Proséminaire SA 2016
– 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 $X^{p,q}$, qui seront construits à partir du chapitre 4, on doit d'abord comprendre quelques structures de sous-groupes de $\mathrm{PSL}_2(q)$.

Contents

1 Structure de sous-groupes

On va d'abord rappeler que si on a un ensemble X et σ une permutation de X avec $x \in X$, l'orbite de x sous 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. Soit H le sous-groupe engendré par σ dans Sym(X). Par le cours d'Algèbre et Géometrie I/II on sait que pour un groupe on a la formule suivante:

$$|H| = |\Omega_x| \cdot |H_x|.$$

Donc pour $x \in X$, par la formule d'orbite on a que $|\Omega_x| = \frac{|H|}{|H_x|}$, où $H_x = \{\alpha \in H\colon \alpha(x) = x\}$ est le stabilisateur de x dans H. Dans notre cas $|H| = p$ par hypothèse, donc soit $|H_x| = 1$ et $|\Omega_x| = $ p, ou $|H_x| = $ p et $|\Omega_x| = 1$. (On peut remarquer que si $|\Omega_x| = 1$, alors x est un point fixe de σ.) □

Comme première application de ce lemme nous prouvons le théorème de Cauchy. Ce théorème donne une condition pour d'élments 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.*

Preuve. On considère le produit $G^p = G \times G \ldots \times G$ (p facteurs). Soit σ la permutation cyclique des facteurs :

$$\sigma(g_1,g_2,\ldots,g_p) = (g_2,\ldots,g_p,g_1).$$

Clairement σ est une permutation de G^p d'ordre p. Maintenant, soit H le sous-ensemble de G^p défini par

$$H = \{(g_1,g_2,\ldots,g_p) \in G^p : g_1g_2\ldots g_p = 1\ \}.$$

Clairement $|H| = |G|^{p-1}$, puisque nous pouvons choisir librement les p - 1 premières coordonnées dans un p-tuple en H. Si $g_1g_2\ldots g_p = 1$, nous obtenons par la conjugaison ${g_1}^{-1}$ que $g_2\ldots g_pg_1 = 1$, ce qui signifie que H est invariant par σ. À partir de maintenant, nous considérons σ comme une permutation de H. Puisque les orbites de σ partitionnent H, et comme $|H|$ est un multiple de p par hypothèse, on voit que la somme des ordres des orbites de σ dans H est congru à 0 modulo p. Par le lemme 1.1 ci-dessus, les orbites sont soit des points fixes, ou ont p éléments. Comme σ a au moins un point fixe dans H, notamment le p-tuple (1,1,...,1), il doit avoir au moins p - 1 autres points fixes, pour correspondre à la congruence ci-dessus. Un tel point fixe est clairement de la forme $(g,g,\ldots,g)$, avec $g \neq 1$. Ce p-tuple étant un élément de H, il doit satisfaire $g^p = 1$, i.e g est d'ordre p dans G. Ceci conclut la preuve. □

Maintenant nous allons donner une nouvelle définition théorique d'un groupe.

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

En particulier, les groupes abéliens sont aussi métabéliens, et les groupes métabéliens sont résolubles. De plus les sous-groupes de groupes métabéliens sont métabéliens.
En 1901, le mathématicien américain Dickson (1874 - 1954), spécialiste en théorie des nombres et en algèbre, a donné une liste, incluant tous les isomorphismes, de tous les sous-groupes de $\mathrm{PSL}_2(q)$, où q est un nombre premier. En faisant particulièrement attention au cas où q est un nombre premier, et 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 possibles:

- Sym(4), d'ordre 24, qui est résoluble mais pas métabélien
- Alt(5), d'ordre 60, qui est simple non-abélien

Notre but dans cette section est de donner une preuve directe de ce fait.

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 (voir exercice 1 à la fin du script, page 14).*

Pour prouver la proposition 1.5 on va d'abord donner une description des éléments d'ordre q dans $\mathrm{PSL}_2(q)$. On rappelle que $\varphi : \mathrm{SL}_2(q) \to \mathrm{PSL}_2(q)$ définie par $\varphi(A) = \varphi_A$ désigne la carte canonique ou 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 $\mathbb{F}_q$).
Exemple: $\mathbb{R} \to P^1(\mathbb{R}^2) = \mathbb{R}^2/\{0,0\}\Big/ \sim$ avec $(x_1, y_1) \backsim (x_2, y_2)$ si et seulement si $(0,0)$ appartient à la ligne qui passe par (x_1, y_1) et (x_2, y_2).

Notation: pour simplicité de calcul, on pose C_b comme la matrice donnée par $C_b = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$.

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 de $\mathbb{F}_q^2$ *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* $b \in \mathbb{F}_q^\times$

Preuve. i) ⇒ ii) Nous rappelons que φ_A est une transformation linéaire fractionnaire sur $P^1(\mathbb{F}_q)$. Vu que $P^1(\mathbb{F}_q) = \mathbb{F}_q \cup \{\infty\}$, alors $|P^1(\mathbb{F}_q)| = q + 1$ ($|\mathbb{F}_q| = q$) 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. $< \varphi_A >= \{\varphi_A^n : n \in \mathbb{N}\}$. On sait par le lemme 1.1 que soit $|< \varphi_A > x| = 1$, soit $|< \varphi_A > x| = q$. Supposons que 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 $PSL_2(q)$, ce qui est une contradiction car φ_A est d'ordre q

Alors $\exists x \in P^1(\mathbb{F}_q)$ tel que $|< \varphi_A > x| = q$. Vu que $|P^1(\mathbb{F}_q)| = q + 1$, il reste un élément $y \notin < \varphi_A > x$ tel que $< \varphi_A > y = y$. Il en suit par le lemme 1.1 que φ_A possède un unique point fixe dans $P^1(\mathbb{F}_q)$ ce qui correspond à un sous-espace unidimensionnel D de $\mathbb{F}_q^2$ 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 $2q$. Donc A est d'ordre q ou $2q$ dans $\mathrm{SL}_2(q)$. On analyse maintenant 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 $|D| = q$, car la droite D est de la forme $D = \begin{pmatrix} a \\ b \end{pmatrix}\mathbb{F}_q$, ça veut dire qu'il reste $q - 1$ points et par le lemme 1.1 ces points sont soit dans une orbite d'ordre 1, soit dans une orbite d'ordre q. Ce dernier cas n'est pas possible car nous avons exactement p - 1 points, donc chaque point est dans une orbite d'ordre 1 et donc A fixe D point par point.

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

$$\Rightarrow A = \varphi_A \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$$

$$\Rightarrow \varphi_A\left(\begin{pmatrix}\lambda & 0\\ 0 & \lambda\end{pmatrix} x\right) = x$$

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

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

ii) $\Rightarrow$ iii) On choisit une base $\{e_1, e_2\}$ de $\mathbb{F}_q^2$, avec $e_1 \in D$ et $e_2 \in \mathbb{F}_q^2 \backslash D$. La matrice A fixe D point par point dans le sens où $A(D) = D$ ou $A(D) = -D$. La matrice A dans cette base est de la forme $\begin{pmatrix}a & b\\ 0 & d\end{pmatrix}$, avec $a = d = \pm 1$ et $b \neq 0$ car par la formule de changement de base on a que $a = \langle Ae_1, e_1\rangle = 1$ car $Ae_1 = e_1$ vu que $e_1 \in D$, puis $c = \langle Ae_1, e_2\rangle = 0$ car $Ae_1 = e_1$ vu que $e_1 \in D$ et $\langle e_1, e_2\rangle = 0$, et enfin $d = \langle Ae_2, e_2\rangle = 1$. Vu que $A \in \mathrm{SL}_2(q) \to \varphi_A \in \mathrm{PSL}_2(q)$, et par la partie d'avant on a que la matrice A est de la forme

$$\begin{pmatrix}\pm 1 & b\\ 0 & \pm 1\end{pmatrix} \text{ dans la base } e_1 \text{ et } e_2.$$

Par la formule de changement de base on sait que $A = BA_{e_1,e_2}B^{-1}$, donc $A_{e_1,e_2} = B^{-1}AB$ et donc $\varphi_{A_{e_1,e_2}} = \varphi(B^{-1}AB) = \varphi(B^{-1})\varphi_A\varphi(B)$. Cela signifie que, dans $PGL_2(q)$, la transformation φ_A est conjugée à $\varphi_{C_{ab}} = \varphi(B^{-1})\varphi_A\varphi(B)$ avec $B \in GL_2(q)$ et $\varphi(B) \in PGL_2(q)$.

iii) $\Rightarrow$ i) Cette implication est immédiate car φ_{C_b} est d'ordre q, en effet

$\begin{pmatrix}1 & b\\ 0 & 1\end{pmatrix}^q = \begin{pmatrix}1 & qb\\ 0 & 1\end{pmatrix} = id$, car $qb = 0$ ($q = p^l$ où p est la caractéristique de $\mathbb{F}_q$).

□

Par la preuve ci-dessus, on peut affirmer les suivantes choses: soient A,$B \in \mathrm{SL}_2(q)$ tel 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. On va d'abord prouver que H contient un unique sous-groupe d'ordre q. En effet, on suppose par contradiction que C_1 et C_2 sont deux sous-groupes distincts d'ordre q. Par le lemme 1.7 et la remarque ci-dessus, ils correspondent à deux différentes lignes D_1, D_2 dans $\mathbb{F}_q^2$. Choisissons une base $\{e_1, e_2\}$ de $\mathbb{F}_q^2$, avec $e_i \in D_i$ (i = 1,2). En travaillant dans cette base (comme on l'a fait avant), on a que

$$C_1 = \varphi\left\{\begin{pmatrix}1 & \lambda\\ 0 & 1\end{pmatrix} : \lambda \in \mathbb{F}_q\right\} \text{ et } C_2 = \varphi\left\{\begin{pmatrix}1 & 0\\ \mu & 1\end{pmatrix} : \mu \in \mathbb{F}_q\right\}.$$

Par le lemme de la section précedente 3.2.1, le sous-groupe engendré par l'union de C_1 et C_2 est $\mathrm{PSL}_2(q)$; donc on aura que $C_1 \cup C_1 \subseteq H = \mathrm{PSL}_2(q)$, ce qui contredit l'hypothèse que H est un sous-groupe propre de $\mathrm{PSL}_2(q)$.
Alors soit C l'unique sous-groupe d'ordre q de H. Par unicité, C est un sous-groupe normal de H ($C \triangleleft H$), c'est-à-dire que $\forall c \in C, \forall h \in H$ on a que $hch^{-1} \in C$.

Assertion. On prouve que si C est l'unique sous-groupe d'ordre q de H, alors C est normal dans H. Si C est l'unique sous-groupe d'ordre q dans H, alors on a que $C = \{e, a, b, ..., s\}$ avec $|C| = q$. Mais alors $hCh^{-1} = \{heh^{-1}, hah^{-1}, ..., hsh^{-1}\}$ possède q éléments, donc vu que $|C| = |hCh^{-1}| = q$ et comme C est un sous-groupe unique dans H on peut conclure que $C = hCh^{-1}$ et donc $C \triangleleft H$.

Avec la conjugaison dans $\mathrm{PSL}_2(q)$, on peut supposer, par le lemme 1.7, que

$$C = \varphi\left\{\begin{pmatrix}1 & \lambda\\ 0 & 1\end{pmatrix} : \lambda \in \mathbb{F}_q\right\},$$

de sorte que l'action de C sur la ligne projective $P^1(\mathbb{F}_q)$ est une translation: $z \mapsto z + \lambda$. Puisque l'unique point fixe de C dans $P^1(\mathbb{F}_q)$ est ∞, et vu que C est sous-groupe normal de H, on a pour tout $\varphi_A \in C$, $\varphi_B \in H$:

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

et donc $\varphi_B(\infty)$ est fixe sous C. Ainsi $\varphi_B(\infty) = \infty$ pour tout $\varphi_B \in H$ (car $C \subseteq H$), 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

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

parfois appelé le sous-groupe de Borel standard de $\mathrm{PSL}_2(q)$. Si on prend le sous-groupe $N = \varphi\left\{\begin{pmatrix}1 & b\\ 0 & 1\end{pmatrix} : b \in \mathbb{F}_q\right\}$, on peut facilement verifier que N est abélien, $N \triangleleft B_0$, et aussi que le quotient B_0/N est abélien, donc par la définition 1.3, B_0 est métabélien. Vu que B_0 est metabélien, alors H aussi vu que $H \subset B_0$. □

Avant de prouver la proposition 1.6, nous avons besoin d'une terminologie en plus.

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 des éléments en H qui commutent avec g:

$$C_H(g) = \{h \in H\colon hg = gh\ \}.$$

b) Le normalisateur $N_H(J)$ de J dans H est le sous-groupe des éléments de H qui normalisent J:

$$N_H(J) = \{h \in H\colon\ hJh^{-1} = J\}$$

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 $J \cap K = Z$.*

Preuve. Nous remarquons d'abord que chaque sous-groupe abélien maximal J de G doit contenir Z. Effectivement, étant donné que Z est un élément du centre, $JZ = ZJ$ est un groupe abélien contenant J. Par maximalité, on doit avoir $JZ = J$, i.e $Z \subseteq J$.

Assertion. Pour tout $g \in G - Z$, le centralisateur $C_G(g)$ est un sous-groupe maximal abélien de G. En effet, soit J un sous-groupe abélien maximal de G contenant $C_G(g)$. Puisque J commute avec g, c'est-à-dire que $\forall h \in J, \forall g \in G - Z$ on a que $hg = gh$ car J est abélien, nous devons avoir que $J \subseteq C_G(g)$, i.e. $J = C_G(g)$.

Le lemme est maintenant facile à prouver. Si J,K sont des sous-groupes abéliens maximaux de G avec $J \cap K \neq Z$, il existe un élément $g \in (J \cap K)$ - Z. Alors $C_G(g)$ est abélien maximal (par l'assertion), et $J \subseteq C_G(g)$, $K \subseteq C_G(g)$ car J,K sont abéliens. Par maximalité nous devons avoir que $J = C_G(g) = K$. □

Remarque. Notez que l'hypothèse dans le lemme 1.9 est héritée pour un sous-groupe de G contenant Z. Nous montrons maintenant que cette hypothèse est satisfaite pour $\mathrm{SL}_2(q)$, avec q nombre premier.

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

Remarque. Le terme matrice scalaire est utilisé pour désigner une matrice qui est un multiple de la matrice identité (multiplication de la matrice identité par un scalaire).

Preuve. Soit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ une matrice non-scalaire de $\mathrm{SL}_2(q)$. On considère la transformation linéaire fractionnaire (transformation de Möbius) φ_A en $P^1(\mathbb{F}_{q^2})$ pour trouver des point fixes, ou bien la ligne sur le corps avec q^2 éléments. L'équation du point fixe est clairement donnée par:

$$\frac{az + b}{cz + d} = z$$

et donc on cherche des z tel que $cz^2 + z(d - a) - b = 0$. On considère la transformation linéaire fractionnaire (transformation de Möbius) φ_A dans $P^1(\mathbb{F}_{q^2})$ car peut-être que l'équation du point fixe n'a pas une solution dans $P^1(\mathbb{F}_q)$ et donc on doit regarder sur l'extension de corps de $\mathrm{SL}_2(q)$ qui est $\mathrm{SL}_2(q^2)$ ($A \in \mathrm{SL}_2(q) \subset \mathrm{SL}_2(q^2)$). En fait, il peut arriver que le polynôme $cz^2 + z(d - a) - b$ ne soit pas réductible sur $\mathbb{F}_q$ mais dans

$\mathbb{F}_{q^2} = \mathbb{F}_q[x]\Big/_{p(x)}$ (avec $p(x)$ réductible) il est réductible, et donc on peut trouver des solutions (des points fixes).
Vu que A est une matrice non-scalaire, par définition on a que $\varphi_A \neq \mathrm{Id}$. φ_A possède une ou deux solutions dans $P^1(\mathbb{F}_{q^2})$. Nous séparons les deux cas:

a) φ_A possède un unique point fixe; avec la conjugaison de $PGL_2(q^2)$, nous pouvons supposer que ce point fixe est ∞; alors φ_A est une translation:

$$\varphi_A(z) = z + b \ (z \in \mathbb{F}_{q^2}),$$

donc la matrice A est clairement de la forme $A = \pm \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$. Le centralisateur de A dans $\mathrm{SL}_2(q^2)$ est le sous-groupe

$$\{\pm \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}, \lambda \in \mathbb{F}_{q^2}\},$$

qui est abélien.

b) φ_A possède deux points fixes; avec la conjugaison de $PGL_2(q^2)$, nous pouvons supposer que les points fixes sont 0 et ∞. Alors $\varphi_A(z) = \alpha^2 z$ pour un $\alpha \in \mathbb{F}_{q^2}^\times$, $\alpha \neq \pm 1$ (car on suppose que la matrice n'est pas scalaire). Cela signifie que A doit être de la forme:

$$A = \pm \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix}.$$

Alors le centralisateur de A dans $\mathrm{SL}_2(q^2)$ est le sous-groupe diagonal, qui est abélien.

□

Lemme 1.11. *Soit q un nombre premier impair. Soit H un sous-groupe de $\mathrm{SL}_2(q)$, contenant des 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. Le résultat est trivial quand H est le sous-groupe des matrices scalaires dans $\mathrm{SL}_2(q)$ car dans ce cas $N_H(H) = H$ et donc $[N_H(H) : H] = [H : H] = 1$. Donc on peut supposer que H, et donc aussi J, contient une certaine matrice non-scalaire A. Comme dans la preuve du lemme 1.11, on considère la transformation linéaire fractionnaire φ_A sur $P^1(\mathbb{F}_{q^2})$.

Assertion. On va d'abord prouver que φ_A possède deux points fixes sur $P^1(\mathbb{F}_{q^2})$. Effectivement, si φ_A possède seulement un point fixe, alors A est conjugué dans $L = \mathrm{SL}_2(q^2)$ à $\pm \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$. Dans ce cas A est d'ordre q ou $2q$, alors q divise $|H|$, ce qui est

clairement une contradiction.

Avec la conjugaison dans L, on peut supposer que les points fixes de φ_A sont $\{0, \infty\}$. Puisque J est abélien on a que $\forall A \in J$, $AB = BA$ $\forall B \in J$ et donc $BAB^{-1} = A$ $\forall A, B \in J$, ce qui implique que $J \subset N_H(J)$. De plus on a $J \subseteq C_L(A) =$ "fixe $\{0, \infty\}$", où

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

Maintenant, 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 $n^{-1}gn \in J$. Donc $n(z)$ est fixe sous J, alors $n(z) \in \{0, \infty\}$. Ceci montre que chaque élément de $N_H(J)$ agit comme une permutation sur $\{0, \infty\}$, ce qui définit un homomorphisme

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

Clairement le noyau $Ker(\omega)$ est contenu dans $C_L(A)$ car$ker(\omega)$ fixe les points $\{0, \infty\}$, et $Ker(\omega)$ est donc abélien. D'autre part, $Ker(\omega)$ contient J car $\omega(g \in J) =$ id et donc $J \subseteq ker(\omega)$. Puisque J est un sous-groupe maximal abélien de H, on doit avoir $Ker(\omega) = J$. Donc par le premier théorème d'isomorphisme on a

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

□

Preuve de la proposition 1.6. Soit H un sous-groupe de $\text{PSL}_2(q)$, avec $|H| > 60$, tel que q ne divise pas $|H|$. Vu que dans la section précédente on a prouvé que pour q impair $|\text{PSL}_2(q)| = \dfrac{q(q^2-1)}{2}$ et pour q pair $|\text{PSL}_2(q)| = q(q^2-1)$, alors on doit avoir que $q \geq 7$, en particulier q est impair. Comme on l'a défà vu dans le lemme 1.1, la transformation de Möbius

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

possède un noyau d'ordre 2. Soit $\tilde{H} = \varphi^{-1}(H)$. En prenant le sous-groupe $P = \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$ dans $\text{SL}_2(q)$, on sait que ce sous-groupe commute avec tous les éléments de $\text{SL}_2(q)$ et par la formule de l'indice on a $|\tilde{H}| = (\tilde{H} : P) \cdot |P|$, donc si on pose $(\tilde{H} : P) = h$ on a que $|\tilde{H}| = 2h$.
On denote 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 de sous-groupes abéliens maximaux J de $\tilde{H}$ avec $[N_{\tilde{H}}(J) : J] = 2$. Par le lemme 1.11 on sait que ce sont les seules possibilités. Notons que, vu que $\tilde{H}$ contient au moins un sous-groupe maximal

abélien, on a que $s+t \geq 1$. 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 toute matrice non-scalaire $A \in \tilde{H}$, il existe un unique indice i $(1 \leq i \leq s+t)$ tel que A est conjugé dans $\tilde{H}$ à un certain élément de J_i.
Existence: évident car A est contenue dans un certain sous-groupe maximal abélien de $\tilde{H}$, lui-même conjugué à un certain J_i.
Unicité: on suppose que A est conjuguée à un élément de J_i et à un élément de J_j, donc:

$$B_i A B_i^{-1} \in J_i \text{ et } B_j A B_j^{-1} \in J_j$$

pour certains $B_i, B_j \in \tilde{H}$. Alors $A \in B_i^{-1} J_i B_i \cap B_j^{-1} J_j B_j$. Par le lemme 1.10, le groupe $\tilde{H}$ satisfait les hypothèses du lemme 1.9. Vu que $B_i^{-1} J_i B_i$ et $B_j^{-1} J_j B_j$ sont des sous-groupes abéliens maximaux de $\tilde{H}$, il suit du lemme 1.9 que $B_i^{-1} J_i B_i = B_j^{-1} J_j B_j$. Donc J_i et J_j sont conjugués dans $\tilde{H}$. Alors $i = j$. Ce prouve l'assertion.

Grâce à l'assertion qu'on vient de montrer, pour un i fixe, le nombre de matrices non-scalaires dans $\tilde{H}$ qui sont conjuguées à un certain élément de J_i est $(|J_i|$ - 2)$\cdot |C_i|$ (on fait "-2" parce qu'on doit enlever le noyau qui est de deux matrices scalaires et donc est d'ordre 2). Mais vu que $Stab_{\tilde{H}}(J_i) = N_{\tilde{H}}(J_i)$, par la formule de l'indice on a que $|\tilde{H}|$ $= (\tilde{H} : N_{\tilde{H}}(J_i)) \cdot |N_{\tilde{H}}(J_i)|$.
$(\tilde{H} : N_{\tilde{H}}(J_i) = |C_i| = \dfrac{|\ \tilde{H}\ |}{|\ N_{\tilde{H}}(J_i)\ |} = \dfrac{|\ \tilde{H}\ |}{|\ J_i\ |\ [N_{\tilde{H}}(J_i) : J_i]}$, donc en multipliant à droite et à gauche l'égalité par $(|J_i|$ - 2) et en posant à droite $|\tilde{H}| = 2h$ et $|J_i| = 2g_i$, on obtient en simplifiant le valeur 2 l'égalité suivante: $(|J_i|$ - 2$)|C_i| = \frac{(g_i - 1)2h}{g_i[N_{\tilde{H}}(J_i):J_i]}$. Donc

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

Après quelques manipulations, ceci conduit à la **relation de base**:

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

Maintenant, vu que $g_i, g_j \geq 2$, par conséquent $1 \text{ - } \dfrac{1}{g_i} \geq \dfrac{1}{2}$ 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 $s + t \geq 1$:

a) $s = 1, t = 0$

b) $s = 1, t = 1$

c) $s = 0, t = 1$

d) $s = 0, t = 2$

e) $s = 0, t = 3$

Nous examinons maintentant ces solutions cas par cas.

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

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

Assertion. $g_1 = 2$. Sinon, pour $g_1 = 3$, on a que $\frac{1}{3} + \frac{1}{2g_2} > \frac{1}{2}$ i.e. $g_2 < 3$, ou $g_2 = 2$. Alors grâce à la relation de base on a que $h = 12$, ce qui contredit le fait que $h > 60$.

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

c) En fait ce cas est impossible: en effet la relation de base donne $1 = \frac{1}{h} + \frac{1}{2} - \frac{1}{2g_1}$, i.e. $\frac{1}{2} + \frac{1}{2g_1} = \frac{1}{h}$. Ce fait contredit l'inégalité $|\tilde{H}| = 2h \geq |N_{\tilde{H}}(J_1)| = 4g_1$.

d) Ce cas est aussi impossible. En effet la rélation de base donne $1 = \frac{1}{h} + \frac{1}{2} - \frac{1}{2g_1} + \frac{1}{2} - \frac{1}{2g_2}$, ou $\frac{1}{h} = \frac{1}{2}(\frac{1}{g_1} + \frac{1}{g_2})$.

Par le lemme 0.9, le sous-groupe $J_1 \cap J_2$ est exactement le sous-groupe des matrices scalaires, i.e. $|J_1 \cap J_2| = 2$. Donc $2h = |\tilde{H}| \geq |J_1 J_2| = 2g_1 g_2$. Par conséquent $\frac{1}{h} = \frac{1}{2}(\frac{g_1 + g_2}{g_1 g_2} \geq \frac{1}{2})$ $\frac{g_1 + g_2}{h}$, i.e. $g_1 + g_2 \leq 2$, ce qui contredit le fait que $g_1 \geq 2$, $g_2 \geq 2$.

e) 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 $g_1 \leq g_2 \leq g_3$.

- Nous remarquons d'abord que $g_1 = 2$. En effet, en supposant $g_1 \geq 3$, on a que $\frac{1}{2g_1} + \frac{1}{2g_2} + \frac{1}{2g_3} \leq \frac{1}{2}$, ce qui contredit l'inégalité précédente. Alors $\frac{1}{2g_2} + \frac{1}{2g_3} = \frac{1}{h} + \frac{1}{4} > \frac{1}{4}$

- Nous observons maintenant que $g_2 = 2$. En effet, si on avait $g_2 \geq 4$, nous aurions $\frac{1}{2g_2} + \frac{1}{2g_3} \leq \frac{1}{4}$, qui contredit l'inégalité ci-dessus. Mais si $g_2 = 3$, alors $\frac{1}{2g_3} = \frac{1}{h} + \frac{1}{12}$, d'où

$$\frac{1}{12} < \frac{1}{2g_3} = \frac{1}{h} + \frac{1}{12} < \frac{1}{60} + \frac{1}{12} = \frac{1}{10};$$

  i.e. $6 > g_3 > 5$, ce qui ne peut pas arriver.

- Alors on a finalement, grâce à la relation de base, 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.

□

2 Exercices

2.1 Exercice 1

Si un groupe H possède un sous-groupe abélien N d'indice 2, alors H est métabélien.

Solution. On va d'abord prouver que N est un sous-groupe normal de H.
Soit H un groupe et N un sous-groupe de H d'indice 2. Par définition de l'indice, il y a seulement deux classes à gauche de N en G:

$$N,\, h_1N$$

où h_1 est un élément de G qui n'est pas dans N. Notons bien que si h_1, h_2 sont deux éléments de H qui ne sont pas dans N, alors h_1h_2 appartient à N. En effet la classe à gauche $h_1h_2N \neq h_1N$ (car $h_1h_2 = h_1n$ impliquerait immédiatement que $h_2 = n \in N$) et donc $h_1h_2N = N$ et $h_1h_2 \in N$.
Soit $n \in N$ un élément arbitraire de N et soit $h \in H$. Si $h \in N$ alors $hnh^{-1} \in N$ et donc $N \triangleleft H$. Autrement on pose $h \notin N$. Ainsi $hn \notin N$ et par la remarque précédente on a que $hnh^{-1} = (hn)h^{-1} \in N$. Donc $\forall n \in N, \forall h \in H$ on a que $hnh^{-1} \in H \Rightarrow N \triangleleft H$.
Il nous reste à montrer que H/N est abélien. On a vu ci-dessus que si h_1, h_2 sont deux éléments de H qui ne sont pas dans N, alors h_1h_2 appartient à N, alors $h_1h_2h_1^{-1}h_2^{-1} \in N$ aussi, donc

$$H/N \text{ abélien} \Leftrightarrow h_1h_2N = h_1Nh_2N = h_2Nh_1N = h_2h_1N \Leftrightarrow h_1h_2N = h_2h_1N \Leftrightarrow h_1h_2h_1^{-1}h_2^{-1}N = N \Leftrightarrow h_1h_2h_1^{-1}h_2^{-1} \in N. \text{ Donc } H/N \text{ est abélien.}$$

Donc on a prouvé que H possède un sous-groupe normal N abélien et que le groupe quotient H/N est aussi abélien, par la définition de groupe métabélien on peut finalement conclure que H est métabélien.

2.2 Exercice 2

Soit G un groupe. Pour $g_1, g_2 \in G$, on définit le commutateur de g_1, g_2 comme $[g_1, g_2] = g_1g_2g_1^{-1}g_2^{-1}$. Montrer que G est métabélien si et seulement si pour tout $g_1, g_2, g_3, g_4 \in G$:

$$[[g_1, g_2], [g_3, g_4]] = 1$$

.

Solution. On définit le sous-groupe des commutateurs par

$$N = ([x, y] \mid x, y \in G)$$

" $\Leftarrow$ ": On a que

$$[[g_1, g_2], [g_3, g_4]] = 1 \Leftrightarrow [g_1, g_2] \cdot [g_3, g_4] \cdot [g_1, g_2]^{-1} \cdot [g_3, g_4]^{-1} = 1 \Leftrightarrow [g_1, g_2] \cdot [g_3, g_4] = [g_3, g_4] \cdot [g_1, g_2]$$

donc $N = ([x, y] \mid x, y \in G)$ est abélien. Il nous reste à montrer que N est un sous-groupe normal de G et que G/N est aussi abélien.

$$g[x, y]g^{-1} = gxyx^{-1}y^{-1}g^{-1} = gxg^{-1}gyg^{-1}gx^{-1}g^{-1}gy^{-1}g^{-1} = (gxg^{-1})(gyg^{-1})(gx^{-1}g^{-1})(gy^{-1}g^{-1}) = [gxg^{-1}, gyg^{-1}].$$

Alors maintenant si $g \in G$ on a que $gNg^{-1} = g([x, y] \mid x, y \in G)g^{-1} = (g[x, y]g^{-1} \mid x, y \in G) = ([gxg^{-1}, gyg^{-1}] \mid x, y \in G) = ([x, y] \mid x, y \in G) = N$. Finalement on a que N est normal dans G.

$$G/N \text{ abélien} \Leftrightarrow g_1g_2N = g_1Ng_2N = g_2Ng_1N = g_2g_1N \Leftrightarrow g_1g_2N = g_2g_1N \Leftrightarrow g_1g_2g_1^{-1}g_2^{-1}N = N \Leftrightarrow g_1g_2g_1^{-1}g_2^{-1} \in N$$

Vu que $g_1g_2g_1^{-1}g_2^{-1} \in N$ car N est le sous-groupe des commutateurs on a que G/N est abélien.
$\Rightarrow G$ est métabélien. $\square$

" $\Rightarrow$ ": Vu que G est métabélien par hypothèse il admet un sous-groupe normal N tel que N et G/N sont abéliens. On pose

$$N = ([x, y] \mid x, y \in G)$$

qui est comme avant le sous-groupe des commutateurs. Par hypothèse on a que N est un sous-groupe normal abélien de G par définition de métabélien. Cela implique que pour tout $g_1, g_2, g_3, g_4 \in G$ on a que:

$$[g_1, g_2] \cdot [g_3, g_4] = [g_3, g_4] \cdot [g_1, g_2] \Rightarrow [g_1, g_2] \cdot [g_3, g_4] \cdot [g_1, g_2]^{-1} \cdot [g_3, g_4]^{-1} = 1 \Rightarrow [[g_1, g_2], [g_3, g_4]] = 1. \ \square$$

2.3 Exercice 3

a) Avec $a = 1$ on peut vérifier que $N = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ est un sous-groupe abélien de $Aff(K)$ et le quotient donné par $Aff(K) \Big/ \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \right\}$ est aussi abélien.

b) Si on pose comme sous-groupe normal de $H_3(K)$ $N = \begin{pmatrix} 1 & 0 & z \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, on peut facilement voir qu'il est abélien et que le quotient $H_3(K)/N$ est aussi abélien.