Le problème des sous-groupes de congruence

Bulois Michaël

11 décembre 2004

Introduction

On s'intéresse ici à $SL_2(A)$, où A est l'anneau des entiers d'un corps K, avec $K = \mathbb{Q}$, $A = \mathbb{Z}$ ou bien K est une extension quadratique de $\mathbb{Q}$ et $A = \mathcal{O}$ est un $\mathbb{Z}$-module de dimension 2. Un résultat sur les groupes de Lie affirme que $SL_n(A)$ possède la *propriété du sous-groupe normal* pour $n \geqslant 3$; c'est à dire que tout sous-groupe normal du réseau $SL_n(A)$ est soit fini et contenu dans le centre, soit d'indice fini dans $SL_2(A)$. Or, ceci est faux dans le cas de $SL_2(A)$. La seconde question que l'on se pose alors est de savoir si tout sous-groupe d'indice fini de $SL_n(A)$ contient un sous-groupe de la forme $Ker(SL_n(A) \to SL_n(A/I))$, où I est un idéal de A. Si c'est le cas, on dit que $SL_n(A)$ possède la *propriété des sous-groupes de congruence*. Ici encore, $SL_n(A)$ possède la propriété des sous-groupes de congruence pour $n \geqslant 3$, alors que ceci est faux pour $n = 2$. L'objectif de ce papier est de décrire la méthode employé dans le chapitre 3 du livre indien de B. Sury [Su].

Sommaire

1 Préliminaires

1.1 Quelques résultats

Dans le cadre de notre étude, nous aurons besoin des deux résultats suivants :

Lemme 1.1 (du ping pong). *Soit G un groupe agissant sur un ensemble S. Supposons que S_1 et S_2 soient des sous-ensembles de S, avec S_2 non inclus dans S_1, que G_1 et G_2 soient des sous-groupes de G tels que G_1 ait au moins 3 éléments et que les propriétés suivantes soient satisfaites : $\forall\, g \in G_1 \setminus \{1\},\ g(S_2) \subset S_1$ et $\forall\, h \in G_2 \setminus \{1\},\ h(S_1) \subset S_2$. Alors, le sous-groupe engendré par G_1 et G_2 est isomorphe au produit libre de G_1 et G_2.*

Démonstration. Nous allons montrer que les mots de la forme $g_1h_1...g_r$, puis $h_0g_1h_1...g_r$, où $g_i \in G_1 \setminus \{1\}$ et $h_i \in G_2 \setminus \{1\}$, ne peuvent être triviaux. Il est alors facile de se ramener à un de ces deux cas par conjugaison par un élément $h \in G_2$ approprié pour montrer la non-trivialité de tous les mots sur G_1 et G_2.
Un mot de la forme $g_1h_1...g_r$, envoie S_2 dans S_1. Comme $S_2 \not\subset S_1$, $g_1h_1...g_r$ est différent de 1.
Supposons maintenant que $h_0g_1h_1...g_r = 1$. Alors comme $h_0 : S_1 \to S_2$ est injectif, $g = g_1h_1...g_r : S_2 \to S_1$ est surjectif donc bijectif. Soit maintenant $g_0 \in G_1 \setminus \{1, g^{-1}\}$. gg_0 envoie S_2 dans $S_1 = g(S_2)$. Donc g_0 envoie S_2 dans $S_1 \cap S_2$. On en déduit que $g_0^{-1} \in G_1$ vérifie : $S_2 \subset g_0^{-1}(S_1 \cap S_2) \subset S_1$, ce qui est absurde. □

Théorème 1.2. *Soit F_k le groupe non abélien libre à k générateurs ($k \geqslant 2$), alors F_k peut être vu comme sous-groupe d'indice fini de F_2.*

Démonstration. On sait que F_k est le groupe fondamental du bouquet de k cercles :
Or, on sait que le bouquet de k cercles est un revêtement à $k-1$ feuillets du bouquet de 2 cercles (voir par exemple [Go]). Donc F_k apparaît comme un sous-groupe d'indice $k-1$ dans F_2.

□

Par exemple F_4 apparait dans F_2 comme sous-groupe d'indice 3 :
$F_4 = \{a; b^2; ba^2b^{-1}; baba^{-1}b^{-1}\}$.

1.2 Groupes finis de type de Lie et problème du sous-groupe de congruence

Maintenant, posons les quelques définitions suivantes. Etant donné un entier $m > 0$, on appelle *sous-groupe principal de congruence de niveau m* et on note $\Gamma(m)$ le sous-groupe de $SL_2(\mathbb{Z})$: $\{g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \mid g \equiv Id \bmod m\}$. Autrement dit, $\Gamma(m) = Ker(SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/m\mathbb{Z}))$. C'est donc un sous-groupe normal d'indice fini dans $SL_2(\mathbb{Z})$. Tout sous-groupe de $SL_2(\mathbb{Z})$ contenant un sous-groupe principal de congruence est appelé un *sous-groupe de congruence*. En particulier, tout sous-groupe de congruence est d'indice fini. La question que l'on se pose alors pour $SL_2(\mathbb{Z})$, est de savoir si tout sous-groupe d'indice fini est un sous-groupe de congruence ; cela s'appelle posseder la *propriété des sous-groupe de congruence* ; on dira aussi *avoir la CSP* (pour *congruence subgroup property*). Nous allons en fait démontrer que $SL_2(\mathbb{Z})$ ne possède pas la *propriété des sous-groupes de congruence.*
Avant de pouvoir montrer cela, il nous faut étudier un peu la structure de $SL_2(\mathbb{Z})$. On a la

Propriété 1.3. *Le sous-groupe engendré par* $A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ *et* $B = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$ *est libre en* A *et* B *et est d'indice 2 dans* $\Gamma(2)$*, donc d'indice fini dans* $SL_2(\mathbb{Z})$*.*

Démonstration. Posons $G_1 = \langle A \rangle$, $G_2 = \langle B \rangle$, $S_1 = \{z \in \mathbb{C} \mid |Re(z)| > 1\}$ et $S_2 = \{z \in \mathbb{C} \mid |z| < 1\}$. Alors, les hypothèses du lemme du ping pong sont satisfaites et $\langle A; B \rangle$ est libre en A et B.
Montrons maintenant que $\langle A; B \rangle$ est d'indice 2 dans $\Gamma(2)$. La méthode ci-dessous est due à Reiner : Pour $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(2)$, on raisonne par récurrence sur $|c|$ pour montrer que $g \in \pm\langle A; B \rangle$. Si $c = 0$ alors $ad = 1$ et $\pm g \in \langle A \rangle$. Si $|c| > 0$, alors on écrit $a = 2q_1c + r_1$ avec $0 <| r_1 |<| c |$ et on a $A^{-q_1}g = \begin{pmatrix} r_1 & * \\ c & * \end{pmatrix}$. Ensuite, on écrit $c = 2q_2r_1 + r_2$ avec $| r_2 |<| r_1 |<| c |$. Donc par hypothèse de récurrence $B^{-q_2}A^{-q_1}g = \begin{pmatrix} r_1 & * \\ r_2 & * \end{pmatrix} \in \pm\langle A; B \rangle$. Donc $\pm g \in \langle A; B \rangle$. Enfin, $-Id \notin \langle A; B \rangle$ car c'est un élément d'ordre 2. □

2 Sous-groupes non de congruence dans $SL_2(\mathbb{Z})$

Dans cette section, nous allons tout d'abord prouver de manière relativement théorique que $SL_2(\mathbb{Z})$ ne possède pas la propriété des sous-groupes de congruence, puis nous énoncerons le critère de Wohlfahrt imposant une condition nécessaire sur les sous-groupes de congruence, ce qui nous permettra de conclure sur un exemple de sous-groupe non de congruence dans $SL_2(\mathbb{Z})$.

2.1 Contraintes sur certains sous-quotients

On dit que G est impliqué dans A s'il existe B, sous-groupe d'indice fini de A tel que G soit quotient de B.
A l'aide des trois résultats suivants, nous allons montrer que le fait de posséder la propriété des sous-groupes de congruence impose des contraintes sur un sous-groupe G impliqué dans $SL_2(\mathbb{Z})$, contraintes qui sont incompatibles avec la présence d'un groupe libre dans $SL_2(\mathbb{Z})$.

Lemme 2.1. *Soit* G *un groupe fini simple impliqué dans* $PSL_2(\mathbb{Z}/m\mathbb{Z})$*, alors* G *est impliqué dans* $PSL_2(\mathbb{Z}/p^r\mathbb{Z})$ *pour un nombre premier* p *et un exposant* $r \geqslant 1$*.*

Démonstration. Soit $\prod_{i=1}^{k} p_i^{r_i}$, la décomposition en facteurs premiers de m. Alors, par le théorème des restes chinois : $PSL_2(\mathbb{Z}/m\mathbb{Z}) \overset{\varphi}{\cong} \prod_{i=1}^{k} PSL_2(\mathbb{Z}/p_i^{r_i}\mathbb{Z})$ où $\varphi = (\varphi_i)_{i \in [|1,k|]}$ avec $\varphi_i : PSL_2(\mathbb{Z}/m\mathbb{Z}) \to PSL_2(\mathbb{Z}/p_i^{r_i}\mathbb{Z})$. Soient A et B tels que $G \cong A/B$ avec $PSL_2(\mathbb{Z}/m\mathbb{Z}) \supseteq A \supsetneq B$. Alors, par l'isomorphisme φ, on a : $\exists i$, $\varphi_i(B) \subsetneq \varphi_i(A)$. Comme A/B est simple, B est distingué maximal dans A. Or $B \subseteq B.(A \cap K) \triangleleft A$ où $K = \ker(\varphi_i)$. Supposons $B.(A \cap K) = A$, auquel cas tout $a \in A$ s'écrit $a = bk$ avec $b \in B$ et $k \in K$ d'où $\varphi_i(A) \subseteq \varphi_i(B)$ ce qui contredit le choix de i. D'où $B.(A \cap K) = B$, c'est-à-dire

$A \cap K = B \cap K$ et

$$\varphi_i(A)/\varphi_i(B) \cong \frac{A/(A \cap K)}{B/(B \cap K)} \cong A/B \cong G.$$

Conclusion, G est impliqué dans $PSL_2(\mathbb{Z}/p_i^{r_i}\mathbb{Z})$. □

Lemme 2.2. *Soit G un groupe fini simple impliqué dans $PSL_2(\mathbb{Z}/p^r\mathbb{Z})$ pour un nombre premier p. Alors G est impliqué dans $PSL_2(\mathbb{Z}/p\mathbb{Z})$.*

Démonstration. Soit K le noyau du morphisme canonique $\pi : PSL_2(\mathbb{Z}/p^r\mathbb{Z}) \to PSL_2(\mathbb{Z}/p\mathbb{Z})$. Montrons que K est un p-groupe. Tout élément x de K s'écrit $x = Id + pM$ avec $M \in M_2(\mathbb{Z}/p^r\mathbb{Z})$. Donc $x^{p^{r-1}} = Id + \sum_{i=1}^{p^{r-1}} \frac{p^{r-1+i}l}{i!} M^i$. Or la valuation en p de $i!$ est plus petite que $i-1$ donc $x^{p^{r-1}} = 1$ et tout élément de K est d'ordre une puissance de p. K est donc bien un p-groupe, il est en particulier nilpotent.
Par ailleurs, on a :

$$\begin{array}{ccc} PSL_2(\mathbb{Z}/p^i\mathbb{Z}) & & \\ \vee & & \\ A & \overset{\varphi}{} & G \end{array}$$

avec $A \cap K \lhd A$, et comme φ est surjectif, $\varphi(A \cap K) \lhd A$. Or $\varphi(A \cap K)$ est nilpotent et n'est pas égal à G, donc $\varphi(A \cap K) = \{1\}$; φ passe au quotient et :

$$\begin{array}{ccc} PSL_2(\mathbb{Z}/p\mathbb{Z}) & \cong & PSL_2(\mathbb{Z}/p^i\mathbb{Z})/K \\ \vee & & \\ A/(A \cap K) & \overset{\bar{\varphi}}{} & G. \end{array}$$

Donc G est impliqué dans $PSL_2(\mathbb{Z}/p\mathbb{Z})$. □

Lemme 2.3. *Les q sous-groupes de Sylow de $PSL_2(\mathbb{F}_{p^r})$ sont abéliens pour $q \neq 2$; p,q premiers.*

Démonstration. Cette démonstration est un cas particulier d'un article de A.J. Weir [W2]. Notons $l = p^r$. Montrons que les q-Sylows de $GL_2(\mathbb{F}_l)$ sont abéliens pour $q \neq 2$. Tout d'abord, $|GL_2(\mathbb{F}_l)| = l(l-1)(l^2-1)$. Si $q = p$, un p-Sylow est donné par $\begin{pmatrix} 1 & \mathbb{F}_l \\ 0 & 1 \end{pmatrix}$ qui est abélien. Nous supposerons donc dans la suite $q \neq p$. Trois cas se présentent : soit $q \mid l-1$, soit $q \mid l^2-1$ et $q \nmid l-1$, soit les q-Sylows sont trivaux.
Intéressons nous au premier cas : on écrit $l = kq^r + 1$ avec $k \wedge q = 1$, $r \geqslant 1$. Alors $l^2 - 1 = q^r(2k + q^r k^2)$ où $(2k + q^r k^2) \wedge q = 1$ (car $q \neq 2$, $r \geqslant 1$). On en déduit que les q-Sylows de $GL_2(\mathbb{F}_l)$ sont d'ordre q^{2r}. Or le q-Sylow (cyclique) S_q de $(\mathbb{Z}/p\mathbb{Z})^*$ est d'ordre q^r. Donc $\begin{pmatrix} S_q & 0 \\ 0 & S_q \end{pmatrix}$ est un q-Sylow abélien de $GL_2(\mathbb{F}_l)$.
Supposons maintenant que $q \nmid (l-1)$ et $l^2 - 1 = kq^r$ avec $k \wedge q = 1$ et $r \geqslant 1$. Alors, regardons $\mathbb{F}_{l^2}$ comme un espace vectoriel de dimension 2 sur $\mathbb{F}_l$; la multiplication par un élément non nul de F_{l^2} définit un automorphisme de F_{l^2}. Ceci induit une application $\varphi : (\mathbb{F}_{l^2})^* \to GL_2(\mathbb{F}_l)$. φ est injective donc $|Im(\mathbb{F}_{l^2}^*)| = kq^r$ et un q-Sylow de $GL_2(\mathbb{Z}/p\mathbb{Z})$ est isomorphe à un sous-groupe de $(\mathbb{F}_{l^2})^*$ et est donc cyclique. □

On sait que tout groupe libre de rang fini se plonge comme sous-groupe d'indice fini dans $PSL_2(\mathbb{Z})$. En conséquence, tout groupe fini G est impliqué dans $PSL_2(\mathbb{Z})$ et on a : $PSL_2(\mathbb{Z}) \supset F \supset N$ où N est d'indice fini dans $PSL_2(\mathbb{Z})$ avec $F/N \cong G$. Supposons que $SL_2(\mathbb{Z})$ ait la CSP. Alors, comme N est d'indice fini dans $PSL_2(\mathbb{Z})$, il existe $m \in \mathbb{N}$ tel que $N \supseteq \Gamma(m)$ et on a $PSL_2(\mathbb{Z})/\Gamma(m) \cong PSL_2(\mathbb{Z}/m\mathbb{Z}) \supset F/\Gamma(m) \supset N/\Gamma(m)$. Donc $G \cong (F/\Gamma(m))/(N/\Gamma(m))$ est impliqué dans $PSL_2(\mathbb{Z}/m\mathbb{Z})$. En prenant G simple, on sait par les lemmes 2.1 et 2.2 que G est impliqué dans $PSL_2(\mathbb{Z}/p\mathbb{Z})$ pour un nombre premier p. Or, si on pose $G := PSL_3(\mathbb{Z}/q\mathbb{Z})$ et $PSL_2(\mathbb{Z}/p\mathbb{Z}) \supset A \supset B$ avec $G \cong A/B$, les q-Sylows de $PSL_2(\mathbb{Z}/p\mathbb{Z})$ sont abéliens d'après le lemme 2.3. Les q-Sylows de A sont donc abéliens et leur image dans G également. Or l'application : $A \to G$ est surjective donc les q-Sylows de G (qui sont image des q-Sylows de A) sont abéliens. Ceci constitue une contradiction car un q-Sylow de G ([W1]) est donné par

$$\{M \in PSL_3(\mathbb{Z}/q\mathbb{Z}) \mid M = \begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix}\}$$

qui est clairement non abélien. En conclusion $SL_2(\mathbb{Z})$ n'a pas la CSP.

2.2 Théorème de Fricke et critère de Wohlfahrt

Pour exhiber un sous-groupe non de congruence par le raisonnement ci-dessus, il nous faudrait écrire $PSL_3(\mathbb{Z}/3\mathbb{Z})$ comme quotient d'un groupe libre et regarder l'image du groupe diviseur dans $\mathbb{F}_2$ puis dans $SL_2(\mathbb{Z})$, ce qui est relativement laborieux. Nous allons donc énoncer ici le critère de Wohlfahrt [WF], basé sur un théorème de Fricke, qui permet de trouver des exemples plus systématiques de sous-groupes non de congruence.

Tout d'abord, introduisons quelques notions. Nous savons que $SL_2(\mathbb{R})$ agit sur $\mathbb{H}^2$, l'espace hyperbolique de dimension 2, vu comme le demi-plan des nombres complexes à partie imaginaire strictement positive. Cette action s'effectue de la façon suivante :

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az+b}{cz+d}.$$

Cette action peut s'étendre en une action sur $\overline{\mathbb{H}^2} = \mathbb{H}^2 \cup \mathbb{R} \cup \{\infty\}$. Nous dirons d'une matrice $P \in SL_2(\mathbb{Z})$ qu'elle est parabolique si elle fixe un seul point ζ de $\overline{\mathbb{H}^2}$. Alors $\zeta \in \mathbb{Q} \cup \{\infty\}$ et il existe $A \in SL_2(\mathbb{Z})$ tel que $P = A^{-1}U^mA$ avec $A(\zeta) = \infty$ et $U = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. L'entier m ci-dessus est défini de façon unique par P et on appelle $\mid m \mid$ *l'amplitude de* P. Si un sous-groupe Γ de $SL_2(\mathbb{Z})$ contient des matrices paraboliques P, on appelle leurs points fixes les *sommets* de Γ. Etant donné un groupe $\Gamma \subset SL_2(\mathbb{Z})$ et un sommet ζ de Γ, le stabilisateur de ζ dans Γ est engendré par un élément P dont l'amplitude définit l'amplitude de ζ ; cette amplitude ne dépend pas de P.

Tout ceci nous permet de définir *niveau général* d'un groupe $\Gamma \subset SL_2(\mathbb{Z})$ comme étant le plus petit commun multiple des amplitudes de ses sommets (s'il existe). On appelle alors $\hat{\Gamma}(m)$ la cloture normale de U^m et on peut facilement vérifier pour un sous groupe

normal Γ, de niveau général m, que $\Gamma \supset \hat{\Gamma}(m)$. Réciproquement, si $\hat{\Gamma}(m) \subset \Gamma$, alors le niveau général de Γ divise m.

Par ailleurs, on appelle *niveau de Klein* d'un sous-groupe de congruence Γ le plus petit entier m tel que $\Gamma(m) \in \Gamma$. On déduit donc des propriétés du niveau général qu'un sous-groupe de congruence Γ de niveau de Klein l vérifie $\hat{\Gamma}(l) \subset \Gamma(l) \subset \Gamma$. Le niveau général d'un sous-groupe de congruence divise donc son niveau de Klein. Le théorème de Fricke nous donne la réciproque :

Théorème 2.4 (Fricke). *Soit Γ un sous-groupe de congruence de niveau général m. Alors $\Gamma(m) \subset \Gamma$.*

Démonstration. Désignons par l le niveau de Klein de Γ. On sait que $m \mid l$. Prenons $M \equiv Id \bmod m$ et montrons que $M \in \Gamma$. En fait, il suffit de montrer pour $R, S \in \Gamma \cap \Gamma(m)$, que $RMS \in \Gamma$. Nous allons donc nous ramener successivement aux cas $d \wedge l = 1$, puis $b \equiv 0 \bmod l$ et $c \equiv 0 \bmod l$.
Montrons que l'on peut supposer $d \wedge l = 1$. Si ce n'est pas le cas, on a $d \neq \pm 1$, $c \neq 0$ et $d \wedge mc = 1$. Donc, par le théorème de Dirichlet, il existe un entier g tel que $(d+gmc, l) = 1$. Donc, si on remplace M par MU^{gm}, nous avons la propriété voulu. Comme $U^{gm} \in \Gamma \cap \Gamma(m)$, nous pouvons remplacer M par MU^{gm}.
Montrons maintenant que nous pouvons supposer $b \equiv \mathrm{mod} l$. Comme $b \equiv 0 \bmod m$ et $m \mid l$, l'équation $b + hmd \equiv 0 \bmod l$ a une solution h. En remplaçant donc M par $U^{hm}M$, nous avons la condition désirée.
Comme M a pour déterminant 1, on a $ad \equiv 1 \bmod l$ et est congrue modulo l à la matrice

$$M_0 = \begin{pmatrix} a & ad-1 \\ 1-ad & d(2-ad) \end{pmatrix}.$$

En posant donc $L = M^{-1}M_0 \in \Gamma(l)$, on a $L \in \Gamma \cap \Gamma(m)$ et M peut être remplacé par $M_0 = ML$. Enfin M_0 peut s'écrire

$$M_0 = \begin{pmatrix} 1 & 0 \\ 1-d & 1 \end{pmatrix} \left[\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & a-1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right] \begin{pmatrix} 1 & d-1 \\ 0 & 1 \end{pmatrix}.$$

Ces trois matrices sont paraboliques, d'amplitude un multiple de m, donc appartiennent à Γ. On a finalement montré que $M_0 \in \Gamma$ ce qui termine la preuve. □

Corollaire 2.5 (Critère de Wohlfahrt). *Soit $G \leqslant SL_2(\mathbb{Z})$ un sous-groupe d'indice fini et soit m tel que $G \supseteq \left\langle \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \right\rangle^N$, la cloture normale de U^m dans $SL_2(\mathbb{Z})$. Alors, G est un sous-groupe de congruence si et seulement si $G \geqslant \Gamma(m)$.*

2.3 Contre-exemples plus systématiques

Appliquons ceci à un exemple de sous-groupe d'indice fini non de congruence dans $SL_2(\mathbb{Z})$. Pour tout mot g appartenant au groupe libre $\left\langle \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}; \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \right\rangle = \langle A; B \rangle$, on définit $E_A(g)$ comme la somme des exposants de A apparaissant dans g, et on définit de même $E_B(g)$ en remplaçant A par B. E_A définit un morphisme de $\langle A; B \rangle$ dans $\mathbb{Z}$. Pour

tout entier strictement positif l, on pose $\Gamma_l = \{g \in \langle A; B\rangle \mid E_A(g) \equiv E_B(g) \equiv 0 \bmod l\}$. Comme c'est le noyau du morphisme $\langle A; B\rangle \to \mathbb{Z}^2 \to (\mathbb{Z}/l\mathbb{Z})^2$ composé du morphisme abélianisant et de la restriction modulo l, il est normal d'indice l^2. Nous allons montrer que si l a un diviseur premier impair p, alors Γ_l n'est pas un sous-groupe de congruence.

Démonstration. En effet, si Γ_l était de congruence, $\Gamma_p \geqslant \Gamma_l$ le serait. Or $A^p = \begin{pmatrix} 1 & 2p \\ 0 & 1 \end{pmatrix} \in \Gamma_p$, donc, par le critère de Wohlfahrt, on aurait $\Gamma_p \geqslant \Gamma(2p)$. Or ceci n'est pas possible compte tenu de leurs indices respectifs dans $SL_2(\mathbb{Z})$:

$$[SL_2(\mathbb{Z}) : \Gamma_p] = p^2[SL_2(\mathbb{Z}) : \langle A; B\rangle] = 12p^2 \nmid 3p(p^2-1) = [SL_2(\mathbb{Z}) : \Gamma(2p)].$$

□

3 Réseaux de l'espace hyperbolique à quotients libres non abéliens

Dans la présente section, nous allons remplacer $\mathbb{Q}$ par $\mathbb{Q}(\sqrt{-D})$, où D désigne le discriminant de l'extension $\mathbb{Q}(\sqrt{-D})$ sur $\mathbb{Q}$; et nous allons remplacer $\mathbb{Z}$ par $\mathcal{O}$ l'anneau des entiers de $\mathbb{Q}(\sqrt{-D})$. Nous savons que c'est un $\mathbb{Z}$-module de base $(1, w)$ où $w = \dfrac{i\sqrt{D}}{2}$ ou $\dfrac{1+i\sqrt{D}}{2}$ suivant que $D \equiv 0$ ou $-1 \bmod 4$. Enfin, pour d entier strictement positif, désignons par $\mathcal{O}_d$ le sous-anneau d'indice d dans $\mathcal{O}$ définit par $\mathcal{O}_d = \mathbb{Z} \oplus \mathbb{Z}dw$. L'objectif de cette section est de prouver que $SL_2(\mathcal{O})$ n'a pas la propriété des sous-groupes de congruence. Autrement dit, tout sous-groupe de $SL_2(\mathcal{O})$ ne contient pas un noyau de la forme $Ker(SL_2(\mathcal{O}) \to SL_2(\mathcal{O}/I))$ où I est un idéal de $\mathcal{O}$.
Pour cela, il serait très utile de faire apparaître un groupe libre non-abélien comme sous-groupe d'indice fini de $SL_2(\mathcal{O})$. Malheureusement, comme $U = \begin{pmatrix} 1 & \mathcal{O} \\ 0 & 1 \end{pmatrix} \cong \mathbb{Z}^2$ est un sous-groupe de $SL_2(\mathcal{O})$, tout sous-groupe libre de $SL_2(\mathcal{O})$ est d'indice infini. Cependant, Grunewald et Schwermer ont démontré qu'il existait un sous-groupe d'indice fini dans $SL_2(\mathcal{O})$ qui a un quotient libre non abélien ; ce qui suffira à démontrer le fait que $SL_2(\mathcal{O})$ ne possède pas la propriété des sous-groupes de congruence. Cette démonstration s'appuie sur l'action de $SL_2(\mathbb{C})$ sur $\mathbb{H}^3$, l'espace hyperbolique de dimension 3, vu comme $\mathbb{C} \times \mathbb{R}^{>0}$.

3.1 le demi-espace hyperbolique et son groupe d'isométries

En effet, on a la propriété suivante (voir [Su]) :

Propriété 3.1. *$SL_2(\mathbb{C})$ agit sur $\mathbb{H}^3$ de la façon suivante :*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot (z, r) = \left(\frac{\overline{(d-cz)}(az-b) - r^2\bar{c}a}{|cz-d| + r^2\,|c|^2}, \frac{r}{|cz-d| + r^2\,|c|^2} \right).$$

Nous allons maintenant définir pour tout $d > 0$, deux sous-ensembles de $\mathbb{H}^3$, B_d et D_d, qui vérifient les propriétés suivantes :

$$\mathbb{H}^3 = \bigcup_{\gamma \in SL_2(\mathcal{O}_d)} \gamma \cdot B_d$$

$$B_d = \bigcup_{s \in \mathcal{O}_d} \begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix} \cdot D_d.$$

Cela se fait en posant $B_d = \{(z,r) \in \mathbb{H}^3 :\mid uz - v \mid^2 + \mid u \mid^2 \geqslant 1$ pour tout $u, v \in \mathcal{O}_d$ qui engendrent l'idéal $\mathcal{O}_d$ tout entier $\}$ et $D_d = B_d \cap F$ où F est un domaine fondamental pour la translation par les éléments de $\mathcal{O}_d$, par exemple $F = \{(x+iy, r) \mid -\frac{1}{2} \leqslant x \leqslant \frac{1}{2}, -\frac{d}{2} Im(w) \leqslant x \leqslant \frac{1}{2} Im(w)\}$. De plus D_d possède la propriété intéressante suivante qui fait de lui presque un domaine fondamental (voir [Su]) :

Propriété 3.2. *Tout point de $\mathbb{H}^3$ possède un voisinage qui n'intersecte qu'un nombre fini de $\gamma(D_d)$ avec $\gamma \in SL_2(\mathcal{O}_d)$.*

3.2 le théorème de Grunewald Schwermer

Un point crucial de la démonstration du fait que $SL_2(\mathcal{O}_d)$ ne possède pas la propriété des sous-groupes de congruence consiste en le théorème suivant que l'on doit à Grunewald et Schwermer (voir [GS]) :

Théorème 3.3. *Le groupe $SL_2(\mathcal{O})$ a un sous-groupe d'indice fini ayant un quotient libre non-abélien.*

L'idée de la preuve est la suivante. On choisit d un entier positif qui vérifiera les bonnes propriétés. $SL_2(\mathcal{O}_d)$ est alors un sous-groupe d'indice fini de $SL_2(\mathcal{O})$. Par ailleurs, on a une application continue naturelle $\phi : SL_2(\mathcal{O}_d) \to \pi_1(\mathbb{H}^3/SL_2(\mathcal{O}_d), h)$ qui à tout élément $\gamma \in SL_2(\mathcal{O}_d)$ associe l'image dans $\mathbb{H}^3/SL_2(\mathcal{O}_d)$ d'un chemin reliant h et $(\gamma.h)$ dans $\mathbb{H}^3$. Ensuite, nous construirons une application continue $\theta : (\mathbb{H}^3/SL_2(\mathcal{O}_d), h) \to (S, p)$, induisant une application θ_* entre leurs groupes fondamentaux, cet espace S ayant un groupe fondamental libre non-abélien. C'est à ce stade, que nous aurons besoin de choisir un élément d de sorte que S soit un bouquet de $W(d)$ cercles avec $W(d) \geqslant 2$. Enfin, $\theta_* \circ \phi$ sera d'image un groupe libre non abélien. Nous aurons alors démontré le théorème.

Il s'agit maintenant de construire ce morphisme θ. La construction est assez calculatoire, c'est pourquoi nous omettrons ici quelques calculs et nous citerons quelques résultats sans démonstration. Une partie des calculs se trouvent dans [Su]
Tout d'abord, pour tout entier $d > 0$, on pose $W(d)$ l'ensemble des entiers m vérifiant les trois propriétés suivantes :

(i) $(m, d) = 1$, $m \neq 2$

(ii) $4m^2 \leqslant d^2 D - 3$,

(iii) $(m, \mid a + w \mid^2) = 1$ pour tout entier a.

Alors nous admettons le lemme 3.4 :

Lemme 3.4. *Il existe un entier $d > 0$ tel que $W(d)$ ait au moins deux éléments.*

Maintenant, choisissons un tel d et pour tout $m \in W(d)$ et tout n premier avec m, on pose $F_{m,n} = B_d \cap \{(z,r) \in \mathbb{H}^3 \mid\mid Im(z - \frac{ndw}{m}) \mid\leqslant \frac{1}{d^4D^2}\}$. Comme $4m^2 \leqslant d^2D$, on a $F_{m,n} \cap F_{m',n'} = \emptyset$ si $(m,n) \neq (m',n')$. Ces ensembles $F_{m,n}$ vont servir de support aux fonctions θ_m et on pose pour $(z,r) \in B_d$:

$$\theta(z,r) = \begin{cases} -exp\{\pi i d^4 D^2 Im(z - \frac{ndw}{m})\} \text{ si } (z,r) \in F_{m,n} \\ 1 \text{ sinon.} \end{cases}$$

Comme $\mathbb{H}^3 = \bigcap_{\gamma \in SL_2(\mathcal{O}_d)} \gamma.B_d$, nous voudrions induire une fonction $\theta'_m : \mathbb{H}^3/SL_2(\mathcal{O}_d) \to S^1$. Ceci est rendu possible par le lemme suivant :

Lemme 3.5. *Soit $\gamma \in SL_2(\mathcal{O}_d)$, $m \in W(d)$, n premier avec m et $(z,r) \in F_{m,n}$. Si $\gamma(z,r) = (z',r') \in B_d$, alors il existe n' premier avec m tel que $Im(z - \frac{ndw}{m}) = Im(z' - \frac{n'dw}{m})$.*

La démonstration de ce lemme résulte de nombreux calculs qui ne peuvent être exposés ici.

Corollaire 3.6. *La fonction $\theta'_m : \mathbb{H}^3/SL_2(\mathcal{O}_d) \to S^1$ définie par $\theta'_m(\overline{(z,r)}) = \theta_m(\gamma(z,r))$ pour un γ tel que $\gamma(z,r) \in B_d$, est bien définie et ne dépend ni du représentant (z,r) choisi, ni du choix de γ.*

On construit donc le graphe suivant :

$$\begin{array}{ccccccc} & & & & \overset{\Phi=(\Phi_m)_{m\in W(d)}}{} & & \\ SL_2(\mathcal{O}_d) & \overset{\phi}{} & \pi_1(\mathbb{H}^3/SL_2(\mathcal{O}_d), h) & \overset{((\theta'_m)_*)_{m\in W(d)}}{} & \pi_1(S,1) & & H_1(S,\mathbb{Z}) \\ & & & & \| & & \| \\ & & & & F_s & & F_s/[F_s,F_s] \end{array}$$

Il nous suffit donc de montrer que Φ est surjective pour montrer que l'image de $\theta_* \circ \phi$ est un groupe libre non abélien.

Propriété 3.7. *L'application Φ est surjective*

Démonstration. Soit $\gamma \in SL_2(\mathcal{O}_d)$, alors s'il existe $(z,r) \in B_d$ tel que $\gamma(z,r) = (z',r') \in B_d$, on a :

$$\Phi_m(\gamma) = \pm \sharp\{(k,m) = 1 \mid Im(z) \leqslant Im(\frac{kdw}{m}) < Im(z')\}$$

suivant que $Im(z) \leqslant Im(z')$ ou non.
Pour montrer la surjectivité de Φ, nous allons construire pour tout $m \in W(d)$ un élément $\gamma_m \in SL_2(\mathcal{O}_d)$ tel que $\Phi_r(\gamma_s) = \delta_{r,s}$. Tout d'abord, ordonons les éléments $m_1, ..., m_s$ de

$W(d)$ de telle façon que $1 > \frac{r_1}{m_1} > ... > \frac{r_s}{m_s}$ où r_i désigne le plus grand entier plus petit que $m_i/2$, premier avec m_i (ceci est rendu possible par l'assertion $m_i \geqslant 3$). Il existe alors un entier $q_i > m_i - r_i$ tel que $r_i q_i \equiv 1 \bmod m$. Il est également possible de montrer que la congruence $|a_i + dw|^2 \equiv -|bi + dw|^2 \bmod m_i$ possède des solutions a_i et b_i. On considère les matrices

$$\sigma_i = \begin{pmatrix} q_i\overline{(a_i + dw)} & * \\ m_i & r_i(a_i + dw) \end{pmatrix}$$

$$\tau_i = \begin{pmatrix} (m_i - r_i)\overline{(b_i + dw)} & * \\ m_i & q_i(b_i + dw) \end{pmatrix}$$

. Ensuite, on considère les éléments $z_i = \frac{r_i(a_i + dw)}{m_i}$, $z_i' = -\frac{q_i\overline{(a_i + dw)}}{m_i}$, $w_i = \frac{q_i(b_i + dw)}{m_i}$, $w_i' = -\frac{(m_i - r_i)\overline{(a_i + dw)}}{m_i}$, $t_i = \frac{1}{m_i}$, qui sont tels que $\sigma_i(z_i, t_i) = (z_i', t_i)$ et $\tau(w_i, t_i) = (w_i', t_i)$. Or, il est possible de démontrer que tout ces éléments de la forme $(\frac{n(a + dw)}{m}, \frac{1}{m})$ appartiennent à B_d. On en conclue donc que

$$\Phi_{m_j}(\sigma_i) = \sharp\{(k, m_j) = 1 \mid \frac{r_i}{m_i} < \frac{k}{m_j} \leqslant \frac{q_i}{m_i}\},$$

$$\Phi_{m_j}(\tau_i) = -\sharp\{(k, m_j) = 1 \mid \frac{m_i - r_i}{m_i} < \frac{k}{m_j} \leqslant \frac{q_i}{m_i}\},$$

$$\Phi_{m_j}(\gamma_i) = \sharp\{(k, m_j) = 1 \mid \frac{r_i}{m_i} < \frac{k}{m_j} \leqslant \frac{m_i - r_i}{m_i}\} = \delta_{i,j}$$

où $\gamma_i = \sigma_i\tau_i$. Ce qui finit de démontrer la surjectivité de Φ et le théorème de Grunewald-Schwermer. □

Terminons cette section en citant le résultat qui permet de conclure la démonstration du fait que $SL_2(\mathcal{O})$ n'a pas la CSP.

Théorème 3.8. *Soit K une extension quadratique de $\mathbb{Q}$, S un ensemble fini de places de K contenant toutes les places archimédiennes, $\mathcal{O}_S$ l'anneau des S-entiers de K et $n \geqslant 2$ un entier . Si un sous-groupe $\Gamma \geqslant SL_n(\mathcal{O}_S)$ a la CSP, alors il n'existe pas de sous-groupe d'indice fini de Γ ayant un groupe libre non abélien comme quotient.*

Références

[Su] B. Sury, *The congruence subgroup problem (an elementary approach aimed at applications)*, Texts and readings in mathematics 24, Hindustan Book Agency (distribué par l'AMS), (2003).

[W1] A.J. Weir, *Sylow p-subgroups of the general linear group over finite fields of characteristic p*, Proceedings of American Mathematical Society 6, 454-464 (1955).

[W2] A.J. Weir, *Sylow p-subgroups of the classical group over finite fields with characteristic prime to p*, Proceedings of American Mathematical Society 6, 529-533 (1955).

[GS] F.J. Grunewald and J. Schwermer, *Free non-abelian quotients of SL_2 over orders of imaginary quadratic numberfields*, Journal of algebra 69, 298-304 (1981).

[La] S. Lang, *Algebra-Second edition*, Addison Wesley Publishing company (1984)

[WF] K. Wohlfahrt, *An extension of F.Klein's level concept*, Illinois Journal of Mathematics, 529-535 (1964).

[Go] C. Godbillon, *Eléments de topologie algébrique*, Hermann Paris, (1971)

[RZ] L. Ribes and P. Zalesskii, *Profinite groups*, Springer, (2000)

[Sa] P. Samuel, *Théorie algébrique des nombres*, Hermann Paris, (1967)