrac{1}{g_1}$, i.e. $h = g_1$. Alors $\tilde{H} = J_1$, i.e. $\tilde{H}$ est abélien, donc H est abélien.

b) **Cas s = 1, t = 1**. La relation de base devient $1 = \dfrac{1}{h} + 1 - \dfrac{1}{g_1} + \dfrac{1}{2}(1 - \dfrac{1}{g_2})$, ou $\dfrac{1}{g_1} + \dfrac{1}{2g_2} = \dfrac{1}{2} + \dfrac{1}{h}$. Maintenant $\dfrac{1}{g_1} + \dfrac{1}{4} \geq \dfrac{1}{g_1} + \dfrac{1}{2g_2} > \dfrac{1}{2}$, donc $2 \leq g_1 < 4$.

• On prouve que $g_1 = 2$ par contradiciton en supposant que $g_1 = 3$.

Avec $g_1 = 2$ on en déduit que $h = 2g_2$, i.e. $[\tilde{H} : J_2] = 2$, et $[H : \varphi(J_2)] = 2$. Donc H possède un sous-groupe abélien d'indice 2.

c) **Cas s = 0, t = 1**. Ce cas est impossible.

d) **Cas s = 0, t = 2**. Ce cas est aussi impossible.

e) **Cas s = 0, t = 3**. La relation de base devient $1 = \frac{1}{h} + \frac{1}{2} - \frac{1}{2g_1} + \frac{1}{2} - \frac{1}{2g_2} + \frac{1}{2} - \frac{1}{2g_3}$, qui donne $\frac{1}{2g_1} + \frac{1}{2g_2} + \frac{1}{2g_3} = \frac{1}{h} + \frac{1}{2} > \frac{1}{2}$. Clairement on pose que $g_1 \leq g_2 \leq g_3$.

- Avec des calculs simples nous remarquons d'abord que $g_1 = 2$ et que $g_2 = 2$.
- Grâce à la relation de base, on a le fait suivant: $h = 2g_3$, i.e. $[\tilde{H} : J_3] = 2$, et $[H : \varphi(J_3)] = 2$. Comme dans le cas (b), H possède un sous-groupe abélien d'indice 2.

□