Sur les présentations de $SL_n(\mathbb{Z})$ par générateurs et relations

Pierre Dehornoy et Jérôme Valentin
Sujet proposé par Frédéric Paulin

15 juin 2005

On s'intéresse dans cet exposé aux parties génératrices de $SL_n(\mathbb{Z})$. On introduit pour cela en première partie la notion de présentation d'un groupe. Dans la deuxième partie, on s'intéresse au cas particulier, plus simple mais très riche, où $n = 2$. Dans la troisième partie, on reprend le cas général, et on donne en particulier une présentation de $SL_n(\mathbb{Z})$. Enfin, dans la quatrième partie, on s'intéresse à des propriétés de génération bornée de $SL_n(\mathbb{Z})$ pour $n \geq 3$.

1 Groupes libres et présentations de groupes

On s'intéresse aux groupes libres, c'est à dire aux groupes F munis d'une partie X vérifiant la propriété universelle suivante : pour tout groupe G, pour toute application $f : X \to G$, il existe un unique homomorphisme $\overline{f} : F \to G$ qui prolonge f. On verra en particulier qu'un tel groupe est unique à isomorphisme près (c'est *le* groupe libre sur X) et engendré par X.

On donne ci-dessous une construction d'un groupe libre sur X à partir de l'ensemble des mots sur l'ensemble X.

Considérons un ensemble X appelé *alphabet*, il existe un ensemble X', en bijection avec X, tel que $X \cap X' = \emptyset$. Soit i une telle bijection. Pour $x \in X$ et $y \in X'$ on notera $i(x) = x^{-1}$ et $i^{-1}(y) = y^{-1}$.

Définition 1 (mots sur X)**.** On appelle *mot* sur X une famille finie $(x_1, ..., x_n)$ d'éléments de $X \cup X'$, que l'on notera $x = x_1x_2...x_n$. L'entier $n = l(x)$ est appelé la *longueur* du mot. On note 1 le mot associé à la famille vide, de longueur nulle

par convention. On identifiera x vu comme {elément de $X \cup X'$ avec le mot x. On notera $M(X, X')$ l'ensemble des mots ainsi définis.

On définit un produit noté ...sur $M(X, X')$ par concaténation des suites, qui vérifie en particulier : $m \cdot 1 = m = 1 \cdot m$.

Proposition 1. *Ce produit confère à $M(X, X')$ une structure de monoïde simplifiable à gauche et à droite dont l'élément neutre est 1. On a la relation $l(x \cdot y) = l(x)l(y)$. Enfin si on a un ensemble X'' vérifiant les mêmes propriétés que X' alors $M(X, X')$ et $M(X, X'')$ sont isomorphes en tant que monoïdes.*

On notera désormais $M(X, X') = M(X)$ et $X' = X^{-1}$.

Définition 2. Le monoïde $M(X)$ ainsi défini est appelé *monoïde libre* sur X.

On définit une relation R' sur $M(X)$ comme suit : $uR'v$ si et seulement s'il existe $a \in X \cup X^{-1}, t_1, t_2 \in M(X)$, tels que $(u, v) = (t_1t_2, t_1aa^{-1}t_2)$ ou $(t_1aa^{-1}t_2, t_1t_2)$. Cette relation est dite d'adjacence, et deux mots en relations sont adjacents.

R' engendre sur $M(X)$ une relation d'équivalence R : uRv si et seulement si $\exists t_1, ..., t_n$ tels que $uR't_1, \ldots, t_iR't_{i+1}, \ldots, t_nR'v$. Cette relation est compatible avec le produit $\cdot$ de $M(X)$.

Proposition 2. *Notons $s : M(X) \to M(X)/R$ la surjection canonique. La loi $\cdot$ passe au quotient, conférant à $M(X)/R$ une structure de groupe ; ce groupe est engendré par $s(X)$.*

Démonstration. Il est clair que R' est compatible avec le produit ; une récurrence sur n (en conservant les notations introduites dans la définition de R) permet alors de voir que R l'est aussi. □

Définition 3 (mots irréductibles)**.** Un mot $u = x_1...x_n \in M(X)$ est dit *irréductible* si pour $1 \leqslant i \leqslant n-1$ on a $x_{i+1} \neq x_i^{-1}$.

Proposition 3. *Chaque classe d'équivalence de $M(X)$ modulo R comporte un et un seul mot irréductible. L'unique mot irréductible équivalent à u sera noté $r(u)$.*

Démonstration. On remarque d'abord que chaque classe contient un mot irréductible : il suffit en effet de choisir un mot de longueur minimale parmi ceux de la classe. Soit maintenant $u = a_1...a_n \in M(X)$. On construit par récurrence une suite de mots irreductibles (u_i) en posant $u_0 = 1; u_1 = a_1; u_2 = a_1a_2$ si $a_1 \neq a_2^{-1}$ et 1 sinon ; puis si u_i est un mot irréductible équivalent à $a_1...a_i$ on construit u_{i+1} de la manière suivante : si $u_i = 1, u_{i+1} = a_{i+1}$; sinon u_i est de la forme $t_1...t_k$ et on pose $u_{i+1} = u_ia_{k+1}$

si $a_{k+1} \neq t_k^{-1}$, $t_1...t_{k-1}$ sinon. Alors u_n est un mot irréductible équivalent à u, que nous noterons $r(u)$. Enfin, par construction, si u et v sont équivalents alors $r(u) = r(v)$, et si u est irréductible alors $r(u) = u$. Donc si u et v sont équivalents et irréductibles, alors $u = r(u) = r(v) = v$, d'où l'unicité. □

Définition 4 (groupe libre)**.** Notons $F(X)$ l'ensemble des mots irréductibles de $M(X)$. Par la proposition précédente, $F(X)$ est en bijection via la restriction de s avec $M(X)/R$. La bijection réciproque transporte la structure de groupe de $M(X)/R$ sur $F(X)$: $F(X)$ est donc un groupe engendré par X. On l'appelle le *groupe libre* engendré par X. Par convention on pose $F(\emptyset) = 1$.

Théorème 4 (propriété universelle du groupe libre)**.** *Soient X un ensemble, G un groupe et $f : X \to G$ une application. Alors il existe un unique homomorphisme de groupes de $F(X)$ dans G qui prolonge f.*

C'est bien la propriété annoncée au début.

Démonstration. Soit $f : X \to G$ une application. f se prolonge à X^{-1} par $f(x^{-1}) = f(x)^{-1}$, puis à $M(X)$ par $f(1) = 1$ et $f(x_1...x_n) = f(x_1)...f(x_n)$. Par récurrence sur la longueur on voit alors que $\forall u, v \in M(x), f(uv) = f(u)f(v)$, et que f est constante sur les classes. Le théorème de factorisation des applications fournit alors $\overline{f} : M(X)/R \to G$ telle que $\overline{f} \circ s = f$. Alors, notant $\overline{s}$ la restriction de s à $F(X)$ et r comme ci-dessus, si $\varphi = \overline{f} \circ \overline{s}$, alors $\varphi \circ r = f$. Donc φ est un homomorphisme de groupes convenable, et l'unicité provient de ce que X engendre $F(X)$. □

En particulier, si X est une partie génératrice d'un groupe G, on a une inclusion $X \hookrightarrow G$, d'où un homomorphisme canonique de $F(X)$ dans G.

Par exemple on peut montrer en utilisant la propriété universelle que le groupe libre engendré par un singleton est isomorphe à $\mathbb{Z}$. On peut aussi montrer que $F(X)$ est non-commutatif dès que $card(X) \geq 2$, qu'un groupe libre est sans torsion, que $F(X)$ et $F(Y)$ sont isomorphes si et seulement si X et Y sont en bijection, et que tout sous-groupe d'un groupe libre est encore un groupe libre (théorème de Schreier).

Définition 5 (Présentation d'un groupe)**.** Soient G un groupe, X une partie génératrice de G, R une partie de $F(X)$, $H(R)$ le sous-groupe distingué de $F(X)$ engendré par R. On dit que le couple $\langle X \mid R \rangle$ est une *présentation* de G si l'homomorphisme canonique $F(X) \hookrightarrow G$ a pour noyau $H(R)$. On appelle alors X l'ensemble des *générateurs* de la présentation, et R l'ensemble des *relations* de la présentation. Dans le cas où X et R sont des ensembles finis on parle de présentation finie.

Remarquons que dans la configuration ci-dessus, on a : $G \simeq F(X)/H(R)$.

Par exemple une présentation du groupe libre engendré par X est $\langle\ X \mid \emptyset\ \rangle$ et une présentation du groupe cyclique d'ordre n est $\langle\ \{a\} \mid a^n\ \rangle$.

La propriété suivante des présentations sera importante dans la troisième partie.

Proposition 5 (Suite exacte de groupes et présentations)**.** *Supposons qu'on a la suite exacte de groupes :* $1 \to F \to G \to H \to 1$*, avec des morphismes* $\varphi : F \to G$ *et* $\psi : G \to H$*, et que* F *et* H *ont pour présentations :*

$$F = \langle\ f_1, \dots, f_m \mid R_1, \dots, R_n\ \rangle \text{ et}$$
$$H = \langle\ h_1, \dots, h_p \mid S_1, \dots, S_q\ \rangle,$$

avec $S_i = h_{i1} \dots h_{ij_i}$ *pour* $i = 1, \dots, q$*. Soit* $g_1, \dots, g_p \in G$ *tels que pour* $k = 1, \dots, q$ *on a* $g_k \in \varphi^{-1}(h_k)$*. Alors, pour* $i = 1, \dots, q$*, il existe* $r_i \in \mathbb{N}$ *et* $s_i : [[1, r_i]] \to [[1, n]]$ *tels que* $g_{i1} \dots g_{ij_i} = \varphi(f_{s_i(1)}) \dots \varphi(f_{s_i(r_i)})$*, et alors, pour tout tel choix des* r_i *et des* s_i*, le groupe* G *admet pour présentation*

$$\langle\ \varphi(f_1), \dots, \varphi(f_n), g_1, \dots, g_p \mid \varphi(R_1), \dots, \varphi(R_m),$$
$$g_{11} \dots g_{1j_1} \varphi(f^{-1}_{s_1(r_1)}) \dots \varphi(f_{s_1(1)})^{-1}, \dots, g_{q1} \dots g_{qj_q} \varphi(f^{-1}_{s_q(r_q)}) \dots \varphi(f_{s_q(1)})^{-1}\ \rangle.$$

Démonstration. Montrons d'abord la partie génération. Soit $g \in G$. Comme $\psi(g) \in H$, il existe $r_g \in \mathbb{N}$ et $s_g : [[1, r_g]] \to [[1, p]]$ tels que $\psi(g) = h_{s_g(1)} \dots h_{s_g(r_g)}$. On a alors $g g^{-1}_{s_g(r_g)} \dots g^{-1}_{s_g(1)} \in ker(\psi) = im(\varphi)$, or $\varphi(f_1), \dots, \varphi(f_m)$ engendrent $im(\varphi)$ donc il existe $r'_g \in \mathbb{N}$ et $s'_g : [[1, r'_g]] \to [[1, m]]$ tels que $g g^{-1}_{s_g(r_g)} \dots g^{-1}_{s_g(1)} = \varphi(f_{s'_1(r'_1)}) \dots \varphi(f_{s'_g(r'_g)})$, on a alors $g = \varphi(f_{s'_1(r'_1)}) \dots \varphi(f_{s'_g(r'_g)}) g_{s_g(1)} \dots g_{s_g(r_g)}$, donc G est engendré par $\varphi(f_1), \dots, \varphi(f_n), g_1, \dots, g_p$.

Comme φ est un morphisme, pour $i = 1 \dots n$, $\varphi(R_i) = 1$ est bien une relation dans G. Pour $i = 1 \dots q$, on a $h_{i1} \dots h_{ij_i} = 1$, donc $g_{i1} \dots g_{ij_i} \in ker(\psi) = im(\varphi)$ et par conséquent il existe $r_i \in \mathbb{N}$ et $s_i : [[1, r_i]] \to [[1, n]]$ tels que $g_{i1} \dots g_{ij_i} = \varphi(f_{s_i(1)}) \dots \varphi(f_{s_i(r_i)})$. Par conséquent $g_{q1} \dots g_{qj_q} \varphi(f^{-1}_{s_q(r_q)}) \dots \varphi(f_{s_q(1)})^{-1} = 1$ est bien une relation dans G.

Soit $g_1 \dots g_l = 1$ une relation dans G. D'aprés la partie génération pour $k \leq l$ on peut supposer que g_k fait partie des générateurs déjà exhibés de G. Comme $im(\varphi) = ker(\psi)$ est distingué dans G, quitte à les changer on peut pousser tous les $\varphi(f_i)$ à gauche dans notre relation qui se réécrit alors

$$\varphi(f_{t_1}) \dots \varphi(f_{t'_k}) g_{t'_1} \dots g_{t'_{k'}} = 1.$$

Via ψ on en déduit la relation $h_{t'_1} \dots h_{t'_{k'}} = 1$, donc les relations données permettent d'exhiber k'' et t'' tels que

$$g_{t'_1} \dots g_{t'_{k'}} = \varphi(f_{t''_1}) \dots \varphi(f_{t''_{k''}}).$$

Notre relation devient alors

$$\varphi(f_{t_1}) \dots \varphi(f_{t'_k}) \varphi(f_{t''_1}) \dots \varphi(f_{t''_{k''}}) = 1.$$

Cette relation se déduit donc d'une relation sur F, et donc les relations $\varphi(R_1)$, ..., $\varphi(R_n)$ permettent de la trivialiser. Par conséquent une relation sur G se déduit bien des relation données, et donc G admet pour présentation celle donnée dans l'énoncé. □

Définition 6 (produit libre de deux groupes)**.** Soient G_1 et G_2 deux groupes. On note $X = G_1 \coprod G_2$ (union disjointe ensembliste). On peut définir comme précedemment la relation R ; alors $M(X)/R$ est un groupe, qui permet de définir (comme ci-dessus) sur l'ensemble des mots réduits de $M(X)$ la seule structure de groupe telle que la restriction de la surjection canonique soit un isomorphisme. On appelle *produit libre* de G_1 et G_2, et on note $G_1 * G_2$ l'ensemble des mots réduits de $M(X)$ muni de cette strucure de groupe.

Proposition 6 (propriété universelle du produit libre)**.** *$G_1 * G_2$ est l'unique groupe à isomorphisme près qui soit solution du problème universel suivant : pour tout groupe H et pour tout couple d'homomorphismes $f_i : G_i \to H$ il existe un unique homomorphisme $f : G_1 * G_2 \to H$ tel que, si $g_i : G_i \hookrightarrow G_1 * G_2$ est l'inclusion canonique, $f \circ g_i = h_i$*

La preuve étant analogue à celle de la propriété universelle du groupe libre, et cette proposition n'étant pas utilisée dans la suite, on se contente de renvoyer à [Fre].

On peut bien-sûr généraliser la notion de produit libre à une famille quelconque de groupes. On peut alors voir le groupe libre sur X comme produit libre d'une famille de groupes tous isomorphes à $\mathbb{Z}$ indexée par X.

Proposition 7 (produit libre de groupes et présentations)**.** *Soient G et H deux groupes, dont des présentations respectives sont*

$$\langle\ g_1, \dots, g_n \mid R_1, \dots, R_m\ \rangle \text{ et}$$
$$\langle\ h_1, \dots, h_p \mid S_1, \dots, S_q\ \rangle.$$

Alors le produit libre $G * H$ de G et H admet pour présentation :

$$\langle\ g_1, \dots, g_n, dots, h_1, \dots, h_p \mid R_1, \dots, R_m, S_1, \dots, S_q\ \rangle.$$

Dans la partie suivante, on verra que $PSL_2(\mathbb{Z})$ est isomorphe au produit libre de $\mathbb{Z}/2\mathbb{Z}$ et de $\mathbb{Z}/3\mathbb{Z}$.

2 $SL_2(\mathbb{Z})$ par générateurs et relations

Le groupe $SL_2(\mathbb{Z})$ joue un rôle particulier, puisqu'il a une structure proche de celle du groupe libre, ce qui n'est pas le cas pour $n \geq 3$. Dans cette partie nous allons donner une présentation par générateurs et relations de $SL_2(\mathbb{Z})$. Pour cela nous observerons son action sur le demi-plan de Poincaré, ce qui nous permettra de démontrer le théorème suivant.

Théorème 8 (présentation de $SL_2(\mathbb{Z})$)**.** *Le groupe $SL_2(\mathbb{Z})$ admet pour présentation par générateurs et relations $\langle\, s,t \mid s^2=(st)^3, s^4=1 \,\rangle$, $\langle\, a,b \mid aba=bab, (aba)^4=1 \,\rangle$ et $\langle\, a,b \mid a^2=b^3, a^4=1 \,\rangle$.*

La démonstration nécessite des notions de géométrie hyperbolique. Nous renvoyons à [Kat] pour un exposé plus complet de ces notions.

Définition 7 (demi-plan de Poincaré)**.** On appelle *demi-plan de Poincaré* le demi-plan supérieur H de $\mathbb{C}$, c'est-à-dire l'ensemble $\{z \in \mathbb{C} \mid Im(z) > 0\}$.

On fait opérer $SL_2(\mathbb{Z})$ sur $\bar{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ par l'action suivante: si $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, on pose $gz = \frac{az+b}{cz+d}$, avec les conventions naturelles suivantes : $\frac{a*\infty+b}{c*\infty+d} = \frac{a}{c}$, $\frac{b}{c*\infty+d} = 0$ et $\frac{az+b}{0} = \infty$. On remarque que l'élément $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ est le seul élément non trivial qui opère trivialement sur $\bar{\mathbb{C}}$, on peut donc considérer que c'est $PSL_2(\mathbb{Z}) = SL_2(\mathbb{Z})/\{\pm 1\}$ qui opère, et alors l'action est fidèle.

Définition 8 (groupe modulaire)**.** On appelle *groupe modulaire* le groupe $PSL_2(\mathbb{Z})$, quotient de $SL_2(\mathbb{Z})$ par $\{\pm Id\}$, noté G par la suite.

Notons que

$$\begin{aligned} Im(gz) &= Im\Big(\frac{az+b}{cz+d}\Big) \\ &= \frac{Im\big((az+b)\overline{(cz+d)}\big)}{|cz+d|^2} \\ &= \frac{(az+b)(c\bar{z}+d)-(a\bar{z}+b)(cz+d)}{2|cz+d|^2} \\ &= \frac{(ad-bc)(z-\bar{z})/2}{|cz+d|^2} \\ &= \frac{Im(z)}{|cz+d|^2}, \end{aligned}$$

donc H est préservé par l'action du groupe modulaire. Désormais, nous ne nous intéresserons plus qu'à l'action de G sur H. Le même calcul montre que H est aussi préservé par l'action de $PSL_2(\mathbb{R})$.

Le lemme suivant va être utile dans la suite.

Lemme 9. *Soit L une demi-droite euclidienne dans $H \cup \mathbb{R}$ orthogonale à l'axe réel, et rencontrant cet axe en a. Alors l'action de la matrice $\begin{pmatrix} 1 & -a \\ 0 & 1 \end{pmatrix}$ envoie L sur l'axe des imaginaires purs de partie imaginaire positive ou nulle.*

Soit C un demi-cercle euclidien dans $H \cup \mathbb{R}$ orthogonal à l'axe réel, et rencontrant cet axe en a et b. Alors l'action de la matrice $\frac{1}{a-b}\begin{pmatrix} 1 & -a \\ 1 & -b \end{pmatrix}$ envoie C sur l'axe des imaginaires purs de partie imaginaire positive ou nulle.

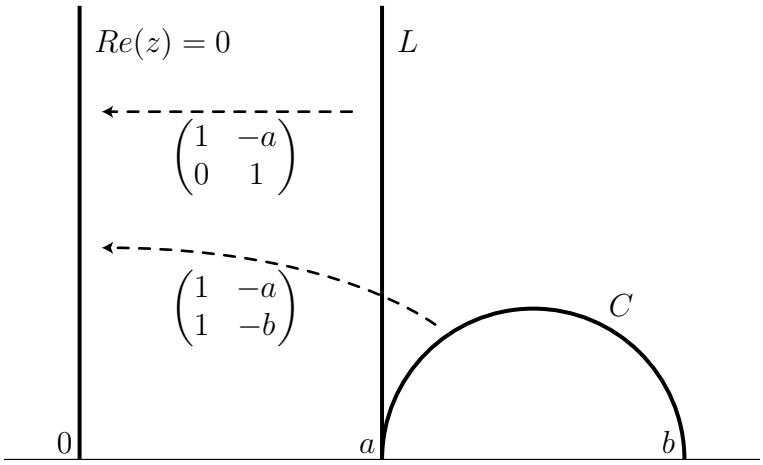

Figure 1: L et CC sont envoyés sur l'axe imaginaire pur

Démonstration. Le cas de la droite L est trivial.

Soit $z \in C$, on a alors $|z - \frac{b+a}{2}| = \frac{|b-a|}{2}$, d'où

$$\begin{aligned} Re\Big(\frac{z-a}{z-b}\Big) &= Re\Big(\frac{(z-a)(z-b)}{|z-b|^2}\Big) \\ &= Re\Big(\frac{(z-\frac{a+b}{2}-\frac{a-b}{2})(\bar{z}-\frac{a+b}{2}+\frac{a-b}{2})}{|z-b|^2}\Big) \\ &= \Big(\frac{\big|z-\frac{a+b}{2}\big|^2 + \frac{a-b}{2}Re\big((z-\frac{a+b}{2})-(\bar{z}-\frac{a+b}{2})\big) - (\frac{a-b}{2})^2}{|z-b|^2}\Big) \\ &= 0. \end{aligned}$$

Donc C est envoyé sur l'axe imaginaire pur. D'autre part on vérifie facilement que a est envoyé en 0, et b en ∞. Donc l'image de C est exactement l'axe imaginaire pur de partie imaginaire strictement positive pour des raisons de connexité. □

Le demi-plan H est intéressant car on peut le munir d'une métrique hyperbolique naturelle.

Définition 9 (distance hyperbolique sur H)**.** On équipe H de la métrique $ds = \frac{|dz|}{Im(z)}$, où $|dz|$ est l'élément de distance euclidien $\sqrt{dx^2+dy^2}$. On appelle l la longueur des courbes asocié et d la distance associée.

Proposition 10. *Les actions des éléments de $PSL_2(\mathbb{R})$ sur H sont des isométries pour la distance d.*

Démonstration. On a déjà vu que H est stable pour l'action de $PSL_2(\mathbb{R})$. Montrons que si $\gamma : I \to H$ est un chemin différentiel, alors pour tout g dans G, on a $l(g(\gamma)) = l(\gamma)$. Supposons que γ soit donné par $z(t) = x(t) + iy(t)$ et que $g(\gamma)$ soit donné par $w(t) = u(t) + iv(t)$. On a alors

$$\frac{dw}{dz} = \frac{a(cz+d) - c(az+b)}{(cz+d)^2} = \frac{1}{(cz+d)^2}.$$

Or on a $v = \frac{y}{|cz+d|^2}$, et donc $|\frac{dw}{dz}| = \frac{v}{y}$. D'où

$$l(g(\gamma)) = \int_0^1 \frac{|\frac{dw}{dt}|}{v(t)}dt = \int_0^1 \frac{|\frac{dw}{dz}\frac{dz}{dt}|}{v(t)}dt = \int_0^1 \frac{|\frac{dz}{dt}|}{y(t)}dt = l(\gamma).$$

L'invariance de la distance hyperbolique découle de la dernière égalité. Par conséquent les éléments de $PSL_2(\mathbb{R})$ sont des isométries de H. □

Remarque 1. On peut montrer que l'ensemble des isométries directes (*i.e* préservant l'orientation) de H est exactement l'ensemble des actions sur H du groupe $PSL_2(\mathbb{R})$.

Proposition 11. *Les géodésiques de H pour la distance d sont les demi-droites euclidiennes perpendiculaires à l'axe des réels, définies par $Re(z) = cste$, et les demi-cercles euclidiens orthogonaux à ce même axe, définis par $|z - x| = cste$, appelés désormais droites hyperboliques.*

Démonstration. Soient z_1, z_2 deux points de H. Supposons tout d'abord $z_1 = ia$ et $z_2 = ib$, avec $b > a$. Si γ est un chemin différentiable joignant z_1 à z_2 avec $\gamma(t) = x(t) + iy(t)$, alors

$$l(\gamma) = \int_0^1 \frac{\sqrt{(\frac{dx}{dt})^2 + (\frac{dy}{dt})^2}}{y(t)} dt \geq \int_0^1 \frac{|\frac{dy}{dt}|}{y(t)} dt \geq \int_0^1 \frac{\frac{dy}{dt}}{y(t)} dt = \int_a^b \frac{dy}{y} = \ln(\frac{b}{a}).$$

Or $\ln(\frac{b}{a})$ est la longueur hyperbolique du segment de l'axe imaginaire joignant ia et ib, donc la géodésique joignant z_1 et z_2 est le segment de l'axe imaginaire qui est entre les deux.

Supposons maintenant z_1, z_2 quelconques. Ils appartiennent alors à un unique cercle euclidien C (resp. droite L si $Re(z_1) = Re(z_2)$) orthogonal à l'axe réel. D'après le lemme 9, il existe une transformation t de $PSL_2(\mathbb{R})$ qui envoie C (resp. L) sur l'axe imaginaire pur. Or $t(C)$ est la géodésique joignant tz_1 à tz_2, donc C est la géodésique joignant z_1 à z_2 puisque t est une isométrie. □

Pour étudier l'action de G sur H, nous allons regarder les images par cette action d'un élément fixé. Pour lier les images de différents points, la notion de domaine fondamental est utile.

Définition 10 (domaine fondamental)**.** On appelle *domaine fondamental* pour l'action de G sur H une partie F de H vérifiant

(*i*) $F = Adh(Int(F))$,

(*ii*) $H = \bigcup_{g \in G} gF$,

(*iii*) $\forall g \in G \setminus \{1\}, Int(F) \cap Int(gF) = \emptyset$.

Proposition 12. *Soit $z_0 \in H$ tel que $Stab(z_0) = \{1\}$. Alors l'ensemble $D_{z_0}(G) = \{z \in H | \forall g \in G, d(z, gz_0) \geq d(z, z_0)\}$ est un domaine fondamental, appelé domaine fondamental de Dirichlet en z_0.*

Démonstration. Soit $z \in H$, comme l'orbite Gz de z dans H est discrète, il existe $z' \in Gz$ minimisant $d(z, z_0)$, d'où $d(z', z_0) \leq d(gz, z_0)$ pour tout g dans G, et donc z' appartient à $D_{z_0}(G)$. Par conséquent $D_{z_0}(G)$ contient au moins un point dans chaque orbite, d'où le point (ii).

Soit $g \in G$, notons $H_g(z_0)$ le demi-plan (hyperbolique) délimité par la médiatrice du segment $[z_0, gz_0]$. On a $D_{z_0}(G) = \bigcap_{g \in G} H_g(z_0)$, et tous ces demi-plans étant fermés, convexes (au sens hyperbolique) et d'intérieur non vide, $D_{z_0}(G)$ est fermé, convexe et d'intérieur non vide, d'où le point (i).

Montrons que deux points distincts z_1, z_2 de l'intérieur de $D_{z_0}(G)$ ne peuvent appartenir à la même orbite. Soit $z \in D_{z_0}(G)$. Si $d(z, z_0) = d(gz, z_0)$, alors $d(z, z_0) = d(z, g^{-1}z_0)$, donc z est sur la médiatrice du segment (non trivial par hypothèse !) $[z_0, g^{-1}z_0]$, donc z appartient à la frontière de $D_{z_0}(G)$. Donc si $z \in Int(D_{z_0}(G))$, alors $d(z, z_0) < d(gz, z_0)$ pour tout $g \in G \setminus \{1\}$. Si les deux points z_1, z_2 appartiennent à la même orbite, cela implique $h(z_1, z_0) < h(z_2, z_0)$ et $d(z_2, z_0) > d(z_1, z_0)$, d'où une contradiction. Ceci démontre (iii). □

Deux éléments de $SL_2(\mathbb{Z})$ vont jouer un rôle particulier dans la suite. On pose $s = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $t = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

Proposition 13. *Le domaine fondamental de Dirichlet $D_{ri}(G)$, pour $r \in \mathbb{R}$ et $r > 1$, est l'ensemble $D = \{z \in H \big| |\Re(z)| \leq 1/2 \text{ et } |z| \geq 1\}$.*

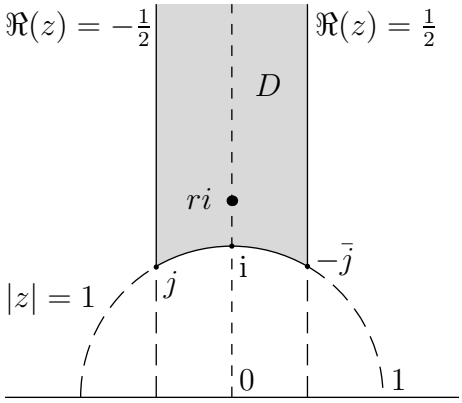

Figure 2: Le domaine fondamental de Dirichlet $D_{ri}(G)$

Démonstration. Notons d'abord que $D_{ri}(G)$ est bien défini puisque ri n'est fixé par aucun élément de $G\backslash\{1\}$. Tout d'abord les trois isométries $t(z) = z+1, t^{-1}(z) = z-1$ et $s(t) = -1/z$ sont bien dans G, et $D = H_t(z_0) \cap H_t^{-1}(z_0) \cap H_s(z_0)$. Ceci montre $D_{ri}(G) \subset D$.

Supposons $D_{z_0}(ri) \subsetneq D$, alors il existe $z \in Int(D)$ et $g \in G$ tels que $gz \in Int(D)$. Posons $gz = \frac{az+b}{cz+d}$, avec $ad - bc = 1$. On a alors

$$|cz + d|^2 = c^2|z|^2 + 2Re(z)cd + d^2 > c^2 + d^2 - |cd| = (|c| - |d|)^2 + |cd|,$$

car $|z| > 1$ et $Re(z) > -\frac{1}{2}$. Cette borne est entière et strictement positive (car sinon $c = d = 0$ qui contredit $ad-bc = 1$). Donc elle vaut au moins 1 et donc $|cz+d| > 1$. On a alors $Im(gz) = \frac{Im(z)}{|cz+d|^2} < Im(z)$ d'où $Im(gz) > Im(z)$. Le même argument marche alors en remplaçant z par gz et g par g^{-1}, d'où $Im(z) > Im(gz)$ et on a une contradiction, d'où la proposition. □

Corollaire 14. *Les seuls domaines qui partagent un segment de frontière de longueur non nulle avec D sont $sD, tD, t^{-1}D$.*

Démonstration. Soit $g \in G$ tel que D et gD aient un segment de longueur non nulle en commun. Alors ce segment est une partie de la médiratrice de $[ri, gri]$, or les seuls bords de D sont des segments des médiatrices de $[ri, sgri]$, $[ri, tri]$ et $[ri, t^{-1}ri]$, donc la médiatrice de $[ri, gri]$ est confondue avec l'une des trois précédentes, donc $gri = sri, tri$ ou $t^{-1}ri$, donc $g = s, t$ ou t^{-1}. □

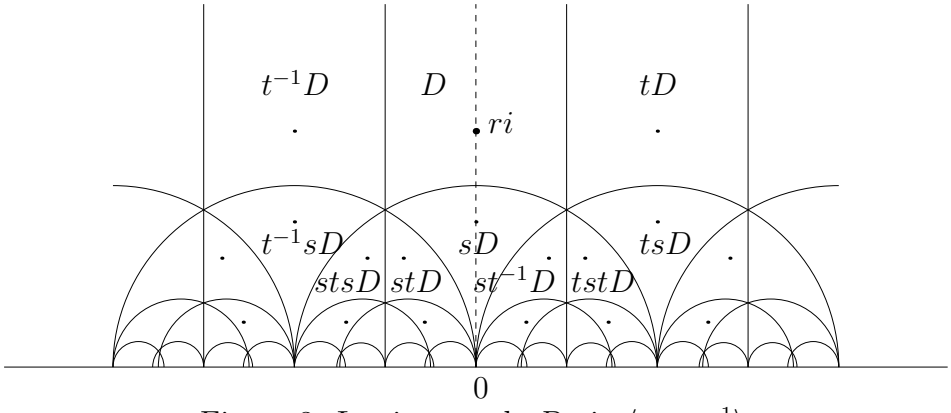

Figure 3: Les images de D via $\langle s, t, t^{-1}\rangle$

Théorème 15. *Le groupe G est engendré par s et t.*

Démonstration. Soit $g \in G$. Choisissons $z_0 \in D$ de telle sorte que le segment géodésique S reliant z_0 à gz_0 ne passe par aucun point ayant un stabilisateur non trivial. Ceci est toujours possible car l'ensemble de ces points est discret. Le segment S traverse donc une suite de domaines fondamentaux. Or cette suite est finie car dans la région $\{z \in H \mid Im(z) \geq Im(gz_0), Re(z_0) \leq Re(z) \leq Re(gz_0)\}$ il ne rencontre qu'un nombre fini de domaines fondamentaux de Dirichlet, car l'action est proprement discontinue. On peut donc supposer que la suite s'écrit $D, g_1D, g_1g_2D, \ldots, g_1g_2 \ldots g_nD = gD$. Pour tout i le segment $[g_1 \ldots g_{i-1}z_0, g_1 \ldots g_iz_0]$ ne rencontre que deux domaines fondamentaux, donc le segment $[z_0, g_iz_0]$ également, or $z_0 \in D$, donc d'après le corollaire précédent on a $g_iz_0 \in sD, tD$ ou $t^{-1}D$, d'où $z_i = s, t$ ou t^{-1}. Par conséquent g est le produit de n termes dans $\{s, t, t^{-1}\}$. □

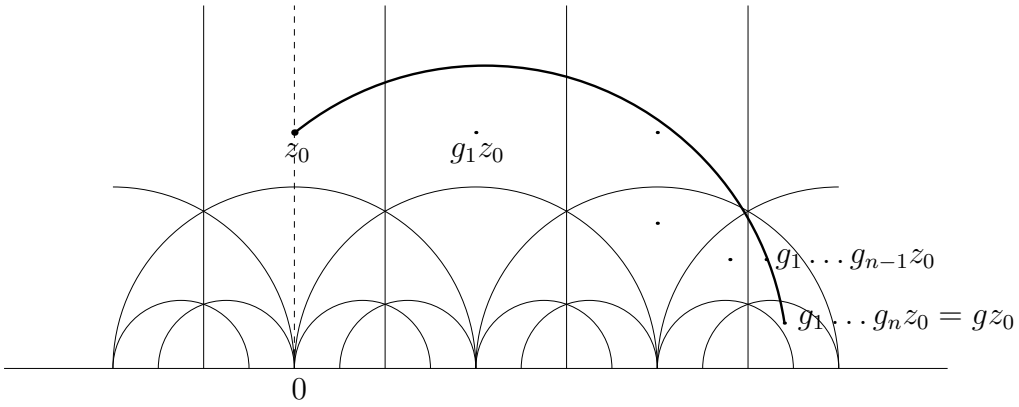

Figure 4: L'arc reliant z_0 à gz_0

Théorème 16. *Le groupe G admet pour présentation : $\langle\ s, t \mid s^2 = (st)^3 = 1\ \rangle$*

Démonstration. La partie génération vient d'être démontrée, il suffit donc de montrer que toute relation sur G se déduit de $s^2 = (st)^3 = 1$. Supposons donc $g_1g_2 \ldots g_n = 1$, avec $n \geq 2$. Comme s et t engendrent G et comme $s^2 = 1$ on peut supposer $g_i = s, t$ ou t^{-1} pour tout i. Choisissons $z_0 \in Int(D)$ et posons $z_i = g_1 \ldots g_iz_0$ (on a donc $z_n = z_0$). Quitte à scinder notre relation en deux, on peut supposer que pour tous i, j avec $1 \leq i, j \leq n$, on a $g_ig_{i+1} \ldots g_j \neq 1$, soit $z_i \neq z_j$. En particulier, le mot $g_1g_2 \ldots g_n$ est réduit sur le groupe libre sur s, t. Notons que la

suite $g_1, \ldots, g_n$ contient au moins un s, sinon on aurait $z_n = t^{\pm n} \neq z_0$, et au moins un t ou t^{-1}, sauf si $n = 2$ et $g_1 = g_2 = s$. Par conséquent, quitte à passer à la suite inverse, notre suite contient au moins un terme de la forme st ou ts. Traitons le premier cas, le second se faisant de même.

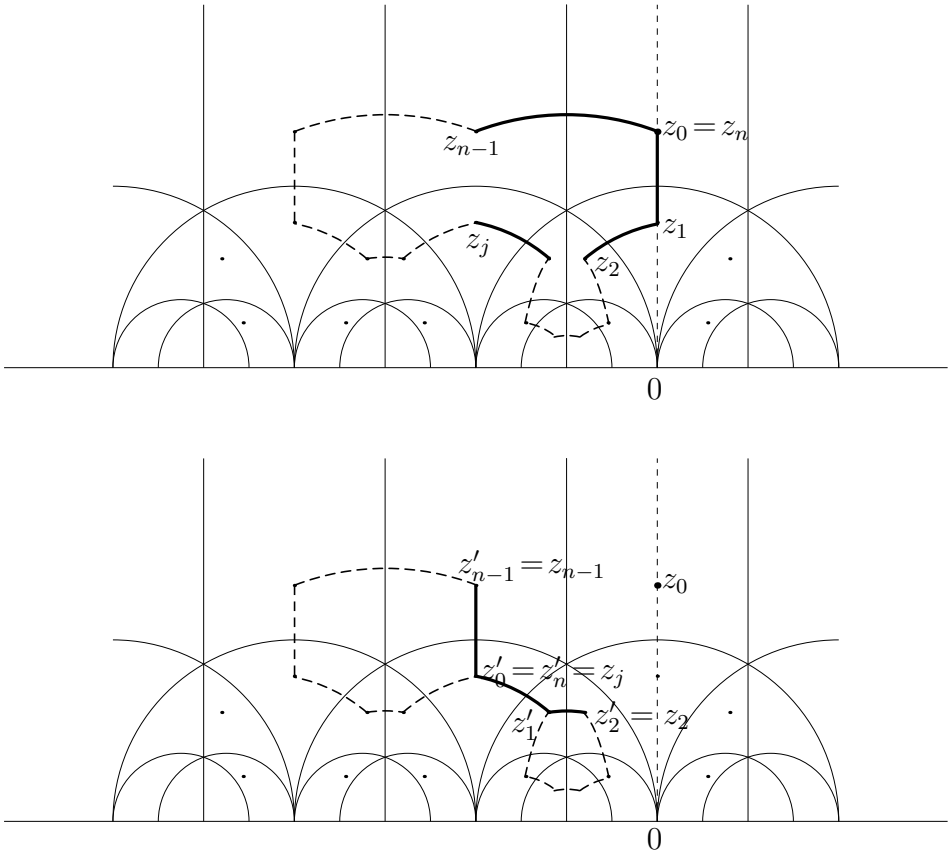

Figure 5: Simplification de la relation $g_1 \ldots g_n = 1$

Quitte à permuter cycliquement les termes de la suite on peut supposer $g_1 = s, g_2 = t$. Comme l'axe imaginaire pur est entièrement compris dans $D \cup sD$, et que le domaine stD est à gauche de cet axe, tous les $z_2, \ldots, z_n$ sont à gauche de cet axe, or $g_n = t$ ou t^{-1}, d'où $g_n = t$. Comme $t^{-1}D \cup t^{-1}sD$ contient l'axe $\Re(z) = -1$ et comme $z_{n-1} \in t^{-1}D$, il existe j avec $3 \leq j \leq n-2$ tel que $z_j \in t^{-1}sD$. Or la relation $(st)^3 = 1$ implique $tst = st^{-1}s$ donc la relation $g_1 g_2 \ldots g_n = 1$ est

équivalente à la relation $t^{-1}sg_3 \dots g_{n-1}s = 1$. Or la suite $z'_0, z'_1, \dots, z'_n$ associée à cette relation, où l'on choisit $z'_0 = z_j$, coïncide avec $z_0, \dots, z_n$ pour tous les éléments compris entre z_2 et z_{n-1}, en particulier on a $z'_0 = z'_j$, et on peut donc scinder notre nouvelle relation $g'_1 \dots g'_n = 1$ en deux relations $g'_2 \dots g'_{j-1} = 1$ et $g'_{j+1} \dots g'_n = 1$ de longueurs strictement plus courtes, et la relation initiale se déduit de ces deux-là. Par récurrence peut donc se ramener aux cas $n = 0, 2$ qui sont triviaux. □

Corollaire 17. *Le groupe $PSL_2(\mathbb{Z})$ est isomorphe au produit libre $\mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/3\mathbb{Z}$.*

On peut maintenant démontrer le théorème 8.

Démonstration. On a la suite exacte suivante

$$0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow SL_2(\mathbb{Z}) \longrightarrow PSL_2(\mathbb{Z}) \longrightarrow 0.$$

Donc d'après le lemme 5, pour déduire une présentation de $SL_2(\mathbb{Z})$ de celle de G qu'on a déjà, il suffit de déterminer les éléments de l'image de $\mathbb{Z}/2\mathbb{Z} \longrightarrow SL_2(\mathbb{Z})$ auxquels sont égaux s^2 et $(st)^3$. Or un calcul facile montre que $s^2 = (st)^3 = -I_2 = \varphi(-1)$, d'où la première présentation. Pour déduire la seconde, il suffit de poser $a = t^{-1}, b = tst$, et pour la troisième de poser $a = s, b = st$. □

La structure de $SL_2(\mathbb{Z})$ est donc proche de celle du produit libre $\mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/3\mathbb{Z}$, et donc elle est proche de celle d'un groupe libre.

3 $SL_n(\mathbb{Z})$ pour $n \geq 3$ par générateurs et relations

Nous allons à présent nous intéresser à $SL_n(\mathbb{Z})$ pour $n \geq 3$.

Définition 11 (matrice élémentaire)**.** Pour $i \leq i \neq j \leq n$, on note e_{ij} la matrice:

$$\begin{pmatrix} 1 & & & \\ & \ddots & 1 & \\ & & \ddots & \\ & & & 1 \end{pmatrix}, \text{ où le 1 se trouve en position } (i, j).$$

Les puissances des e_{ij} pour $i \neq j$ sont appelées *matrices élémentaires*.

Dans un premier temps, nous allons montrer que les matrices élémentaires engendrent $SL_n(\mathbb{Z})$, puis nous dégagerons des relations entre celles-ci et montrerons qu'elles engendrent presque toutes les relations entre matrices élémentaires.

Théorème 18. *Les matrices élémentaires engendrent $SL_n(\mathbb{Z})$ pour $n \geq 3$.*

Démonstration. Soit M une matrice de $SL_n(\mathbb{Z})$ de la forme

$$\begin{pmatrix} * & * & \dots & * \\ * & * & \dots & * \\ \vdots & \vdots & & \vdots \\ * & * & \dots & * \\ u_1 & u_2 & \dots & u_n \end{pmatrix}.$$

La multiplication à gauche par une matrice élémentaire e_{ij}^l consiste à ajouter l fois la j-ième ligne à la i-ième, et la multiplication à droite par e_{ij}^l consiste à ajouter l fois la i-ième colonne à la j-ième. Le jeu consiste donc à faire des opérations sur les lignes et les colonnes pour se ramener de M à la matrice I_n. Ces deux types d'opérations seront désormais appelées opérations élémentaires.

Comme M est inversible, on a $u_1\mathbb{Z} + u_2\mathbb{Z} + \ldots + u_n\mathbb{Z} = \mathbb{Z}$, ie les u_i sont premiers entre eux. On distingue alors deux cas. Soit il existe $i < n$ tel que $u_i = 0$ et alors en une opération élémentaire on peut amener u_n à la place de u_i, et de là $u_1\mathbb{Z} + u_2\mathbb{Z} + \ldots + u_{n-1}\mathbb{Z} = \mathbb{Z}$. Soit, puisque $n \geq 3$, il existe $t \in \mathbb{Z}$ tel que

$$t \equiv 1 \text{ mod tous les premiers divisant } u_1, \ldots, u_{n-1},$$
$$t \equiv 0 \text{ mod tous les premiers divisant } u_2, \ldots, u_{n-1} \text{ mais pas } u_1.$$

Pour l'existence de t, on peut utiliser le lemme suivant : Soient P_1 et P_2 deux ensembles finis et disjoints de nombres premiers. Alors il existe t tel que t soit congru à 1 modulo tout élément de P_1 et à 0 modulo tout élément de P_2. En effet, si on note π_i le produit des éléments de P_i pour $i \in 1, 2$ il suffit de choisir t dans $(\pi_2\mathbb{Z}) \cap (1 + \pi_2\mathbb{Z})$, dont on voit qu'il est non-vide grâce au thórême de Bezout, puisque $pgcd(\pi_1, \pi_2) = 1$. En une opération élémentaire on peut transformer u_1 en $u_1 + tu_n$. On a alors $(u_1 + tu_n)\mathbb{Z} + u_2\mathbb{Z} + \ldots + u_{n-1}\mathbb{Z} = \mathbb{Z}$. En effet, soit p un diviseur premier commun à $u_1 + tu_n, u_2, ..., u_{n-1}$. D'une part p divise u_1, car sinon par définition de t, p ne diviserait pas $u_1 + tu_n$. Donc, toujours par définition de t, p ne divise pas t. Or, il divise $u_1 + tu_n$ et u_1, donc aussi tu_n, donc u_n. Ainsi p divise tous les u_i, qui sont premiers entre eux ; contradiction. Ainsi, $pgcd(u_1 + tu_n, u_2, ..., u_{n-1}) = 1$, ce qui conclut. Il suffit alors d'utiliser $n-1$ opérations élémentaires pour amener un 1 en position (n, n). De là $2(n-1)$ opérations permettent de supprimer les coefficients non nuls sur la dernière ligne et la dernière colonne, et donc de transformer notre matrice en

$$\begin{pmatrix} * & \dots & * & 0 \\ \vdots & & \vdots & \vdots \\ * & \dots & * & 0 \\ 0 & \dots & 0 & 1 \end{pmatrix}.$$

Une récurrence facile permet alors de se ramener au cas des matrices de $SL_2(\mathbb{Z})$ qui a été déjà traité. □

Pour décrire $SL_n(\mathbb{Z})$ par générateurs et relations, on cherche alors à trouver toutes les relations naturelles existant entre les e_{ij}. On vérifie facilement que

$$\begin{aligned} [e_{ij}, e_{kl}] &= 1 && \text{si } j \neq k, i \neq l \\ [e_{ij}, e_{jk}] &= e_{ik} && \text{si } i \neq k. \end{aligned}$$

On vérifie également que $e_{12}e_{21}e_{12}$ est la matrice $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ de rotation d'angle $\pi/2$, d'où $(e_{12}e_{21}e_{12})^4 = 1$. Le résultat que nous démontrerons est le suivant.

Théorème 19 (présentation de $SL_n(\mathbb{Z})$)**.** *Pour $n \geq 3$, $SL_n(\mathbb{Z})$ admet pour présentation par générateurs et relations*

$$\begin{aligned} \langle e_{ij}, i \neq j \mid\ & [e_{ij}, e_{kl}] = 1 && \text{pour } j \neq k, i \neq l, \\ & [e_{ij}, e_{jk}] = e_{ik} && \text{pour } i \neq k, \\ & (e_{12}e_{21}e_{12})^4 = 1 \rangle. \end{aligned}$$

Pour démontrer ce théorème, nous allons d'abord démontrer quelques lemmes qui sont vrais dans un cadre plus général que celui de l'anneau $\mathbb{Z}$.

On s'intéresse à $GL_n(\Lambda)$ le groupe des matrices inversibles de taille $n \times n$ à coefficients dans l'anneau Λ. On va supposer dès maintenant Λ commutatif car cette hypothèse sera indispensable dans les calculs qui suivent. Le groupe $GL_n(\Lambda)$ s'injecte naturellement dans $GL_{n+1}(\Lambda)$ par $M \mapsto \begin{pmatrix} & & & 0 \\ & M & & \vdots \\ & & & 0 \\ 0 & \dots & 0 & 1 \end{pmatrix}$. On notera $GL(\Lambda)$ la limite inductive (ou directe) des $GL_n(\Lambda)$. Les éléments unipotents seront notés comme dans le cas $\Lambda = \mathbb{Z}$: on note e_{ij}^{λ} la matrice ayant des 1 sur la diagonale et un λ en position (i, j), pour $i \neq j$ et $\lambda \in \Lambda$. On note $E_n(\Lambda)$ le sous-groupe de $GL_n(\Lambda)$ engendré par les e_{ij}^{λ}, et $E(\Lambda)$ leur limite inductive. Une reformulation du théorème 18 est l'égalité $GL_n(\mathbb{Z}) = E_n(\mathbb{Z})$.

Une question qui se pose et dont nous cherchons la réponse dans le cas $\Lambda = \mathbb{Z}$ est : quelles sont les relations existant entre les générateurs de $E(\Lambda)$? On a les relations déjà exhibées, appelées *relations de Steinberg*

$$e_{ij}^{\lambda} e_{ij}^{\mu} = e_{ij}^{\lambda+\mu} \tag{1}$$
$$[e_{ij}^{\lambda}, e_{kl}^{\mu}] = 1 \qquad si\ j \neq k, i \neq l \tag{2}$$
$$[e_{ij}^{\lambda}, e_{jk}^{\mu}] = e_{ik}^{\lambda\mu} \qquad si\ i \neq k. \tag{3}$$

L'idée est alors d'introduire un groupe abstrait défini par générateurs et relations et qui imite le comportement déjà observé des e_{ij}^{λ}.

Définition 12 (groupe de Steinberg)**.** Pour $n \geq 3$, le *groupe de Steinberg* $St_n(\Lambda)$ est le groupe défini par les générateurs x_{ij}^{λ}, pour $1 \leq i, j \leq n, i \neq j, \lambda \in \Lambda$, et les relations :

$$x_{ij}^{\lambda} x_{ij}^{\mu} = x_{ij}^{\lambda+\mu}$$
$$[x_{ij}^{\lambda}, x_{kl}^{\mu}] = 1 \qquad si\ j \neq k, i \neq l$$
$$[x_{ij}^{\lambda}, x_{jk}^{\mu}] = x_{ik}^{\lambda\mu} \qquad si\ i \neq k.$$

Le groupe $St_n(\Lambda)$ s'injecte naturellement dans $St_{n+1}(\Lambda)$, on peut donc parler de la limite inductive $ST(\Lambda)$.

On définit le morphisme canonique

$$\Phi \ : \ St_n(\Lambda) \to GL_n(\Lambda)$$
$$x_{ij}^{\lambda} \mapsto e_{ij}^{\lambda}.$$

L'image par Φ de $St_n(\Lambda)$ est évidemment égale au sous-groupe $E_n(\Lambda)$. En passant à la limite directe, on obtient le morphisme $\Phi \ : \ St(\Lambda) \to GL(\Lambda)$, d'image $E(\Lambda)$. Ce qu'on veut déterminer est donc le noyau de Φ, ou plutôt le noyau $\ker(\Phi|_{St_n(\Lambda)}) = \ker(\Phi)|_{St_n(\Lambda)}$. En K-théorie, (voir par exemple [Mil]) ce noyau a une grande importance.

Définition 13. On appelle $K_2\Lambda$ le noyau de $\Phi \ : \ St(\Lambda) \to GL(\Lambda)$.

Le théorème 19 découle alors du théorème suivant.

Théorème 20. *Pour $n \geq 3$, le groupe $St_n(\mathbb{Z})$ est une extension centrale :*

$$1 \ \to \ C_n \ \to \ St_n(\mathbb{Z}) \ \to \ E_n(\mathbb{Z}) \ \to \ 1$$

où C_n est cyclique d'ordre 2 engendré par $(x_{12}x_{21}x_{12})^4$.

Pour démontrer ce dernier théorème, on a besoin de quelques résultats généraux sur $St_n(\Lambda)$. On va s'intéresser dans $St_n(\Lambda)$ à quelques éléments particuliers. Pour toute unité u de Λ on pose

$$y_{ij}(u) = x_{ij}^u x_{ji}^{-u^{-1}} x_{ij}^u \qquad \text{et} \qquad z_{ij}(u) = y_{ij}(u)y_{ij}(-1).$$

On appelle Y_n le sous-groupe de $St_n(\Lambda)$ engendré par les $y_{ij}(u)$ pour $1 \leq i, j \leq n, i \neq j, u \in \Lambda$. On a encore $Y_n \subset y_{n+1}$, et on notera donc Y la limite inductive des Y_n.

On a par exemple, si $n \geq 3$:

$$\Phi(y_{13}(u)) = \begin{pmatrix} & & u \\ & 1 & \\ -u^{-1} & & \end{pmatrix} \text{ et } \Phi(z_{13}(u)) = \begin{pmatrix} u & & \\ & 1 & \\ & & u^{-1} \end{pmatrix}.$$

L'image par Φ de $y_{ij}(u)$ est le produit d'une matrice de transposition et d'une matrice diagonale de déterminant 1. On en déduit que l'image par Φ d'un élément y de Y_n est le produit d'une matrice de permutation π et d'une matrice diagonale d de déterminant 1. Le groupe Y tire son importance du lemme suivant.

Lemme 21. *Soit y un élément de Y_n tel que $\Phi(y) = \pi d$, le conjugué $yx_{ij}^\lambda y^{-1}$ est égal à $x_{\pi(i)\pi(j)}^{d_{ii}\lambda d_{jj}^{-1}}$. Le groupe Y_n agit transitivement sur la partie génératrice $x_{ij}^\lambda, i \neq j, \lambda \in \Lambda$ du groupe de Steinberg $St_n(\Lambda)$. On a plus précisément, avec y comme ci-dessus : $yy_{ij}(u)y^{-1} = y_{\pi(i)\pi(j)}(d_{ii}ud_{jj}^{-1})$.*

Démonstration. On a $\pi d e_{ij}^\lambda d^{-1}\pi^{-1} = e_{\pi(i)\pi(j)}^{d_{ii}\lambda d_{jj}^{-1}}$. Il suffit donc de faire la preuve pour $y = y_{kl}(u)$ (ceux-cis engendrent Y, et on a vu que leurs images par Φ s'écrivent comme produit d'une matrice de permutation et d'une matrice diagonale). Il y a alors 7 cas suivant les égalités entre i, j, k, l.

Traitons juste le cas $i = k, j \neq l$. On a

$$\begin{aligned} y_{il}(u)x_{ij}^\lambda y_{il}(-u) &= x_{il}^u x_{li}^{-u^{-1}}(x_{il}^u x_{ij}^\lambda x_{il}^{-u})x_{li}^{u^{-1}} x_{il}^{-u} \\ &= x_{il}^u (x_{li}^{-u^{-1}} x_{ij}^\lambda x_{li}^{u^{-1}})x_{il}^{-u} \\ &= x_{il}^u x_{lj}^{-u^{-1}\lambda}(x_{ij}^\lambda x_{il}^{-u}) = (x_{il}^u x_{lj}^{-u^{-1}\lambda} x_{il}^{-u})x_{ij}^\lambda \\ &= x_{ij}^{-\lambda} x_{lj}^{-u^{-1}\lambda} x_{ij}^\lambda = x_{lj}^{-u^{-1}\lambda}. \end{aligned}$$

Les autres cas se traitent de manière similaire. □

Corollaire 22. *Le noyau C_n de $\Phi|_{Y_n}$ est dans le centre de $St_n(\Lambda)$.*

Démonstration. Si $\Phi(y) = I$ pour $y \in Y_n$, appliquons Φ à $yx_{ij}^{\lambda}y^{-1} = x_{kl}^{\mu}$, on a alors $e_{ij}^{\lambda} = e_{kl}^{\mu}$, d'où $i = j, k = l, \lambda = \mu$, donc $x_{ij}^{\lambda} = x_{kl}^{\mu}$, et par conséquent $yx_{ij}^{\lambda} = x_{ij}^{\lambda}y$. □

Corollaire 23. *Pour tout $u \in \Lambda$, on a la relation $y_{ij}(u) = y_{ji}(-u^{-1})$.*

Démonstration. Il suffit d'appliquer la formule du lemme 21 à $y = y_{ij}(u)$, d'où $y_{ij}(u) = yy_{ij}(u)y^{-1} = y_{ji}(-u^{-1}uu^{-1}) = y_{ji}(-u^{-1})$. □

Appliquons maintenant le lemme 21 à $y = z_{ij}(u)$: on a pour i, j, k distincts :

$$\begin{aligned} z_{ij}(u)z_{ik}(v)z_{ij}(u)^{-1} &= z_{ij}(u)y_{ik}(v)y_{ik}(-1)z_{ij}(u)^{-1} \\ &= y_{ik}(uv)y_{ik}(-u) = z_{ik}(uv)z_{ik}(u)^{-1}. \end{aligned}$$

En multipliant par $z_{ik}(v)^{-1}$ à droite, on obtient

$$[z_{ij}(u), z_{ik}(v)] = z_{ik}(uv)z_{ik}(u)^{-1}z_{ik}(v)^{-1}. \quad (*)$$

Le terme de droite ne dépend pas de j. Par symétrie, il ne dépend pas de k non plus. Montrons qu'il ne dépend même pas de i. En effet, on a $y_{ri}(1)z_{ij}(u)y_{ri}(-1) = z_{rj}(u)$ donc $y_{ri}(1)[z_{ij}(u), z_{ik}(v)]y_{ri}(-1) = [z_{rj}(u), z_{rk}(v)]$. Or d'après (*), $[z_{ij}(u), z_{ik}(v)]$ est dans C_n, qui est central dans $St_n(\Lambda)$, donc

$$[z_{ij}(u), z_{ik}(v)] = [z_{rj}(u), z_{rk}(v)],$$

et $[z_{ij}(u), z_{ik}(v)]$ est bien indépendant de i. Ce crochet joue donc un rôle important puisqu'il ne dépend que de u et v. Nous montrerons plus loin que C_n est engendré par ces crochets.

Définition-Lemme 24. *On appelle symbole de Steinberg, noté $\{u, v\}$, le crochet $[z_{ij}(u), z_{ik}(v)] = z_{ik}(uv)z_{ik}(u)^{-1}z_{ik}(v)^{-1}$ (pour $i \neq j$ et $i \neq k$) . Il est*
(i) antisymétrique : $\{v, u\} = \{u, v\}^{-1}$,
(ii) bimultiplicatif : $\{uv, w\} = \{u, w\}\{v, w\}$,
(iii) à valeurs dans le groupe C_n.

Démonstration. Le point *(i)* découle de la formule générale $[a, b] = [b, a]^{-1}$.
Le point *(ii)* provient du calcul suivant :

$$\begin{aligned} \{uv, w\} &= [z_{ij}(uv), z_{ik}(w)] = [[z_{ir}(u), z_{ij}(v)]z_{ij}(v)z_{ij}(u), z_{ik}(w)] \\ &= [z_{ij}(v)z_{ij}(u), z_{ik}(w)] \text{ car } [z_{ir}(u), z_{ij}(v)] \in C_n \text{ qui est central} \\ &= [z_{ij}(v), [z_{ij}(u), z_{ik}(w)]][z_{ij}(u), z_{ik}(w)][z_{ij}(v), z_{ik}(w)] \\ &= [z_{ij}(u), z_{ik}(w)][z_{ij}(v), z_{ik}(w)] \text{ car } [z_{ij}(u), z_{ik}(w)] \in C_n \text{ qui est central.} \end{aligned}$$

(On n'a pas besoin que $n \geq 3$ ici car on n'a pas besoin que $r \neq k$.)
Le point (iii) se vérifie sur l'écriture matricielle de $\Phi(z_{ik}(uv)z_{ik}(u)^{-1}z_{ik}(v)^{-1})$. □

Il reste un dernier lemme technique à démontrer avant de commencer la démonstration principale.

Lemme 25. *Tous les $z_{ij}(u)$ peuvent s'exprimer en fonction des $z_{1k}(u)$, au sens où ils sont combinaison algébriques des $z_{1k}(u)$ et de leurs inverses.*

Démonstration. Si $j = 1$, le résultat voulu est simplement le corollaire 22. Traitons maintenant le cas où $j \neq 1$. D'une part on a $z_{ik}(u)y_{jk}(1)z_{ik}(u)^{-1}y_{jk}(-1) = y_{jk}(u)y_{jk}(-1) = z_{jk}(u)$ en utilisant le lemme 20. D'autre part on a $z_{ik}(u)(y_{jk}(1)z_{ik}(u)^{-1}y_{jk}(-1)) = z_{ik}(u)z_{ij}(u)^{-1}$, toujours grâce au lemme 20. Par conséquent on a $z_{jk}(u) = z_{ik}(u)z_{ij}(u)^{-1}$. En prenant $i = 1$ on a le résultat souhaité. □

On peut maintenant démontrer le théorème qui montre l'importance des symboles de Steinberg.

Théorème 26. *Le sous-groupe central $C_n = Ker(\Phi|_{Y_n})$ de $St_n(\Lambda)$ est engendré par les symboles $\{u, v\}$.*

Démonstration. Soit $Z_n \subset Y_n$ le sous-groupe engendré par les $z_{ij}(u)$. D'après le lemme 21, il s'agit d'un sous-groupe distingué de Y_n.

Montrons tout d'abord $C_n \subset Z_n$. Modulo Z_n, on a $y_{ij}(u) \equiv y_{ij}(1)$ par définition de $z_{ij}(u)$. Notons y_{ij} leur classe commune modulo Z_n. D'après le corollaire 23, on a $y_{ij} = y_{ji}$. Soit $c = y_{i_1j_1}(u_1)\dots y_{i_kj_k}(u_k)$ un élément de C_n. Fixons $l \in [|2, n|]$. Par le lemme 21, on a $y_{ij}y_{1l} = y_{\pi(1)\pi(l)}y_{ij}$ où π est la transposition (i, j). Un tel échange diminue la somme des l tels que y_{1l} apparait dans l'écriture de c, donc modulo Z_n on peut ramener tous les y_{1l} à gauche dans l'écriture de c. À l'aide des relations $y_{1l}y_{1l} = 1$ et $y_{1j}y_{1l} = y_{1l}y_{jl}$ pour $j \neq l$, on peut éliminer des y_{1l} à gauche de c de sorte qu'il n'en reste qu'un. Mais cet unique y_{1l} ne peut exister car sinon $\Phi(c)$ ne serait pas égal à l'identité. On peut par le même procédé éliminer $y_{2l}, y_{3l}, \dots$, et finalement on obtient $c \equiv I \bmod Z_n$. Par conséquent C_n s'écrit comme produit de $z_{ij}(u)$.

D'après le lemme 25, c peut donc s'écrire comme produit des $z_{1l}(u)$ et leurs inverses. Soit C'_n le sous-groupe de C_n engendré par les symboles $\{u, v\}$, on a

$$z_{1l}(uv) \equiv z_{1l}(u)z_{1l}(v) \bmod C'_n, \text{ et}$$
$$z_{1j}(u)z_{1l}(v) \equiv z_{1l}(v)z_{1j}(y) \bmod C'_n,$$

et par conséquent c peut s'écrire comme produit

$$c \equiv z_{12}(u_2)z_{13}(z_3)\dots z_{1n}(u_n) \bmod C'_n.$$

De cette écriture, on déduit que $\Phi(c)$ est la matrice diagonale $diag(u_2\dots u_n, u_2^{-1}, \dots, u_n^{-1})$. Or on a $\Phi(c) = 1$, d'où $u_2 = \dots = u_n = 1$, soit $c \equiv I \bmod C'_n$, ce qui signifie que c peut s'écrire comme produit de symboles de Steinberg. □

L'étape suivante dans la preuve du théorème 20 est de montrer que le sous-groupe central C_n est le noyau de Φ tout entier. Pour cela, on a besoin d'un résultat d'algèbre linéaire.

Le groupe $St_n(\mathbb{Z})$ agit à droite sur le module $\mathbb{Z}^n$ à travers le morphisme naturel $St_n(\mathbb{Z}) \to E_n(\mathbb{Z})$ et l'action de $E_n(\mathbb{Z})$ sur $\mathbb{Z}^n$, les éléments de $\mathbb{Z}^n$ étant regardés comme vecteurs-lignes. Pour $n = 2$, on a par exemple

$$(a, b)x_{12} = (a, a + b) \text{ et } (a, b)x_{21} = (a + b, b).$$

On utilise alors la norme $\mathbb{L}_1$ sur $\mathbb{Z}^n$ définie par

$$\|(a_1, \dots, a_n)\| = |a_1| + \dots + |a_n|.$$

Notons que l'action de Y_n sur $\mathbb{Z}^n$ préserve la norme.

Lemme 27 (lemme de Silvester)**.** *Soit β l'un des vecteurs de base standard de $\mathbb{Z}^n$, c'est-à-dire tel que $\|\beta\| = 1$. Tout élément de $St_n(\mathbb{Z})$ pour $n \geq 2$ peut s'écrire comme un produit $g_1g_2\dots g_ry$, où $y \in Y_n$ et chaque g_i est un générateur de Steinberg $x_{ij}^{\pm 1}$, tel que*

$$\|\beta g_1\| \leq \|\beta g_1 g_2\| \leq \dots \leq \|\beta g_1 \dots g_n\|.$$

Démonstration. À chaque suite $g_1, \dots, g_r$ de générateurs de Steinberg, on associe la suite $s_0 = 1, s_1, \dots, s_r$ d'entiers positifs définis par $s_i = \|\beta g_1 \dots g_i\|$. On va mesurer la déviation de cette suite par rapport à une suite monotone à l'aide d'un couple d'entiers naturels (λ, μ). Si la suite $s_0, s_1, \dots, s_r$ est monotone on pose $\lambda = \mu = 1$. Sinon on pose

$$\lambda = max\{s_i | s_i > s_{i+1}\} \text{ et } \mu = max\{i | s_i > s_{i+1}\}$$

On ordonne les paires (λ, μ) lexicographiquement.

Nous allons démontrer le lemme par récurrence su (λ, μ). Lorsque $(\lambda, \mu) = (1, 1)$ il n'y a rien à démontrer, et sinon on va montrer que le mot $g_1 \dots g_n y$ peut être modifié grâce aux relations de Steinberg de sorte à faire décroitre la paire (λ, μ). L'ordre lexicographique étant bien fondé, en répétant l'opération un nombre fini de fois, on obtient le mot recherché.

Supposons donc $(\lambda, \mu) > (1, 1)$. On a alors $\lambda = s_\mu > s_{\mu+1}$, $\mu \geq 1$ et $s_{\mu-1} \leq s_\mu$. Quitte à renuméroter les coordonnées et à conjuguer chaque g_i par un certain y_{kl} on peut supposer $g_\mu = x_{12}$. Posons $\beta g_1 \dots g_\mu = (a, b, c, \dots) \in \mathbb{Z}^n$. On a alors $\beta g_1 \dots g_{\mu+1} = (a, b-a, c, \dots)$. L'inégalité $s_{\mu-1} \leq s_\mu$ implique $|b-a| \leq |b|$. Cette condition équivaut à

$$|a| \leq 2|b| \text{ et si } a \neq 0 \text{ alors } ab > 0. \tag{4}$$

La preuve du lemme se divise en 7 cas selon la nature de $g_{\mu+1}$, 4 pour lesquels $g_{\mu+1}$ commute avec $g_\mu = x_{12}$ et 3 pour lesquels ces deux éléments ne commutent pas. Nous ne traiterons qu'un cas dans chaque catégorie, les autres se traitant avec des méthodes tout à fait similaires.

Cas 1: Supposons $g_{\mu+1} = x_{1j}^\varepsilon, j \geq 3$ qui commute avec $g_\mu = x_{12}$. Sans restreindre la généralité on peut supposer $j = 3, n = 3$. On a donc $(a, b, c) \xrightarrow{g_{\mu+1}} (a, b, \varepsilon a + c)$ avec $|c| > |\varepsilon a + c|$. Dans le mot $g_1 \dots g_r y$ remplaçons le produit $g_i g_{i+1} = x_{12} x_{13}^\varepsilon$ par $x_{13}^\varepsilon x_{12}$. La transformation $(a, b-a, c) \xrightarrow{x_{12}} (a, b, c) \xrightarrow{x_{13}^\varepsilon} (a, b, \varepsilon a + c)$ est remplacée par

$$(a, b-a, c) \xrightarrow{x_{13}^\varepsilon} (a, b-a, \varepsilon a + c) \xrightarrow{x_{12}} (a, b, \varepsilon a + c).$$

Les s_i sont inchangés, sauf $s_\mu = \|(a, b, c)\|$ qui est remplacé par $s_{\mu'} = \|(a, b-a, \varepsilon a + c)\|$, or on a $s_{\mu-1} > s_{\mu'}$, donc on a $(\lambda', \mu') < (\lambda, \mu)$.

Cas 2: Supposons $g_{\mu+1} = x_{21}^\varepsilon$ qui ne commute pas avec g_μ. L'idée supplémentaire à utiliser est d'introduire un y_{12} pour se débarasser du défaut de commutation. Le produit $g_\mu g_{\mu+1}$ correspond à la transformation $(a, b-a) \xrightarrow{x_{12}} (a, b) \xrightarrow{x_{21}^\varepsilon} (a + \varepsilon b, b)$. Si $\varepsilon = 1$, alors a et b sont de signes opposés ce qui contredit la seconde inégalité de (4). Donc $\varepsilon = -1$. Remplaçons le produit $x_{12} x_{21}^{-1}$ par $x_{21} y_{21} (-1)$ qui lui est égal. On peut pousser y_{21} à droite de $g_{\mu+2} \dots g_r$ sans rien changer à la suite $s_0, \dots, s_r$, puisque la norme est invariante par l'action des éléments de Y_n. La transformation associée devient alors $(a, b-a) \xrightarrow{x_{21}} (b, b-a)$ qui réduit (λ, μ) puisque λ est diminué. □

Théorème 28. *Pour $n \geq 2$, le noyau du morphisme $\Phi : St_n(\mathbb{Z}) \to E_n(\mathbb{Z})$ est contenu dans Y_n.*

Démonstration. Montrons le résultat par récurrence sur n. Celui-ci est clair pour $n = 1$. Supposons donc $n \geq 2$. Soit $\beta = (0, \dots, 0, 1)$. D'après le lemme de Silvester tout élément du noyau de Φ s'écrit comme un produit $g_1 \dots g_r y$ avec $y \in Y_n$ et $1 \leq \|\beta g_1\|$
$le \cdots \leq \|\beta g_1 \dots g_r y\| = 1$. On en déduit $1 = \|\beta g_1\| = \cdots = \|\beta g_1 \dots g_r y\| = 1$ et

par conséquent g_1, puis inductivement tous les g_i, laisse invariant β. Donc le mot $g_1 \dots g_r$ ne contient aucun générateur du type x_{nj}^{ε}. S'il contient des x_{in}^{ε}, on peut par les relations de Steinberg les envoyer tous à gauche. Notons x le produit de ces x_{in}^{ε}, le produit $g_1 \dots g_r y$ est donc égal à $xi(w)y$ pour un certain $w \in St_{n-1}(\mathbb{Z})$ où i désigne le morphisme naturel $St_{n-1}(\mathbb{Z}) \to St_n(\mathbb{Z})$. Les deux matrices $\Phi(x)$ et $\Phi(w)$ sont donc de la forme

$$\begin{pmatrix} 1 & & 0 & * \\ & \ddots & & * \\ 0 & & 1 & * \\ 0 & \dots & 0 & 1 \end{pmatrix} \text{ et } \begin{pmatrix} & & & 0 \\ & * & & \vdots \\ & & & 0 \\ 0 & \dots & 0 & 1 \end{pmatrix}.$$

Or leur produit vaut 1 donc $\Phi(x) = \Phi(w) = I$. D'après les relations de Steinberg, le sous-groupe de $St_n(\mathbb{Z})$ engendré par $x_{1n}, \dots, x_{n-1n}$ est commutatif, or x est un élément de ce sous-groupe, d'image par Φ triviale, d'où $x = 1$. Par hypothèse de récurrence, on a également $w = 1$, et donc $g_1 \dots g_n y = y \in Y_n$, d'où le résultat. □

Comme on sait que le groupe Y_n est engendré par les symboles de Steinberg, il ne reste plus qu'à calculer dans $St_n(\mathbb{Z})$ les crochets $\{-1, 1\}, \{1, -1\}$ et $\{-1, -1\}$.

Lemme 29. *Pour tout anneau Λ commutatif et pour tout $u \in \Lambda$ on a $\{-u, u\} = \{u, -u\} = 1$.*

Démonstration. D'après le lemme 21, on a $y_{ij}(-u.u) = y_{ij}(u)y_{ij}(-1)y_{ij}(-u)$, d'où $z_{ij}(-u.u) = z_{ij}(u)z_{ij}(-u)$ qui est la relation voulue : en effet on a $u, -u = z_{ij}(-u \cdot u)z_{ij}(-u)^{-1}z_{ij}(u)^{-1}$. □

Lemme 30. *L'élément $\{-1, -1\}$ de $St_n(\mathbb{Z})$ est d'ordre 2.*

Démonstration. On renvoie à un cours de topologie algébrique, par exemple [Pau1] ou [God] pour des précisions sur les résultats que nous admettrons.

On sait déjà par le lemme 24 que $\{-1, -1\}^{-1} = \{-1, -1\}$. Il s'agit donc de montrer $\{-1, -1\} \neq 1$. Il suffit d'établir ce fait dans $St(n, \mathbb{R})$, puisqu'on a une inclusion naturelle $St(n, \mathbb{Z}) \hookrightarrow St(n, \mathbb{R})$.

On introduit d'abord la notion de revêtement universel. Un revêtement universel sur un espace topologique connexe et localement connexe par arcs B est un revêtement $\pi : B \to \tilde{B}$ avec $\tilde{B}$ connexe, tel que pour tout revêtement connexe $p : X \to B$ avec X connexe et pour tous $\tilde{b} \in \tilde{B}$ et $x \in X$ tels que $\pi(\tilde{b}) = p(x)$, il existe un morphisme de revêtements $\Phi : \tilde{B} \to X$ de π sur p tel que $\Phi(\tilde{b}) = x$.

On peut montrer qu'un revêtement universel est unique à isomorphisme près et que tout espace séparé, connexe et localement contractile (en particulier tous

les espaces que nous aurons à considérer dans cette preuve) admet un revêtement universel. Enfin on peut montrer que si $p : X \to B$ est un revêtement avec X simplement connexe alors p est un revêtement universel. (On désignera par (*) ce résultat.)

On aura également besoin d'un résultat sur le relêvement des chemins :

Si $p : X \to B$ est un relêvement et $f : Y \to B$ une application continue, un relêvement de f est une application continue $\tilde{f} : Y \to X$ telle que $p \circ \tilde{f} = f$. Alors pour tout chemin c dans B d'origine b, et pour tout $x \in p^{-1}(b)$ il existe un unique relêvement $\tilde{c}$ de c d'origine x.

Enfin, on utilisera le fait que le revêtement universel de $SO(3)$ s'identifie avec la sphère $\mathbb{S}^3$ des quaternions de norme 1. Identifiant $\mathbb{R}^3$ avec l'espace des quaternions purs $\mathbb{H}^*$ (*ie* de partie réelle nulle), étant donné $q \in \mathbb{S}^3$ on définit un élément Φ_q de $SO(3)$ par $h \in \mathbb{R}^3 \to q(0,h)q^{-1} \in \mathbb{H}^* \simeq \mathbb{R}^3$. On en déduit un homomorphisme de groupes $\Phi : q \in \mathbb{S}^3 \to \Phi_q \in SO(3)$, dont on montre que c'est un revêtement, donc le revêtement universel d'après (*). En particulier tout quaternion de norme 1 détermine une rotation de $\mathbb{R}^3$. Notamment, k et j déterminent les rotations de matrices respectives :

$$r_j = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} = h_{13}(-1) \text{ et } r_k = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = h_{12}(-1).$$

Considérons maintenant le revêtement universel $\widetilde{SL(n,\mathbb{R})}$ de $SL(n,\mathbb{R})$. Le chemin $t \to e_{ij}^{t\lambda}$, paramétré par $[0,1]$, se relève en un unique chemin d'origine 1 de $\widetilde{SL(n,\mathbb{R})}$, dont on notera $\widetilde{e_{ij}^{\lambda}}$ l'extrémité. Les éléments $\widetilde{e_{ij}^{\lambda}}$ ainsi définis vérifient encore les relations de Steinberg, ce qui permet de définir un homomorhisme $\tilde{f}$ de $St(n,\mathbb{R})$ dans $\widetilde{SL(n,\mathbb{R})}$ par $x_{ij}^{\lambda} \to \widetilde{e_{ij}^{\lambda}}$.

En exhibant des chemins dans $St_n(\mathbb{R})$ de 1 à $h_{12}(-1)$ et de 1 à $h_{13}(-1)$ et en les relevant en des chemins dans $\widetilde{SL(n,\mathbb{R})}$ de 1 à j et de 1 à k respectivement, on montre que les images de $h_{12}(-1)$ et de $h_{13}(-1)$ sont k et j respectivement.

Voyant $\{-1,-1\}$ comme élément de $St_3\mathbb{R})$ et écrivant $\{-1,-1\} = [h_{12}(-1), h_{13}(-1)]$ on obtient donc : $\widetilde{\Phi}(-1,-1) = kjk^{-1}j^{-1} = -1$, donc $\{-1,-1\} \neq 1$. □

La preuve du théorème 20 est maintenant complète : le thérème 28 nous assure que le noyau de $\Phi|_{St_n(\mathbb{Z})}$ est dans le groupe Y_n, le théorème 26 nous prouve que ce noyau est engendré par les symboles de Steinberg, et enfin les deux derniers lemmes nous montrent que seul $\{-1,-1\} = (x_{12}x_{21}x_{12})^4$ est non nul et donc que C_n est cyclique d'ordre 2.

4 Génération bornée de $SL_n(\mathbb{Z})$ pour n≥ 3

Dans cette dernière partie, nous allons montrer que le groupe $SL_n(\mathbb{Z})$ pour n≥ 3 a une structure quasi opposée à celle de $SL_2(\mathbb{Z})$ puisque ce dernier a une structure presque libre, alors que $SL_n(\mathbb{Z})$ pour n≥ 3 a la propriété dite de génération bornée.

Définition 14. Un groupe G est dit *à génération bornée* par rapport à la partie S s'il existe un entier naturel n tel que tout élément de G peut s'écrire comme produit d'au plus n puissances d'éléments de S.

Par exemple, un groupe abélien de type fini a la propriété de génération bornée par rapport à n'importe quelle famille génératrice, tandis qu'un produit libre ne l'a pas par rapport à sa partie génératrice canonique. En effet si $g_1 \in G_1$ et $g_2 \in G_2$, alors $(g_1g_2)^n \in G_1 * G_2$ est le produit d'au moins $2n$ éléments de la partie génératrice canonique de $G_1 * G_2$. En particulier un groupe libre n'a pas cette propriété, et ni $PSL_2(\mathbb{Z})$ ni $SL_2(\mathbb{Z})$ par rapport aux parties génératrices exhibées ne l'ont plus.

Nous allons montrer que pour $n \geq 3$, le groupe $SL_n(\mathbb{Z})$ a cette propriété de génération bornée. Pour cela, nous aurons besoin de quatre lemmes préliminaires de nature combinatoire et arithmétique.

Lemme 31. *Soit ε un entier positif ou nul, M et N deux éléments de $SL_n(\mathbb{Z})$ avec*

$$M = \begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ et } N = \begin{pmatrix} a^\varepsilon & b & 0 \\ x & y & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

alors en au plus 17 opérations élémentaires on peut transformer M^ε en N.

Démonstration. Posons $L = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$. On a $L^2 = -I + tr(L).L$. Définissons récursivement deux suites de fonctions polynômiales (f_n) et (g_n) par :

$$f_0(t) = 1 \ , \ g_0(t) = 0$$
$$f_{n+1}(t) = -g_n(t) \ , \ g_{n+1}(t) = tg_n(t) + f_n(t).$$

Posons $f = f_\varepsilon(tr(L))$ et $g = g_\varepsilon(tr(L))$, on vérifie par une récurrence facile que pour tout $n \in \mathbb{N}$, on a : $L^N = f_n(tr(L))I + g_n(tr(L))L$, d'où en particulier :

$$L^\varepsilon = fI + gL.$$

Une récurrence facile montre que $g_{n+1}(t)g_{n-1}(t) = g_n(t)^2 - 1$, donc $f(t)$ divise $g(t)^2 - 1$, par conséquent f divise $g^2 - 1$, et il existe donc dans $\mathbb{Z}$ une factorisation $f = f_+f_-$ avec

$$g+1 = jf_+ \text{ et } g-1 = kf_-.$$

Posons

$$F = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & f_- \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & k & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & g & f_- \\ 0 & k & 1 \end{pmatrix},$$

$$G = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1-f_+ \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ -f_- & 1 & 0 \\ j & 0 & 1 \end{pmatrix} = \begin{pmatrix} * & 0 & * \\ -f_- & 1 & 0 \\ g & 0 & f_+ \end{pmatrix}.$$

On a alors

$$H = FG = \begin{pmatrix} * & 0 & * \\ 0 & g & f \\ 1 & * & * \end{pmatrix}.$$

Il suffit alors de 4 opérations élémentaires pour transformer H en

$$J = \begin{pmatrix} 1 & 0 & -b \\ 0 & g & f+ga \\ * & * & * \end{pmatrix}.$$

Par exemple, cette suite d'opérations convient :

$$\begin{pmatrix} * & 0 & * \\ 0 & g & f \\ 1 & * & * \end{pmatrix} \to \begin{pmatrix} * & 0 & * \\ 0 & g & f+ga \\ 1 & * & * \end{pmatrix} \to \begin{pmatrix} 1 & * & * \\ 0 & g & f+ga \\ * & 0 & * \end{pmatrix}$$
$$\to \begin{pmatrix} 1 & 0 & * \\ 0 & g & f+ga \\ * & * & * \end{pmatrix} \to \begin{pmatrix} 1 & 0 & -b \\ 0 & g & f+ga \\ * & * & * \end{pmatrix}$$

Comme modulo b les matrices M et M^ε sont triangulaires inférieures, on a $f + ga \equiv a^\varepsilon \bmod b$, pour le voir il suffit de remarquer que $L^\varepsilon = fI + gL$ et de comparer les termes en position $(1,1)$, donc en une opération élémentaire on peut transformer N en

$$K = \begin{pmatrix} f+ga & b & 0 \\ * & y & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Posons

$$L = KJ = \begin{pmatrix} f+ga & bg & 0 \\ * & * & 1 \\ * & * & * \end{pmatrix}.$$

Il suffit de 6 opérations élémentaires pour passer de L à M^ε, (procédé analogue à celui tranformant H en J) donc en tout 17 opérations pour passer de N à M^ε. □

Le lemme suivant est le lemme clé pour démontrer la propriété de génération bornée de $SL_n(\mathbb{Z})$.

Lemme 32. *Soit*

$$M = \begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

un élément de $SL_3(\mathbb{Z})$. Soit ϕ la fonction indicatrice d'Euler. Si $pgcd(\phi(b), \phi(c))$ divise ε, alors on peut passer de la matrice M^ε à la matrice I en au plus 38 opérations élémentaires.

Démonstration. D'après le théorème de Bézout, on peut choisir $r, s \in \mathbb{Z}$ tels que $r\phi(b) - s\phi(c) = pgcd(\phi(b), \phi(c))$, or d'après le petit théorème de Fermat, il existe $b', c' \in \mathbb{Z}$ tels que $a^{r\phi(b)} = 1 + bb'$ et $d^{s\phi(c)} = 1 + cc'$. Posons alors

$$B = \begin{pmatrix} 1 & b & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ b' & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} a^{r\phi(b)} & b & 0 \\ b' & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

$$C = \begin{pmatrix} 1 & -c & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ -c' & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} d^{s\phi(c)} & -c & 0 \\ -c' & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

D'après le lemme précédent, B peut être transformée en $M^{r\phi(b)}$ en 17 opérations élémentaires, et par analogie C en $M^{-s\phi(c)}$, puisque :

$$M^{-1} = \begin{pmatrix} d & -c & 0 \\ b & a & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Par conséquent $M^{r\Phi(b)-s\phi(c)} = M^{pgcd(\Phi(b),\Phi(c)}$ peut être transformmée en $2 * 17 + 4 = 38$ opérations élémentaires en la matrice I. □

Lemme 33. *Soit* $M' = \begin{pmatrix} a' & b' \\ * & * \end{pmatrix} \in SL_2(\mathbb{Z})$. *Alors il existe* $a, b \in \mathbb{Z}$ *tels que*

(*i*) a *et* b *sont premiers avec* $b \equiv 5$ *mod 6,*

(*ii*) a *ne divise pas* $b-1$,

(*iii*) M' *peut être transformée en au plus 4 opérations élémentaires en* $\begin{pmatrix} a^2 & b \\ * & * \end{pmatrix}$.

Démonstration. Montrons qu'en 2 opérations élémentaires, on peut transformer M' en $M'' = \begin{pmatrix} a'' & b'' \\ * & * \end{pmatrix}$ avec $a'' \equiv 3 \bmod 4$ et b'' impair. En effet a' et b' ne sont pas tous deux pairs, donc on peut choisir $\varepsilon \in 0, 1$ tel que $b'' = b' + \varepsilon a'$ soit impair, puis choisir η tel que $a'' = a' + \eta b'' \equiv 3 \bmod 4$ et $a'' \neq 0 \bmod 3$. Donc en deux opérations, on peut transformer M' en M''.

Si le symbole de Legendre $\left(\begin{smallmatrix} b'' \\ a'' \end{smallmatrix}\right)$ vaut 1, alors par le théorème de la progression arithmétique de Dirichlet, il existe un nombre premier b satisfaisant $b \equiv 1 \bmod 4$, $b \equiv 2 \bmod 3$. D'où, d'après la loi de réciprocité quadratique, $\left(\begin{smallmatrix} a'' \\ b \end{smallmatrix}\right) = (-1)^{\frac{(a''-1)(b-1)}{4}} \left(\begin{smallmatrix} b'' \\ a'' \end{smallmatrix}\right) = 1$, et donc il existe a tel que $a^2 \equiv a'' \bmod b$. En 2 opérations élémentaires, on peut alors passer de M'' à $\begin{pmatrix} a^2 & b \\ * & * \end{pmatrix}$.

Si $\left(\begin{smallmatrix} b'' \\ a'' \end{smallmatrix}\right) = -1$, alors par le théorème de Dirichlet, il existe b premier satisfaisant $b \equiv 3 \bmod 4$, $b \equiv 2 \bmod 3$. Donc d'après la loi de réciprocité quadratique on a $\left(\begin{smallmatrix} a'' \\ b \end{smallmatrix}\right) = (-1)^{\frac{(a''-1)(b-1)}{4}} \left(\begin{smallmatrix} b'' \\ a'' \end{smallmatrix}\right) = 1$, et donc il existe a tel que $a^2 \equiv a'' \bmod b$. En 2 opérations élémentaires on peut alors passer de M'' à $\begin{pmatrix} a^2 & b \\ * & * \end{pmatrix}$. □

Lemme 34. *Soient* a, b *premiers tels que ni* a *ni 3 ne divisent* $b-1$. *Alors pour tout* $e \in \mathbb{Z}$, *il existe* $c \in \mathbb{Z}$ *tel que* $c \equiv e$ *mod* a *et* $pgcd(\phi(b), \phi(c)) = 2$.

Démonstration. D'après le théorème de Dirichlet, il existe c premier tel que $c \equiv 3 \bmod b-1$ et $c \equiv e \bmod a$. On a alors $c - 1 \equiv 2 \bmod b-1$, or $b-1$ et $c-1$ sont impairs, d'où $pgcd(\phi(b), \phi(c)) = pgcd(b-1, c-1) = 2$. □

On peut maintenant démontrer le théorème voulu avec une borne effective pour la propriété de génération bornée

Théorème 35. *Le groupe $SL_n(\mathbb{Z})$ est à génération bornée, toute matrice de $SL_n(\mathbb{Z})$ peut s'écrire comme produit de $(3n^2 - n)/2 + 54$ matrices élémentaires.*

Démonstration. La preuve donnée du théorème 18 montre que pour $n \geq 3$, il suffit de $3n - 2$ opérations élémentaires pour se ramener d'une matrice de taille n à une matrice de taille $n - 1$. Par récurrence, il faut donc $(3n^2 - n - 10)/2$ opérations élémentaires pour transformer une matrice quelconque de $SL_n(\mathbb{Z})$ en une matrice de la forme

$$M' = \begin{pmatrix} a' & b' & & & \\ c' & d' & & & \\ & & 1 & & \\ & & & \ddots & \end{pmatrix}.$$

D'après le lemme 33, en 4 opérations, on peut transformer M' en

$$M'' = \begin{pmatrix} a^2 & b & & & \\ c'' & d'' & & & \\ & & 1 & & \\ & & & \ddots & \end{pmatrix},$$

où a et b satisfont les conditions du lemme 33. D'après le lemme 34 il existe $c \in \mathbb{Z}$ tel que $c \equiv e \bmod a$ et $pgcd(\phi(b), \phi(c)) = 2$. Soit $d \in \mathbb{Z}$ et

$$M = \begin{pmatrix} a & b & & & \\ c & d & & & \\ & & 1 & & \\ & & & \ddots & \end{pmatrix},$$

En appliquant le lemme 31, on peut alors transformer M'' en M^2 en 17 opérations, et en appliquant le lemme 32, on peut transformer M^2 en I en 38 opérations. Toutes ces dernières transformations ont nécessité $4 + 17 + 38$ opérations élémentaires, d'où le résultat. □

Il est à noter que le seul obstacle à la construction effective des $(3n^2 - n)/2 + 54$ matrices élémentaires est l'impossibilité algorithmique actuelle de trouver un nombre premier dans un progression arithmétique.

Bibliographie

[Bau] G. Baumslag, *Topics in Combinatorial Group Theory*, Lectures in Mathematics ETH Zürich, Birkäuser Verlag, (1993).

[CK] D. Carter, G. Keller, *Bounded elementary generation of $SL_n(\mathcal{O})$*, American Journal of Mathematics, 105 (1984) 673-687.

[Fre] J. Fresnel, *Groupes*, Hermann, (2001).

[KN] M. Kassabov, N. Nikolov, *Universal lattices and property τ*, preprint `arXiv:math.GR/0502112` (2005).

[Kat] S. Katok, *Fuchsian groups*, Chicago Lectures in Mathematics, Chicago University Press, (1992).

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

[Lan] S. Lang, *Algebra*, Addison-Wesley, (1984).

[Mil] J. Milnor, *Introduction to Algebraic K-theory*, Annals of Mathematics Studies, Princeton University Press, 72 (1971).

[Pau1] F. Paulin, *Topologie algébrique élémentaire*, cours à l'ENS, `http://www.dma.ens.fr/edition/NotesCours/topoalg.ps`

[Pau2] F. Paulin, *Géométrie différentielle*, cours à l'ENS, `http://www.dma.ens.fr/edition/NotesCours/index.html`

[Ser] J.-P. Serre, *Cours d'Arithmétique*, Presses universitaires de France, (1970).