Introduction à la théorie géométrique des groupes

Cours de Master 2, année 2016-2017

Université de Montpellier

Thomas Haettel

en cours de rédaction

Table des matières

Chapitre 1

Notions de topologie algébrique

De bonnes références sont [God71], [Hat02] et [Pau10].

Nous allons faire de brefs rappels de topologie algébrique élémentaire, avec notamment le groupe fondamental d'un espace topologique, qui est l'un des premiers invariants, et qui est au coeur du lien entre groupes discrets et topologie. Nous rappellerons également la classification des surfaces compactes.

1.1 Homotopie, groupe fondamental

Définition 1.1.1. *Soient X et Y deux espaces topologiques, et $f, g : X \to Y$ deux applications continues. On dit que f et g sont* ***homotopes****, et on note $f \sim g$, s'il existe une application continue $h : X \times [0,1] \to Y$ telle que $h(\cdot, 0) = f$ et $h(\cdot, 1) = g$. Autrement dit, on peut "passer continûment" de f à g.*

Si de plus A est une partie de X, on dit que f et g sont ***homotopes relativement*** *à A s'il existe une application continue $h : X \times [0,1] \to Y$ telle que $h(\cdot, 0) = f$, $h(\cdot, 1) = g$ et $\forall a \in A, \forall t \in [0,1], h(a,t) = f(a) = g(a)$. Autrement dit, on peut "passer continûment" de f à g "en laissant A fixe".*

Exemples.

- Si f et g sont deux applications continues quelconques de $[0,1]$ dans $\mathbb{R}$ ou $\mathbb{R}^2$, elles sont homotopes. Si $f(0) = g(0)$ et $f(1) = g(1)$, f et g sont homotopes relativement à $\{0,1\}$.
- Si $f : t \in [0,1] \mapsto e^{i\pi t} \in \mathbb{S}^1$ et $g : t \in [0,1] \mapsto e^{-i\pi t} \in \mathbb{S}^1$ parcourent les deux demi-cercles de $\mathbb{S}^1$ entre les points opposés 1 et -1, f et g ne sont pas homotopes relativement à $\{0,1\}$ (même si elles sont homotopes).
- Si $f : z \in \mathbb{S}^1 \mapsto z \in \mathbb{S}^1$ parcourt le cercle $\mathbb{S}^1$ et $g : z \in \mathbb{S}^1 \mapsto 1 \in \mathbb{S}^1$ est constante, alors f et g ne sont pas homotopes.

Remarque. Pour le cercle $\mathbb{S}^1$, on choisira indifférement comme modèle le cercle unité de $\mathbb{C}$, ou bien le quotient $\mathbb{R}/\mathbb{Z}$, ou encore le quotient $[0,1]/(0 \sim 1)$.

Définition 1.1.2. *Soit X un espace topologique. Un* ***lacet*** *de X est une application continue du cercle $\mathbb{S}^1$ dans X. Si $x_0 \in X$ est un point base, un* ***lacet basé en*** *x_0 est une application continue $\ell : \mathbb{S}^1 \to X$ telle que $\ell(0) = x_0$ (où $0 \in \mathbb{S}^1$ désigne un point base de $\mathbb{S}^1$).*

Définition 1.1.3. *Soit X un espace topologique, et $\ell, \ell' : \mathbb{R}/\mathbb{Z} \to X$ deux lacets. On définit la concaténation de ℓ et ℓ' comme le lacet suivant :*

$$\begin{array}{rcl} \ell \cdot \ell' : \mathbb{R}/\mathbb{Z} & \to & X \\ t \in \left[0, \dfrac{1}{2}\right] & \mapsto & \ell(2t) \\ t \in \left[\dfrac{1}{2}, 1\right] & \mapsto & \ell'(2t-1). \end{array}$$

Notons que si ℓ et ℓ' sont basés en $x_0 \in X$, alors $\ell \cdot \ell'$ est basé en x_0.

Proposition 1.1.4. *Soit X un espace topologique, et $x_0 \in X$ un point base. L'ensemble des classes d'homotopies de lacets $\mathbb{R}/\mathbb{Z} \to X$ basés en x_0, relativement à $0 \in \mathbb{R}/\mathbb{Z}$, muni de la loi de composition interne de concaténation, est un groupe, noté $\pi_1(X, x_0)$ et appelé* ***groupe fondamental*** *de X en x_0.*

Démonstration. [Idée] L'élément neutre est la classe d'homotopie du lacet constant en x_0 (d'où l'importance de l'homotopie). L'inverse de la classe d'homotopie $[\ell]$ d'un lacet $\ell : \mathbb{R}/\mathbb{Z} \to X$ est la classe d'homotopie $[\overline{\ell}]$ du lacet $\overline{\ell} : \mathbb{R}/\mathbb{Z} \to X : t \mapsto \ell(1-t)$ parcouru en sens inverse. $\square$

Exemples.

- On a $\pi_1(\mathbb{R}, 0) = \{1\}$, et de même $\pi_1(\mathbb{R}^2, 0) = \{1\}$.
- Le cercle $\mathbb{S}^1$ a pour groupe fondamental $\mathbb{Z}$. Plus précisément, l'application suivante est un isomorphisme de groupes :

$$\begin{array}{rcl} \mathbb{Z} & \to & \pi_1(\mathbb{S}^1, 1) \\ n & \mapsto & \left[z \in \mathbb{S}^1 \mapsto z^n\right]. \end{array}$$

  Autrement dit, le nombre n de tours qu'un lacet fait autour de $\mathbb{S}^1$ détermine entièrement le lacet à homotopie près.
- On a $\pi_1(\mathbb{R}^2 \backslash \{(0,0)\}, (1,0)) \simeq \mathbb{Z}$.
- On a $\pi_1(\mathbb{S}^2, x_0) = \{1\}$.
- Le tore $\mathbb{T}^2 = \mathbb{S}^1 \times \mathbb{S}^1$ a pour groupe fondamental $\mathbb{Z}^2$. Plus précisément, l'application suivante est un isomorphisme de groupes :

$$\begin{array}{rcl} \mathbb{Z}^2 & \to & \pi_1(\mathbb{T}^2, (1,1)) \\ (n,p) & \mapsto & \left[z \in \mathbb{S}^1 \mapsto (z^n, z^p)\right]. \end{array}$$

Proposition 1.1.5. *Soit X un espace topologique, et x_0, y_0 deux points de X appartenant à la même composante connexe par arcs. Alors $\pi_1(X, x_0)$ et $\pi_1(X, y_0)$ sont isomorphes. En particulier, si X est connexe par arcs, le groupe fondamental de X ne dépend pas du point base (à isomorphisme près).*

Démonstration. [Idée] Si $f : [0,1] \to X$ est un chemin continu de $f(0) = x_0$ à $f(1) = y_0$, alors l'application suivante est un isomorphisme de groupes :

$$\begin{array}{rcl} \pi_1(X, y_0) & \mapsto & \pi_1(X, x_0) \\ [\ell] & \mapsto & \left[f \cdot \ell \cdot \overline{f}\right]. \end{array}$$

$\square$

Proposition 1.1.6. *Si $f : X \to Y$ est un homéomorphisme entre deux espaces topologiques X et Y, et si $x_0 \in X$, alors $\pi_1(X, x_0)$ et $\pi_1(Y, f(x_0))$ sont isomorphes.*

Exemples.

- $\mathbb{R}$ et $\mathbb{S}^1$ ne sont pas homéomorphes.
- $\mathbb{S}^1$ et $\mathbb{S}^2$ ne sont pas homéomorphes.
- $\mathbb{S}^2$ et $\mathbb{T}^2$ ne sont pas homéomorphes.

Définition 1.1.7. *Un espace topologique X connexe par arcs est dit **simplement connexe** s'il vérifie l'une des conditions équivalentes suivantes :*

- *son groupe fondamental est trivial,*
- *toute application continue de $\mathbb{S}^1$ dans X se prolonge à une application continue du disque $\mathbb{D}^2$ dans X,*
- *deux chemins de même origine et même extrémité sont homotopes (relativement aux extrémités).*

Exemples.

- $\mathbb{R}$, $\mathbb{R}^2$ et $\mathbb{S}^2$ sont simplement connexes.
- $\mathbb{S}^1$, $\mathbb{T}^2$ ne sont pas simplement connexes.

Exercice 1. *On dit qu'un espace topologique X est **contractile** si l'application identité $X \to X$ est homotope à une application constante.*

Montrer que si X est contractile, alors X est simplement connexe.

Proposition 1.1.8. *Soient (X, x_0) et (Y, y_0) deux espaces topologiques connexes par arcs pointés, et soit $f : X \to Y$ une application continue telle que $f(x_0) = y_0$. Alors l'application suivante est un morphisme de groupes :*

$$\begin{array}{rcl} f_* : \pi_1(X, x_0) & \to & \pi_1(Y, y_0) \\ [\ell] & \mapsto & [f \circ \ell]. \end{array}$$

Exercice 2. *Soit X un espace topologique et $A \subset X$ un sous espace. On dit que A est un **rétracte par déformation** de X s'il existe une application continue $h : X \times [0,1] \to X$ telle que :*

- $\forall x \in X, h(x, 0) = x$,
- $\forall x \in X, h(x, 1) \in A$ *et*
- $\forall a \in A, h(a, 1) = a$.

Montrer que si A est un rétracte par déformation de X et $x_0 \in A$, alors $\pi_1(X, x_0)$ et $\pi_1(A, x_0)$ sont naturellement isomorphes.

Exemple. $\mathbb{S}^1$ est un rétracte par déformation de $\mathbb{R}^2 \backslash \{(0,0)\}$.

1.2 Revêtements

Définition 1.2.1. *Soient X et B deux espaces topologiques. Une application continue $f : X \to B$ est un* **revêtement** *si tout point $y \in B$ admet un voisinage ouvert V tel que $f^{-1}(V) = \bigsqcup_{i\in I} U_i$ soit une réunion disjointe non vide d'ouverts U_i de X, tels que pour tout $i \in I$, $f|_{U_i} : U_i \to V$ soit un homéomorphisme.*

Exemples.

- L'identité $X \to X$ est un revêtement.
- L'application $\mathbb{S}^1 \to \mathbb{S}^1$ qui à z associe z^2 est un revêtement.
- L'application $t \in \mathbb{R} \to e^{2i\pi t} \in \mathbb{S}^1$ est un revêtement.

Définition 1.2.2. *Soit G un groupe et X un ensemble. Une* **action de groupe** *de G sur X est une application de $G \times X$ dans X, notée $(g, x) \mapsto g \cdot x$, telle que*

$$\forall g, h \in G, \forall x \in X, g \cdot (h \cdot x) = (gh) \cdot x.$$

L'action est dite **libre** *si le stabilisateur de tout point est trivial :*

$$\forall g \in G, \forall x \in X, g \cdot x = x \Rightarrow g = e.$$

L'action est dite **fidèle** *si l'action de tout élément non trivial est non triviale :*

$$\forall g \in G, (\forall x \in X, g \cdot x = x) \Rightarrow g = e.$$

Définition 1.2.3. *Soit G un groupe discret agissant sur un espace topologique X. L'action est dite continue si, pour tout $g \in G$, l'application $x \in X \mapsto g \cdot x \in X$ est un homéomorphisme.*

L'action est dite **propre, ou proprement discontinue** *si pour tout compact $K \subset X$, l'ensemble $\{g \in G \mid g \cdot K \cap K \neq \emptyset\}$ est fini.*

On note $G\backslash X$ l'espace des orbites de l'action. C'est le quotient de X par la relation d'équivalence : $x \sim y$ s'il existe $g \in G$ tel que $g \cdot x = y$, muni de la topologie quotient.

Exemples.

- Considérons l'action de $\mathbb{Z}$ sur $\mathbb{R}$ par translations :

  $$\begin{array}{rcl} \mathbb{Z} \times \mathbb{R} & \to & \mathbb{R} \\ (n, x) & \mapsto & n + x. \end{array}$$

  C'est une action continue, libre, fidèle et propre. Son quotient est le cercle $\mathbb{R}/\mathbb{Z} \simeq \mathbb{S}^1$.

- Considérons l'action de $\mathbb{Z}$ sur $\mathbb{R}/\mathbb{Z}$ par rotations de multiples d'un angle fixé $\alpha \in \mathbb{R}$:

  $$\begin{array}{rcl} \mathbb{Z} \times \mathbb{R}/\mathbb{Z} & \to & \mathbb{R}/\mathbb{Z} \\ (n, x) & \mapsto & n\alpha + x. \end{array}$$

  C'est une action continue, non propre.

  Si α est rationnel, elle n'est pas libre ni fidèle.

  Si α est irrationnel, elle est libre et fidèle.

Proposition 1.2.4. *Soit G un groupe discret agissant librement, continûment et proprement sur un espace topologique séparé X. Alors chaque orbite de G est discrète, et la projection canonique $X \to G\backslash X$ est un revêtement.*

Exemple. L'action de $\mathbb{Z}$ sur $\mathbb{R}$ par translations définit le revêtement $t \in \mathbb{R} \mapsto t+\mathbb{Z} \in \mathbb{R}/\mathbb{Z}$.

Théorème 1.2.5. *Si X est un espace simplement connexe et B est un espace connexe par arcs, alors tout revêtement $X \to B$ est un homéomorphisme.*

Définition 1.2.6. *Un espace topologique X est dit* ***semilocalement simplement connexe*** *si tout point $x \in X$ admet un voisinage U tel que tout lacet en x contenu dans U soit homotope, dans X, au lacet constant en x.*

Exemple. L'espace des anneaux hawaïens : $X = \bigcup_{n \geqslant 1} \mathbb{S}(\frac{1}{n}, \frac{1}{n}) \subset \mathbb{R}^2$ n'est pas semilocalement simplement connexe.

Théorème 1.2.7. *Soit X un espace topologique séparé, connexe, localement connexe par arcs et semilocalement simplement connexe. Alors X admet un revêtement simplement connexe $\tilde{X} \to X$. Il est unique à homéomorphisme près, et s'appelle le* ***revêtement universel*** *de X.*

Exemples.

- On a $\widetilde{\mathbb{S}^1} = \mathbb{R}$.
- On a $\widetilde{\mathbb{T}^2} = \mathbb{R}^2$.
- On a $\widetilde{\mathbb{S}^2} = \mathbb{S}^2$.
- De manière générale, si X est déjà simplement connexe, alors $\tilde{X} = X$.

Définition 1.2.8. *Soit $f : X \to B$ un revêtement. Un* ***automorphisme de revêtement*** *est un homéomorphisme $g : X \to X$ tel que $f = f \circ g$. L'ensemble des automorphismes, muni de la composition, forme un groupe appelé* ***groupe de revêtement****.*

Exemples.

- Considérons le revêtement $t \in \mathbb{R} \to e^{2i\pi t} \in \mathbb{S}^1$. Son groupe de revêtement est isomorphe à $\mathbb{Z}$, engendré par l'homéomorphisme $t \mapsto t+1$ de $\mathbb{R}$.
- Considérons le revêtement $z \in \mathbb{S}^1 \mapsto z^p \in \mathbb{S}^1$, où $p \in \mathbb{Z}^*$. Son groupe de revêtement est isomorphe à $\mathbb{Z}/p\mathbb{Z}$, engendré par l'homéomorphisme $z \mapsto ze^{\frac{2i\pi}{p}}$ de $\mathbb{S}^1$.

Théorème 1.2.9. *Soit X un espace topologique séparé, connexe, localement connexe par arcs et semilocalement simplement connexe. Soit G le groupe de revêtement du revêtement universel $\tilde{X} \to X$. Alors G agit continûment, proprement et librement sur $\tilde{X}$, G est isomorphe au groupe fondamental de X et X est naturellement homéomorphe au quotient $G\backslash\tilde{X}$.*

On a une forme de réciproque du résultat précédent.

Théorème 1.2.10. *Soit X un espace topologique séparé, simplement connexe et localement connexe par arcs, et soit G un groupe discret agissant continûment, librement et proprement sur X. Alors G est isomorphe au groupe fondamental de $G\backslash X$, et X est le revêtement universel de $G\backslash X$.*

1.3 Surfaces

Définition 1.3.1. *Une **variété topologique** de dimension d (resp. orientable) est un espace topologique X spéaré, à base dénombrable, muni d'une famille maximale d'ouverts $\mathcal{U}$ de X recouvrant X, telle que :*

- *Pour tout ouvert $U \in \mathcal{U}$, on se donne un homéomorphisme ϕ_U entre U et un ouvert de $\mathbb{R}^2$.*
- *Pour tous ouverts $U, V \in \mathcal{U}$ tels que $U \cap V \neq \emptyset$, l'application $\phi_V \circ (\phi_U|_{U\cap V})^{-1}$: $\phi_U(U \cap V) \to \phi_V(U \cap V)$ est un homéomorphisme (resp. homéomorphisme préservant l'orientation).*

Définition 1.3.2. *Une **surface** est une variété topologique de dimension* 2.

Remarque. On supposera toujours que les variétés topologiques

Exemples.

- Les variétés topologiques de dimension 1 sont $\mathbb{R}$ et $\mathbb{S}^1$.
- Le plan $\mathbb{R}^2$ est une surface orientable.
- La sphère $\mathbb{S}^2$ est une surface orientable.
- Le tore $\mathbb{T}^2$ est une surface orientable.
- Le plan projectif $\mathbb{RP}^2$ est une surface non orientable.
- La sphère $\mathbb{S}^2 \backslash \{p_1, p_2, p_3\}$ privée de 3 points est une surface orientable.
- De manière générale, tout ouvert d'une surface est encore une surface.

Définition 1.3.3. *Soient S, S' deux surfaces. La **somme connexe** $S\#S'$ est définie de la manière suivante : on considère deux disques ouverts $D \subset S$ et $D' \subset S'$, et on considère le recollement $S\#S'$ de $S\backslash D$ et de $S'\backslash D'$ le long de $\partial D \simeq \partial D'$. A homéomorphisme près, $S\#S'$ ne dépend pas du choix de D et D'.*

Exemples.

- Pour toute surface S, on a $S\#\mathbb{S}^2 \simeq S$.
- La somme connexe $\mathbb{R}^2\#\mathbb{R}^2$ est homéomorphe au cylindre $\mathbb{R}\times\mathbb{S}^1$, ou encore à la sphère $\mathbb{S}^2$ privée de 2 points.
- La surface $\mathbb{T}^2\#\mathbb{T}^2$ "ressemble à une bouée à deux trous". On dit que c'est une surface de genre 2.
- La somme connexe $\mathbb{RP}^2\#\mathbb{RP}^2$ est homéomorphe à la bouteille de Klein.

Théorème 1.3.4 (Classification des surfaces)**.** *Soit S une surface compacte connexe.*

- *Si S est orientable, S est homéomorphe à la somme connexe $S_g = \mathbb{T}^2\#\ldots\#\mathbb{T}^2$ d'un nombre fini $g \geqslant 0$ de tores $\mathbb{T}^2$ (avec la convention $S_0 = \mathbb{S}^2$).*

- *Si S est non-orientable, S est homéomorphe à la somme connexe $\mathbb{RP}^2 \# \dots \# \mathbb{RP}^2$ d'un nombre fini non nul $g \geqslant 1$ de plans projectifs $\mathbb{RP}^2$.*

*L'entier $g \geqslant 0$ s'appelle le **genre** de la surface S.*

Théorème 1.3.5 ("Uniformisation topologique")**.** *Toute surface simplement connexe est homéomorphe soit au plan $\mathbb{R}^2$, soit à la sphère $\mathbb{S}^2$.*

- *Le revêtement universel de la sphère $\mathbb{S}^2$ et du plan projectif $\mathbb{RP}^2$ est homéomorphe à la sphère $\mathbb{S}^2$.*

- *Le revêtement universel de toute autre surface compacte connexe est homéomorphe au plan $\mathbb{R}^2$.*

Corollaire 1.3.6. *Pour tout entier $g \geqslant 1$, le **groupe de surface** $\pi_1(S_g)$ a une action continue, libre et propre sur $\mathbb{R}^2$, dont le quotient est homéomorphe à S_g.*

Exemples.

- Le groupe $\mathbb{Z}^2$ agit par translation sur $\mathbb{R}^2$, et a pour quotient le tore $\mathbb{T}^2$.

- Considérons le groupe K de transformations affines de $\mathbb{R}^2$, engendré par $a : (x, y) \mapsto (x+1, y)$ et $b : (x, y) \mapsto (-x, y+1)$. C'est une action continue, libre et propre sur $\mathbb{R}^2$, dont le quotient est homéomorphe à la bouteille de Klein : son groupe fondamental est isomorphe à K.

- Le groupe fondamental du plan projectif $\mathbb{RP}^2$ est isomorphe à $\mathbb{Z}/2\mathbb{Z}$ (**Exercice**).

Théorème 1.3.7 (Perelman 2003, Conjecture de Poincaré)**.** *Soit X une variété topologique de dimension 3, compacte (sans bord). Si X est simplement connexe, alors X est homéomorphe à la sphère $\mathbb{S}^3$.*

Remarque. Il existe une "classification" des variétés compactes de dimensions 3, c'est la géométrisation de Perelman-Thurston.

Chapitre 2

Constructions de groupes discrets

De bonnes références sont [dlH00], [Löh11], [Bow06] et [Bau93].

On peut distinguer trois grandes méthodes permettant de construire des groupes discrets :

- si X est un espace topologique, on peut considérer son groupe fondamental,
- si X est un espace muni d'une "structure", on peut considérer son groupe de symétries,
- on peut définir un groupe à partir de règles de simplification, c'est ce qu'on appelle une présentation de groupes, que l'on va notamment détailler dans cette partie.

2.1 Groupes de type fini

Définition 2.1.1. *Soit G un groupe et S une partie de G. On dit que G est* ***engendré*** *par S si le plus petit sous-groupe de G contenant S est G. Si G est engendré par une partie finie, on dit que G est* ***de type fini****.*

Exemples.

- Le groupe $\mathbb{Z}$ est engendré par $S = \{1\}$. Il est aussi engendré par $S = \mathbb{N}$, ou bien par $S = \{-2, 17\}$, par exemple. Donc $\mathbb{Z}$ est de type fini.
- Le groupe $\mathbb{Z}^n$ est engendré par $S = \{(1, 0, \ldots, 0), \ldots, (0, \ldots, 0, 1)\}$.
- Le groupe symétrique $\mathfrak{S}_n$ est engendré par une permutation et un n-cycle. Il est aussi engendré par les $n - 1$ transpositions consécutives $(1, 2), (2, 3), \ldots, (n - 1, n)$.
- Le groupe diédral d'ordre $2 \times n$, noté $D_{2\times n}$, est le groupe des symétries d'un n-gone régulier du plan. Il est engendré par une réflexion et une rotation d'angle $\frac{2\pi}{n}$.
- Le groupe $\mathbb{Q}$ n'est pas de type fini (**Exercice**).
- Un groupe non dénombrable n'est pas de type fini (**Exercice**).
- Si X est un ensemble infini, le groupe $\mathfrak{S}_f(X)$ des permutations de X à support fini n'est pas de type fini.

- Soit X une variété topologique compacte, ou bien un CW-complexe fini. Alors le groupe fondamental $\pi_1(X)$ est de type fini. On retrouve l'exemple de $\mathbb{Z}^n$ comme groupe fondamental du tore de dimension n, $(\mathbb{S}^1)^n$.
- Soit X l'espace des anneaux hawaïens : $X = \bigcup_{n \geqslant 1} \mathbb{S}(\frac{1}{n}, \frac{1}{n}) \subset \mathbb{R}^2$. Bien que X soit un espace topologique compact, son groupe fondamental n'est pas de type fini.

Exercice 3. *Soit G un groupe de type fini, et S une partie génératrice infinie de G. Montrer qu'il existe une partie finie de S qui engendre G.*

Exercice 4. *Pour tout entier $n \geqslant 1$, le groupe* $\mathrm{GL}(n, \mathbb{Z})$ *est de type fini, engendré par les matrices :*

$$\begin{pmatrix} 0 & 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ \dots & \dots & \ddots & \dots & \dots & \dots \\ 0 & 0 & 0 & \ddots & 0 & 0 \\ 0 & 0 & 0 & \dots & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & \dots & 0 & 0 \\ 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \ddots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \ddots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix} \textit{ et } \begin{pmatrix} -1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \ddots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix}$$

Définition 2.1.2. *Soient deux groupes G et H. Un* ***isomorphisme*** *entre G et H est un morphisme de groupes $G \to H$ qui est aussi une bijection. Si G et H sont isomorphes, on notera $G \simeq H$ (sil n'y a pas d'ambiguïté). Un isomorphisme entre G et G s'appelle un* ***automorphisme*** *de G. L'ensemble* $\mathrm{Aut}(G)$ *des automorphismes de G, muni de la composition, est un groupe.*

Exemples.

- Le groupe diédral $D_{2\times 3}$ est isomorphe au groupe symétrique $\mathfrak{S}_3$.
- Les groupes $(\mathbb{C}^*, \times)$ et $\mathbb{R} \times \mathbb{S}^1$ sont isomorphes.
- $\mathrm{Aut}(\mathbb{Z}) \simeq \{\pm 1\}$.
- Plus généralement, si $n \geqslant 1$, alors $\mathrm{Aut}(\mathbb{Z}^n) \simeq \mathrm{GL}(n, \mathbb{Z})$.
- $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq \mathbb{Z}/n\mathbb{Z}^*$.

Proposition 2.1.3. *Les groupes $\mathbb{Z}^n$ et $\mathbb{Z}^m$ sont isomorphes si et seulement si $n = m$.*

Démonstration. Le sous-groupe de $\mathbb{Z}^n$ engendré par les carrés de tous les éléments est $(2Z)^n$. C'est un sous-groupe caractéristique (invariant par tous les automorphismes), dont le quotient est $(\mathbb{Z}/2\mathbb{Z})^n$. Si $\mathbb{Z}^n$ et $\mathbb{Z}^m$ sont isomorphes, leurs quotients $(\mathbb{Z}/2\mathbb{Z})^n$ et $(\mathbb{Z}/2\mathbb{Z})^m$ le sont aussi, donc ils ont le même cardinal : $2^n = 2^m$, donc $n = m$. □

2.2 Sous-groupes

Définition 2.2.1. *Soit G un groupe, et H un sous-groupe de G. On dit que H est **d'indice fini** dans G si son indice $|G/H|$ est fini.*

Exemples.

- Pour tout $n \geqslant 1$, $n\mathbb{Z}$ est un (le) sous-groupe d'indice n de $\mathbb{Z}$.
- Pour tout $n \geqslant 2$, $\mathrm{SL}(n, \mathbb{Z})$ est un sous-groupe d'indice 2 de $\mathrm{GL}(n, \mathbb{Z})$ (**Exercice**).

Proposition 2.2.2. *Soit G un groupe, et H un sous-groupe d'indice fini de G. Alors H est de type fini si et seulement G est de type fini.*

Démonstration. Supposons que H est de type fini. Soit S une partie génératrice finie de H, et soit T un ensemble de représentants de $H\backslash G$. Alors $S' = S \cup T$ engendre G : soit $g \in G$, alors il existe $t \in T$ tel que $gt \in H$. Alors il existe $s_1, \ldots, s_n \in S$ tels que $gt = s_1 \ldots s_n$, d'où $g = t^{-1}s_1 \ldots s_n$. Ainsi G est de type fini.

Réciproquement, supposons que G est de type fini. Soit S une partie génératrice finie de G, et notons $\{t_1 = 1, \ldots, t_p\}$ des représentants de $H\backslash G$. Pour tous $s \in S \cup S^{-1}$ et $1 \leqslant j \leqslant p$, il existe donc un (unique) $k = k(s, j)$ tel que $t_j s \in Ht_k$. Soit $S' = \{t_j s t_{k(s,j)}^{-1} \mid s \in S \cup S^{-1}, 1 \leqslant j \leqslant p\}$: c'est une partie finie de H, montrons qu'elle engendre H. Soit $h \in H$: comme S engendre G, on peut écrire $h = s_1 s_2 \ldots s_n$, où $s_i \in S \cup S^{-1}$ pour tout $1 \leqslant i \leqslant n$.

Remarquons qu'on peut écrire $h = s_1 t_{k_1}^{-1} t_{k_1} s_2 t_{k_2}^{-1} t_{k_2} s_3 \ldots s_n t_{k_n}^{-1} t_{k_n}$, où pour tout $1 \leqslant i \leqslant n$, on a $t_{k_{i-1}} s_i t_{k_i}^{-1} \in H$ (avec $t_{k_0} = t_1 = 1$). Comme $h \in H$, on a $t_{k_n} \in H$ donc $t_{k_n} = 1$. Ainsi h est un produit de n éléments de S' : H est de type fini. □

Exemple. Si G est un groupe de type fini et H est un sous-groupe quelconque de G, H n'est pas nécessairement de type fini : soient

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}(2, \mathbb{Q}), a = 2^n, b = \frac{p}{2^q}, \text{ où } n, p, q \in \mathbb{Z} \right\} \text{ et } H = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in G, a = 1 \right\}.$$

Alors G est engendré par les matrices $\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ (**Exercice**). Le sous-groupe H, qui est isomorphe à $\mathbb{Z}[\frac{1}{2}]$, n'est pas de type fini.

Exercice 5. *Soit $G = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathrm{GL}(2, \mathbb{C}) \mid a, d \in \{1, i, -1, -i\} \text{ et } b \in \mathbb{Z}[i] \right\}$. Montrer que G est un groupe, et que G a un sous-groupe d'indice fini isomorphe à $\mathbb{Z}^2$.*

2.3 Opérations élémentaires pour construire de nouveaux groupes

Définition 2.3.1. *Soit $(G_i)_{i \in I}$ une famille de groupes, alors on peut définir :*

- *le **produit direct** $\prod_{i \in I} G_i$, qui n'est autre que le produit cartésien des groupes G_i,*

- *le* ***produit restreint*** $\sum_{i\in I} G_i$*, qui est le sous-groupe du produit direct* $\prod_{i\in I} G_i$ *constitué des élément* $(g_i)_{i\in I}$ *tels que* $g_i = 1$*, sauf pour un nombre fini d'indices* $i \in I$*. Si les groupes* G_i *sont abéliens, on l'appelle plutôt somme directe, et on le note* $\bigoplus_{i\in I} G_i$*.*

Exemple. Le groupe $\prod_{\mathbb{Z}} \mathbb{Z}$ n'est pas dénombrable, tandis que le groupe $\bigoplus_{\mathbb{Z}} \mathbb{Z}$ l'est.

Définition 2.3.2. *Soient* N *et* Q *deux groupes, et* $f : Q \to \mathrm{Aut}(N)$ *un morphisme de groupes. Alors on définit le* ***produit semi-direct*** $N \rtimes_f Q$ *comme le groupe ayant pour ensemble sous-jacent le produit cartésien* $N \times Q$*, muni de la loi de groupes* $(g,h)\cdot(g',h') = (g \cdot f(h)(g'), h \cdot h')$*. Notons que* N *est alors un sous-groupe normal de* $N \rtimes_f Q$*, et que* Q *est un quotient de* $N \rtimes_f Q$*.*

Exemples.

- Si $f : Q \to \mathrm{Aut}(N)$ est le morphisme trivial (constant égal à id_N), alors $Q \rtimes_f N = Q \times N$.
- Le groupe diédral $D_{2\times n}$ est isomorphe au produit semi-direct $\mathbb{Z}/n\mathbb{Z} \rtimes_f \mathbb{Z}/2\mathbb{Z}$, où $f : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ est par exemple donné par $f(1) : k \mapsto -k$.
- Le groupe diédral $D_{2\times n} \simeq \mathbb{Z}/n\mathbb{Z} \rtimes_f \mathbb{Z}/2\mathbb{Z}$ n'est pas isomorphe au produit direct $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (**Exercice**).

Exemple. L'**allumeur de réverbères** est défini par le produit semi-direct du groupe $N = \bigoplus_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$ et du groupe $Q = \mathbb{Z}$, avec le morphisme

$$\begin{array}{rcl} f : \mathbb{Z} & \to & \mathrm{Aut}(\bigoplus_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}) \\ p & \mapsto & ((a_n)_{n\in\mathbb{Z}} \mapsto (a_{n-p})_{n\in\mathbb{Z}})\,. \end{array}$$

Il représente la situation d'un allumeur de réverbères se déplaçant le long d'une droite ($\mathbb{Z}$), pouvant allumer ou éteindre une lampe ($0, 1 \in \mathbb{Z}/2\mathbb{Z}$) à chaque élément de $\mathbb{Z}$. On le note $\mathbb{Z}/2\mathbb{Z} \wr \mathbb{Z}$ (produit en couronne).

Ce groupe $\mathbb{Z}/2\mathbb{Z} \wr \mathbb{Z}$ est engendré par les deux éléments suivants :

$$\begin{aligned} g &= (\delta_0, 0) \text{ (l'allumeur de reverbères allume la lampe à la position 0)} \\ h &= ((0)_{n\in\mathbb{N}}, 1) \text{ (l'allumeur de reverbères se déplace vers la droite de 1)} \end{aligned}$$

Notons que le sous-groupe $N = \bigoplus_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$ n'est pas de type fini.

Définition 2.3.3. *Soit* G *un groupe.*

- *Le* ***sous-groupe dérivé*** *de* G *est le sous-groupe de* G *engendré par les commutateurs* $[g,h] = ghg^{-1}h^{-1}$*, où* $g, h \in G$*, noté* $D(G)$ *ou* $[G,G]$*.*
- *L'****abélianisé*** *de* G *est le groupe quotient* $G/D(G)$*, c'est le plus grand quotient abélien de* G*.*

Exemples.

- Le sous-groupe dérivé de $\mathbb{Z}^n$ est le sous-groupe trivial $\{0\}$, son abélianisé est $\mathbb{Z}^n$.
- Si $n \geqslant 2$, le sous-groupe dérivé de $\mathfrak{S}_n$ est le sous-groupe alterné $\mathfrak{A}_n$, son abélianisé est isomorphe à $\mathbb{Z}/2\mathbb{Z}$.

2.4 Groupes libres

Définition 2.4.1. *Soit F un groupe et S une partie de F. On dit que F est* ***librement engendré*** *par S si pour tout groupe G et pour tout application $\phi : S \to G$, il existe un unique morphisme de groupes $\overline{\phi} : F \to G$ prolongeant ϕ :*

$$\begin{array}{ccc} S & \xrightarrow{\phi} & G \\ \downarrow & \nearrow_{\overline{\phi}} & \\ F & & \end{array}$$

Cette propriété s'appelle la ***propriété universelle****. Si un groupe est librement engendré par une partie, on dit que c'est un* ***groupe libre****.*

Exemples.

- Le groupe $\mathbb{Z}$ est librement engendré par $\{1\}$ (et par $\{-1\}$).
- Le groupe trivial $\{1\}$ est librement engendré par $\emptyset$.
- Les groupes $\mathbb{Z}/n\mathbb{Z}$ (pour $n \geqslant 2$) et $\mathbb{Z}^2$ ne sont pas libres (**Exercice**).

Proposition 2.4.2. *Si un groupe F est librement engendré par une partie S, alors il est engendré par S.*

Démonstration. Notons G le sous-groupe de F engendré par S. Appliquons la propriété universelle à l'inclusion $\phi : S \hookrightarrow G$: elle s'étend en un morphisme $\overline{\phi} : F \to G$. Si l'on compose ce morphisme avec l'inclusion $G \hookrightarrow F$, nous obtenons un morphisme $F \to F$ valant l'identité sur S. Par unicité, ce morphisme est l'identité, donc $G = F$. Ainsi S engendre F. $\square$

Proposition 2.4.3. *Pour tout ensemble S, il existe un groupe F contenant S et librement engendré par S. De plus, il est unique, à isomorphisme unique près. On le note $F(S)$.*

Démonstration. Soit M l'ensemble des mots (suites finies de caractères) sur l'alphabet $A = S \sqcup S^{-1}$. Soit F le sous-ensemble constitué des mots réduits, i.e. tels qu'il n'y ait pas consécutivement une lettre et son inverse. Alors, si on munit F de la loi de composition interne de composition-simplification, F est un groupe.

Il est clair que F est engendré par S, montrons que F vérifie la propriété universelle : soient G un groupe et $\phi : S \to G$ une application. Définissons $\overline{\phi} : F \to G$ par l'application qui au mot $a_1 \dots a_n$ de F associe le produit des éléments $a_1, \dots, a_n$ dans G, noté $\overline{a_1 \dots a_n}^G$. Comme la simplification consécutive d'une lettre et de son inverse est vérifiée dans G, $\overline{\phi}$ est bien un morphisme de groupes. De plus, comme $\overline{\phi}$ doit étendre ϕ et que S est génératrice, $\overline{\phi}$ est unique. Le groupe F est donc librement engendré par S.

Montrons que le groupe F est unique, à isomorphisme unique près : soit F' un groupe librement engendré par S. En appliquant la propriété universelle pour F à l'inclusion $S \subset F'$, on obtient l'existence d'un morphisme $\psi : F \to F'$ égal à l'identité sur S. En appliquant la propriété universelle pour F' à l'inclusion $S \subset F$, on obtient l'existence d'un morphisme $\psi' : F' \to F$ égal à l'identité sur S. En conséquence, le morphisme $\psi' \circ \psi : F \to F$ est égal à l'identité sur S, donc en appliquant l'unicité dans la propriété universelle pour F à l'inclusion $S \subset F$, on en déduit que $\psi' \circ \psi = \mathrm{id}_F$. De même, $\psi \circ \psi' = \mathrm{id}_{F'}$. Ainsi ψ est un isomorphisme entre F et F'. Par unicité de ψ, cet isomorphisme est unique. $\square$

Exemples.

- On peut voir le groupe $\mathbb{Z}$ comme l'ensemble des mots $\{a^n, n \in \mathbb{Z}\}$, muni de la concaténation-simplification.
- Le groupe libre sur $S = \{a, b\}$ est l'ensemble des mots réduits sur $\{a, b, a^{-1}, b^{-1}\}$. Par exemple, les premiers mots de ce groupe sont $\{1, a, a^{-1}, b, b^{-1}, ab, ab^{-1}, a^{-1}b, a^{-1}b^{-1}, \dots\}$.

Exercice 6. *Soit F le groupe librement engendré par $S = \{a, b\}$. Montrer que F est aussi librement engendré par $\{a, ab\}$. En déduire que F est librement engendré par une infinité de parties.*

Exercice 7. *Soit F le groupe librement engendré par $S = \{a, b\}$. Montrer que le groupe $\mathrm{Aut}(F)$ est infini.*

Proposition 2.4.4. *Soit F un groupe libre de type fini. Alors toutes les parties engendrant librement F ont le même cardinal, appelé le **rang** de F.*

Démonstration. Supposons que F soit librement engendré par une partie S de cardinal r. Nous allons montrer que F a exactement $2^r - 1$ sous-groupes d'indice 2.

Si $\phi : S \to \mathbb{Z}/2\mathbb{Z}$ est une application quelconque, d'après la propriété universelle elle s'étend en un morphisme de groupes $\overline{\phi} : F \to \mathbb{Z}/2\mathbb{Z}$. Le noyau de ce morphisme est soit un sous-groupe d'indice 2, soit F lui-même (si $\overline{\phi}$ est le morphisme trivial). De plus, si $\phi, \phi' : S \to \mathbb{Z}/2\mathbb{Z}$ sont deux applications distinctes, leurs noyaux sont différents. Ainsi F a au moins $2^r - 1$ sous-groupes d'indice 2.

Réciproquement, si H est un sous-groupe de F d'indice 2, alors l'action de F sur F/H par multiplication à gauche induit un morphisme non trivial ψ de F dans $\mathfrak{S}(F/H) \simeq \mathfrak{S}_2 \simeq \mathbb{Z}/2\mathbb{Z}$, tel que $H = \ker \psi$. Notons ϕ la restriction de ψ à S : par unicité dans la propriété universelle, nous avons $\psi = \overline{\phi}$. Ainsi F a exactement $2^r - 1$ sous-groupes d'indice 2. $\square$

Proposition 2.4.5. *Pour tout rang $r \in \mathbb{N}$, il existe un unique (à isomorphisme près) groupe de libre de rang r, noté $\mathbb{F}_r$.*

Démonstration. C'est une conséquence des résultats précédents et de l'unicité dans la propriété universelle. $\square$

Remarque. Le groupe libre $\mathbb{F}_r$ est aussi le groupe fondamental d'un bouquet de r cercles $\displaystyle\bigvee_{i=1}^{r} \mathbb{S}^1$.

Théorème 2.4.6 (Forme normale). *Soit $r \geqslant 1$, et $\mathbb{F}_r$ le groupe librement engendré par $a_1, \dots, a_r$. Tout élément de $\mathbb{F}_r$ s'écrit, de manière unique, comme un mot $a_{n_1}^{p_1} \dots a_{n_\ell}^{p_\ell}$, où $\ell \in \mathbb{N}$, pour tout $1 \leqslant i \leqslant \ell$, $1 \leqslant n_i \leqslant r$ et $p_i \in \mathbb{Z} \backslash \{0\}$, et si a_{n_i} et $a_{n_{i+1}}$ sont deux lettres consécutives, on a $n_i \neq n_{i+1}$.*

Remarque. Si G est un groupe engendré par r éléments, c'est un quotient de $\mathbb{F}_r$.

Proposition 2.4.7. *L'abélianisé de $\mathbb{F}_r$ est isomorphe à $\mathbb{Z}^r$.*

Démonstration. Notons $S = \{s_1, \dots, s_r\}$ une partie de $\mathbb{F}_r$ engendrant librement $\mathbb{F}_r$. Pour tout $1 \leqslant i \leqslant r$, notons $\phi_i : \mathbb{F}_r \to \mathbb{Z}$ le morphisme associé à l'application $\delta_{s_i} : S \to \mathbb{Z}/2\mathbb{Z}$. C'est le morphisme qui à un mot sur l'alphabet $S \cup S^{-1}$ associe le nombre d'occurences de $s_i^{\pm 1}$, comptées avec le signe.

Considérons le morphisme produit $\phi = \prod_{i=1}^{r} \phi_i : \mathbb{F}_r \to \mathbb{Z}^r$. Comme tout commutateur $[g,h] = ghg^{-1}h^{-1}$ a autant d'occurences d'une lettre que de son inverse, on en déduit que $D(\mathbb{F}_r) \subset \ker \phi$. Nous allons montrer l'inclusion réciproque.

Soit $g \in \ker \phi$, et voyons-le comme un mot sur l'alphabet $S \cup S^{-1}$. Supposons pour simplifier que la première lettre de g soit s_1. Comme le nombre total d'occurences de $s_1^{\pm 1}$ est 0, quelque part dans le mot g se trouve s_1^{-1} : écrivons $g = s_1 h s_1^{-1} k$, où $h, k \in \mathbb{F}_r$. Alors $g = s_1 h s_1^{-1} h^{-1} h k = [s_1, h] h k$. Comme $[s_1, h] \in D(\mathbb{F}_r)$ et que la longueur de hk est plus courte que celle de g, par récurrence on montre que g est un produit de commutateurs, donc $g \in D(\mathbb{F}_r)$.

En conclusion $D(\mathbb{F}_r) = \ker \phi$, donc l'abélianisé de $\mathbb{F}_r$ est isomorphe à $\mathbb{Z}^r$. □

Exercice 8. *Donner un autre preuve du fait que si $\mathbb{F}_n$ est isomorphe à $\mathbb{F}_m$, alors $m = n$, en considérant les abélianisés.*

2.5 Présentation des groupes

Définition 2.5.1. *Soit F un groupe et R une partie de F, on note $\langle\langle R \rangle\rangle$ le plus petit sous-groupe normal de F contenant R.*

Définition 2.5.2. *Soit $\mathbb{F}(S)$ le groupe libre sur un ensemble S (ensemble de* ***générateurs****), et R un sous-ensemble de $\mathbb{F}(S)$ (ensemble de* ***relations****). On définit le groupe*

$$\langle S \mid R \rangle = \mathbb{F}(S)/\langle\langle R \rangle\rangle.$$

C'est le "plus grand groupe" engendré par S dans lequel les relations R sont vérifiées (i.e. les mots de R deviennent triviaux lorsqu'ils sont évalués dans ce groupe).

Une ***présentation*** *d'un groupe G est un isomorphisme entre G et un groupe $\langle S \mid R \rangle$. On dit qu'un groupe G est de* ***présentation finie*** *s'il existe un ensemble S fini et un sous-ensemble fini R de $\mathbb{F}(S)$ tels que G soit isomorphe à $\langle S \mid R \rangle$.*

Remarque. On notera parfois une relation $g = h$ au lieu de gh^{-1}, pour simplifier les notations.

Exemples.

- Le groupe $\mathbb{Z}$ de présentation finie : par exemple, $\langle a \mid \rangle$ est une présentation de $\mathbb{Z}$. De même, $\langle a, b \mid ab^{-1} \rangle$ ou $\langle a, b \mid a^n b^{-n}, n \in \mathbb{Z} \rangle$ sont aussi des présentations du groupe $\mathbb{Z}$.
- Une présentation du groupe trivial est $\langle \mid \rangle$, ou bien $\langle a \mid a \rangle$, par exemple.
- Le groupe libre $\mathbb{F}_r$ a pour présentation $\langle s_1, \dots, s_r \mid \rangle$, d'où son nom de groupe libre : il n'a aucune relation.

- Le groupe $\mathbb{Z}^2$ a pour présentation $\langle a, b \mid ab = ba\rangle$.
- Le groupe $\mathbb{Z}/n\mathbb{Z}$ a pour présentation $\langle a \mid a^n\rangle$.
- Le groupe diédral $D_{2\times n}$ a pour présentation $\langle a, b \mid a^n, b^2, bab^{-1} = a^{-1}\rangle$.
- Le groupe symétrique $\mathfrak{S}_n$ a pour présentation $\langle s_1, \dots, s_{n-1} \mid s_1^2 = s_2^2 = \dots = s_{n-1}^2 = 1, \forall 1 \leqslant i, j \leqslant n-1, s_i s_j = s_j s_i$ si $|i-j| \geqslant 2,$ et $s_i s_j s_i = s_j s_i s_j$ si $|i-j| = 1\rangle$, où s_i correspond à la transposition $(i, i+1)$.
- Le groupe de Klein K de transformations affines de $\mathbb{R}^2$, engendré par $a : (x, y) \mapsto (x+1, y)$ et $b : (x, y) \mapsto (-x, y+1)$, a pour présentation $K = \langle a, b \mid bab^{-1} = a^{-1}\rangle$.
- Il peut être difficile de déterminer quel groupe une présentation peut donner : par exemple, le groupe $\langle a, b, c \mid a^2b, b^2c, ca^{-3}\rangle$ est le groupe trivial (**Exercice**).
- Montrer que le groupe $\langle a, b, c \mid aabaa = cbacc, abc = bab, ccac = baba\rangle$ est infini. On pourra montrer qu'il a un quotient isomorphe à $\mathbb{Z}$ (**Exercice**).
- Soit X une variété topologique compacte, ou bien un CW-complexe fini. Alors le groupe fondamental $\pi_1(X)$ est de présentation finie. On retrouve l'exemple de $\mathbb{Z}^n$ comme groupe fondamental du tore de dimension n, $(\mathbb{S}^1)^n$.

Remarque. Tout groupe a une présentation (infinie en général) : si G est un groupe, alors G est une partie génératrice de G, notons R le sous-groupe normal de $\mathbb{F}(G)$ tel que G soit isomorphe à $\mathbb{F}(G)/R$. Alors G a pour présentation $\langle G \mid R\rangle$.

Proposition 2.5.3. *Le groupe G de présentation $\langle S \mid R\rangle$ vérifie la propriété universelle suivante : pour tout groupe H, et pour toute application $\phi : S \to H$ telle que, pour tout mot $s_1 \dots s_n$ de R, on ait $\phi(s_1)\dots\phi(s_n) = 1 \in H$, il existe un unique morphisme $\overline{\phi} : G \to H$ étendant ϕ.*

Démonstration. D'après la propriété universelle pour le groupe libre $F(S)$, il existe un unique morphisme $\psi : F(S) \to H$ étendant ϕ. D'après la condition sur ϕ, pour tout $g \in R \subset F(S)$, on a $\psi(g) = 1$. Par conséquent, l'application ψ passe au quotient en un morphisme de groupes $\overline{\phi} : G \to H$ étendant ϕ. Par unicité de ψ, $\overline{\phi}$ est unique. □

Théorème 2.5.4 (Neumann)**.** *Il y a une infinité non dénombrable de groupes engendrés par 2 éléments deux à deux non isomorphes.*

Proposition 2.5.5. *Le groupe libre $\mathbb{F}_2$ a une infinité non dénombrable de sous-groupes normaux.*

Démonstration. Notons $S = (s_i)_{i\in\mathbb{Z}}$ un ensemble de générateurs indexé par $\mathbb{Z}$, et considérons les relations

$$R = \{[[s_i, s_j], s_k] = 1\}_{i,j,k\in\mathbb{Z}} \bigcup \{[s_i, s_j] = [s_{i+k}, s_{j+k}]\}_{i,j,k\in\mathbb{Z}}.$$

Notons G_0 le groupe de présentation (infinie) $\langle S \mid R\rangle$.

Etape 1 Le sous-groupe dérivé $D(G_0)$ est le groupe abélien libre engendré par les $u_i = [s_0, s_i]$, pour $i \in \mathbb{Z}$.

Tout d'abord, chaque u_i est un commutateur, donc appartient bien à $D(G_0)$. De plus, $D(G_0)$ est aussi engendré par les commutateurs des éléments de S (car $[g, hk] = [g,h]h[g,k]h^{-1}$). Ainsi, d'après les relations R, tout commutateur d'éléments de S est égal à l'un des u_i. Par ailleurs, d'après les relations R, les u_i commutent deux à deux. Ainsi $D(G_0)$ est le groupe abélien libre engendré par les u_i, pour $i \in \mathbb{Z}$.

Etape 2 Notons $\phi : G_0 \to G_0$ l'automorphisme de G_0 qui à s_i associe s_{i+1}, pour tout $i \in \mathbb{Z}$. On peut alors définir le produit semi-direct $G = G_0 \times_\phi \mathbb{Z}$ (où on considère le morphisme $\mathbb{Z} \to \mathrm{Aut}(G_0)$ qui à $1 \in \mathbb{Z}$ associe ϕ). Alors $D(G_0)$ est inclus dans le centre de G.

Pour tout $g \in D(G_0)$, on a $\phi(g) = g$. En effet, d'après les relations R, on a $\phi(u_i) = [\phi(s_0), \phi(s_i)] = [s_1, s_{i+1}] = [s_0, s_i] = u_i$.

Etape 3 Pour toute partie X de $\mathbb{Z}$, notons N_X le sous-groupe de $D(G_0)$ engendré par $\{u_x, x \in X\}$. Comme $D(G_0)$ est inclus dans le centre de G, N_X est un sous-groupe normal de G. Ainsi G contient une infinité non dénombrable de sous-groupes normaux.

Etape 4 Notons $t \in \mathbb{Z} \subset G$ un générateur, alors le groupe G est engendré par s_0 et t. Ainsi G est un quotient de $\mathbb{F}_2$. Par conséquent, tout sous-groupe normal de G définit un unique sous-groupe normal de $\mathbb{F}_2$. Il y en a donc une infinité non dénombrable. □

Proposition 2.5.6. *Soit G un groupe de type fini ayant une infinité non dénombrable de sous-groupes normaux. Alors G a une infinité non dénombrable de quotients deux à deux non isomorphes.*

Démonstration. Par l'absurde, supposons que G n'a qu'une quantité dénombrable de quotients deux à deux non isomorphes. Alors il existe un quotient Q de G tel qu'il existe une infinité non dénombrable $\mathcal{N}$ de sous-groupes normaux de G tel que, pour tout $N \in \mathcal{N}$, le quotient G/N soit isomorphe à Q. Cela fournit une infinité non dénombrable de morphismes de G dans Q, deux à deux distincts. Ceci est impossible, car G est de type fini et Q est dénombrable. □

Démonstration. [Preuve du théorème de Neumann] Comme le groupe libre $\mathbb{F}_2$ a une infinité non dénombrable de sous-groupes normaux, d'après la proposition précédente le groupe libre $\mathbb{F}_2$ a une infinité non dénombrable de quotients deux à deux non isomorphes. Chaque quotient de $\mathbb{F}_2$ est un groupe engendré par 2 éléments. □

Corollaire 2.5.7. *Il existe une infinité non dénombrable de groupes de type fini, mais pas de présentation finie.*

Démonstration. Il existe une quantité dénombrable de présentations finies. □

Exemple. Le groupe de l'allumeur de réverbères $\mathbb{Z}/2\mathbb{Z} \wr \mathbb{Z}$ est de type fini, mais pas de présentation finie (admis). Une présentation (infinie) du groupe $\mathbb{Z}/2\mathbb{Z} \wr \mathbb{Z}$ est $\langle a, b \mid a^2 = 1, \forall n \in \mathbb{Z}, [b^n a b^{-n}, a] = 1 \rangle$.

2.6 Produits libres

Proposition 2.6.1. *Soit $(G_i)_{i\in I}$ une famille de groupes. Le* ***produit libre*** *des groupes $(G_i)_{i\in I}$ est le groupe G contenant chacun des groupes $(G_i)_{i\in I}$ et satisfaisant la propriété universelle suivante : pour tout groupe H, et pour tous morphismes de groupes $\phi_i : G_i \to H$, il existe un unique morphisme de groupes $G \to H$ étendant chacun des morphismes ϕ_i. Le groupe G est unique, à isomorphisme unique près, on le note $G = \star_{i\in I} G_i$.*

Démonstration. Considérons, pour chaque $i \in I$, une présentation (éventuellement infinie) $\langle S_i \mid R_i \rangle$ du groupe G_i. Alors le groupe $G = \langle \bigcup_{i\in I} S_i \mid \bigcup_{i\in I} R_i \rangle$ vérifie la propriété universelle : c'est une conséquence immédiate de la propriété universelle pour une présentation de groupes. $\square$

Théorème 2.6.2 (Forme normale)**.** *Tout élément de $\star_{i\in I} G_i$ s'écrit, de manière unique, comme un mot $g_1 \dots g_n$, où $n \in \mathbb{N}$, où chaque g_k appartient à l'un des $G_i \backslash \{e\}$, et où deux éléments consécutifs g_k et g_{k+1} n'appartiennent pas au même G_i.*

Démonstration. L'existence est claire, car $G = \star_{i\in I} G_i$ est engendré par $\cup_{i\in I} G_i$.

Pour l'unicité, considérons l'ensemble W des mots réduits, i.e. des mots $(g_1, \dots, g_n)$, où $n \in \mathbb{N}$, où chaque g_k appartient à l'un des $G_i \backslash \{e\}$, et où deux éléments consécutifs g_k et g_{k+1} n'appartiennent pas au même G_i.

Alors, pour tout $i \in I$ notons $\phi_i : G_i \to \mathfrak{S}(W)$ le morphisme qui à $g \in G_i$ et $(g_1, \dots, g_n) \in W$ associe :

- $(g, g_1, \dots, g_n)$ si $g \neq 1$ et $g_1 \notin G_i$,
- $(gg_1, g_2, \dots, g_n)$ si $g_1 \in G_i$ et $gg_1 \neq 1$ et
- $(g_2, \dots, g_n)$ si $gg_1 = 1$.

D'après la propriété universelle, il existe un unique morphisme de groupes $G \to \mathfrak{S}(W)$ prolongeant chaque ϕ_i. Alors, si $g \in G$, nous avons $\phi(g)(\varepsilon) \in W$ est l'unique mot réduit représentant g. $\square$

Exemples.

- Le groupe libre $\mathbb{F}_r$ est le produit libre de r copies de $\mathbb{Z}$.
- Le produit libre $\mathbb{Z}/2\mathbb{Z} \star \mathbb{Z}/2\mathbb{Z}$ est isomorphe au groupe diédral infini $D_\infty = \simeq \mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$: notons a et b les générateurs des deux copies de $\mathbb{Z}/2\mathbb{Z}$. Alors $\mathbb{Z}/2\mathbb{Z} \star \mathbb{Z}/2\mathbb{Z}$ est l'ensemble des mots en $a = a^{-1}$ et $b = b^{-1}$, qui alternent toujours entre a et b. Ainsi l'application suivante définit un isomorphisme :

$$\begin{array}{rcl} \varphi : \mathbb{Z}/2\mathbb{Z} \star \mathbb{Z}/2\mathbb{Z} & \to & \mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} \\ a & \mapsto & (1,1) \\ b & \mapsto & (0,1) \end{array}$$

  On a alors $\varphi(ab) = (1,0)$, $\varphi(aba) = (2,1)$, $\varphi(ba) = (-1,0)$, et de manière générale, pour tout $n \in \mathbb{Z}$, $\varphi((ab)^b) = (n,0)$.

- Le groupe $\mathbb{Z}/2\mathbb{Z} \star \mathbb{Z}/3\mathbb{Z}$ est isomorphe à $\mathrm{PSL}(2,\mathbb{Z})$ (admis pour l'instant). Il est aussi étroitement relié au groupe de tresses à 3 brins.

Exercice 9. *Soient A et B deux groupes non triviaux. Montrer que $A \star B$ contient un élément d'ordre infini, et que $A \star B$ est de centre fini.*

Exercice 10. *Soient A, B deux groupes, et soit $N = \langle\langle A \rangle\rangle$ le sous-groupe normal de $G = A \star B$ engendré par A. Montrer que $G/N \simeq B$.*

Exercice 11. *Soient A et B deux groupes abéliens. Montrer que l'abélianisé de $A \star B$ est isomorphe à $A \times B$.*

Exercice 12. *Soient $n, m \geqslant 1$, et soit $G_{n,m} = \mathbb{Z}/n\mathbb{Z} \star \mathbb{Z}/m\mathbb{Z}$. Montrer que $G_{n,m}$ est isomorphe à $G_{n',m'}$ si et seulement si $\{n, m\} = \{n', m'\}$.*

Proposition 2.6.3 (Cas particulier de Van Kampen)**.** *Soient une famille $(X_i, x_i)_{i \in I}$ d'espaces topologiques pointés. Alors le bouquet $(X, x) = \bigvee_{i \in I} (X_i, x_i)$ a pour groupe fondamental le produit libre $\pi_1(X, x) \simeq \star_{i \in I} \pi_1(X_i, x_i)$.*

Exemples.

- On retrouve ainsi que le groupe fondamental du bouquet de r cercles est le groupe libre de rang r.
- Le bouquet de deux tores a pour groupe fondamental $\mathbb{Z}^2 \star \mathbb{Z}^2$.

2.7 Produit amalgamé

Proposition 2.7.1. *Soient A, B et C trois groupes, et deux morphismes $\alpha : C \to A$ et $\beta : C \to B$. Le* ***produit amalgamé*** *de A et B au-dessus de C est le groupe G, avec des morphismes naturels de A et B vers G, satisfaisant la propriété universelle suivante : pour tout groupe H, et pour tous morphismes de groupes $\phi_A : A \to H$ et $\phi_B : B \to H$ tels que $\phi_A \circ \alpha = \phi_B \circ \beta : C \to H$, il existe un unique morphisme de groupes $G \to H$ étendant ϕ_A et ϕ_B. Le groupe G est unique, à isomorphisme unique près, on le note $G = A \star_C B$.*

Démonstration. Considérons des présentations $\langle S_A \mid R_A \rangle$ de A et $\langle S_B \mid R_B \rangle$ de B. Notons $R = R_A \cup R_B \cup \{\alpha(c) = \beta(c), c \in C\}$. Alors le groupe $G = \langle S_A \cup S_B \mid R \rangle$ vérifie la propriété universelle.

Soient H, $\phi_A : A \to H$ et $\phi_B : B \to H$ tels que $\phi_A \circ \alpha = \phi_B \circ \beta : C \to H$. Considérons l'application $\phi = \phi_A \cup \phi_B : S = S_A \cup S_B \to H$. Pour tout mot g de R_A, comme ϕ_A est un morphisme de groupes, on a $\phi(g) = 1$. De même, pour tout mot g de R_B, comme ϕ_B est un morphisme de groupes, on a $\phi(g) = 1$. Enfin, pour tout mot $g = \alpha(c)\beta(c)^{-1} \in R$, où $c \in C$, on a $\phi(g) = \phi_A(\alpha(c))\phi_B(\beta(c)^{-1}) = 1$ par hypothèse. Ainsi d'après la propriété universelle pour la présentation de G, il existe un unique morphisme $\overline{\phi} : G \to H$ étendant ϕ. En particulier, ce morphisme étend les morphismes ϕ_A et ϕ_B. □

Théorème 2.7.2 (Forme normale)**.** *Soient A, B et C trois groupes, et deux morphismes $\alpha : C \to A$ et $\beta : C \to B$. Soit A' (resp. B') un ensemble de représentants de $C \backslash A$ (resp. $C \backslash B$). Tout élément du produit amalgamé $A \star_C B$ s'écrit, de manière unique :*

$$cg_1 g_2 \cdots g_n,$$

où $c \in C$, $n \in \mathbb{N}$ et $g_i \in A' \cup B' \backslash C$, tels que deux éléments consécutifs g_i et g_{i+1} n'appartiennent pas au même ensemble A' ni B'.

Exemples.

- Le "groupe du trèfle" $G_\clubsuit = \langle a, b \mid aba = bab \rangle$ est isomorphe au produit de deux copies de $\mathbb{Z}$, amalgamées au-dessus des sous-groupes $2\mathbb{Z}$ et $3\mathbb{Z}$ respectivement (**Exercice**). Autrement dit, $G_\clubsuit \simeq \langle x, y \mid x^2 = y^3 \rangle$. C'est aussi le groupe fondamental du complémentaire du noeud de trèfle dans $\mathbb{R}^3$, d'où son nom.

- Le groupe $\mathrm{SL}(2,\mathbb{Z})$ est isomorphe au produit amalgamé $\mathbb{Z}/6\mathbb{Z} \star_{\mathbb{Z}/2\mathbb{Z}} \mathbb{Z}/4\mathbb{Z}$ (voir plus loin).
- (Admis) Si $\mathbb{K}$ est un corps commutatif, on a $\mathrm{GL}(2,\mathbb{K}[X]) \simeq \mathrm{GL}(2,\mathbb{K}) \star_{B(\mathbb{K})} B(\mathbb{K}[X])$, où $B \subset \mathrm{GL}(2)$ désigne le sous-groupe triangulaire supérieur.
- (Admis) Si p est un nombre premier, alors $\mathrm{SL}(2,\mathbb{Z}[\frac{1}{p}]) \simeq \mathrm{SL}(2,\mathbb{Z}) \star_C \mathrm{SL}(2,\mathbb{Z})$, où $C = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}) \mid c \equiv 0[p]\}$.

Exercice 13. *Soient A, B, C trois groupes, et $\alpha : C \to A$, $\beta : C \to B$ deux morphismes.*

- *Si $C = \{1\}$, montrer que $A \star_C B \simeq A \star B$.*
- *Si $B = \{1\}$, montrer que $A \star_C B \simeq A/\langle\langle \alpha(C) \rangle\rangle$.*
- *Si $\beta : C \to B$ est un isomorphisme, montrer que $A \star_C B \simeq A$.*
- *Si A, B et C sont finis, et que $[A : \alpha(C)] = [B : \beta(C)] = 2$, montrer que $A \star_C B$ a un sous-groupe d'indice fini isomorphe à $\mathbb{Z}$.*

Théorème 2.7.3 (Van Kampen, admis)**.** *Soit X un espace topologique, qui soit la réunion de deux ouverts connexes par arcs A et B, chacun contenant le point base $x_0 \in X$, tels que l'intersection $C = A \cap B$ soit connexe par arcs. Alors le groupe fondamental $\pi_1(X, x_0)$ est naturellement isomorphe au produit amalgamé de $\pi_1(A, x_0)$ et de $\pi_1(B, x_0)$ au-dessus de $\pi_1(C, x_0)$.*

Corollaire 2.7.4. *Le groupe fondamental d'une surface orientable compacte de genre $g \geqslant 1$ sans bord a pour présentation*

$$\langle a_1, b_1 a_2, b_2, \ldots, a_g, b_g \mid [a_1, b_1][a_2, b_2] \ldots [a_g, b_g] = 1 \rangle.$$

Le groupe fondamental d'une surface compacte orientable de genre $g \geqslant 0$ avec $p \geqslant 1$ composantes de bord est libre de rang $2g - 1 + p$.

Corollaire 2.7.5. *Le groupe fondamental d'une surface non-orientable compacte de genre $g \geqslant 1$ sans bord a pour présentation*

$$\langle a_1, \ldots, a_g \mid a_1^2 a_2^2 \ldots a_g^2 = 1 \rangle.$$

Le groupe fondamental d'une surface compacte non orientable de genre $g \geqslant 1$ avec $p \geqslant 1$ composantes de bord est libre de rang $g + p - 1$.

2.8 Extension HNN

Théorème 2.8.1 (Higman-Neumann-Neumann)**.** *Soient G un groupe, $A, B \subset G$ deux sous-groupes de G et $\alpha : A \to B$ un isomorphisme de groupes. Il existe un unique groupe G_0, avec des morphismes naturels de G et $\mathbb{Z}$ vers G_0, vérifiant la propriété universelle suivante. Pour tout groupe H, et pour tous morphismes $\phi_G : G \to H$ et $\phi_{\mathbb{Z}} : \mathbb{Z} \to H$ tels que $\forall a \in A, \phi_{\mathbb{Z}}(1)\phi_G(a)\phi_Z(1)^{-1} = \phi_G(\alpha(a))$, il existe un unique morphisme $\phi : G_0 \to H$ étendant ϕ_G et $\phi_{\mathbb{Z}}$. On l'appelle **extension HNN** de G par α, et on le note $G\star_\alpha$ ou $G\star_A$.*

Démonstration. Il suffit de considérer le quotient G_0 du produit libre $G \star \mathbb{Z}$ par le sous-groupe normal engendré par les $tat^{-1}\alpha(a)^{-1}$, où $a \in A$ et t désigne un générateur fixé de $\mathbb{Z}$. □

Théorème 2.8.2 (Forme normale, Lemme de Britton)**.** *Soient G un groupe, $A, B \subset G$ deux sous-groupes de G et $\alpha : A \to B$ un isomorphisme de groupes. Tout écriture dans l'extension HNN $G\star_\alpha$ de l'élément neutre sous la forme :*

$$1 = g_0 t^{\varepsilon_1} g_1 t^{\varepsilon_2} \dots t^{\varepsilon_n} g_n,$$

où $n \in \mathbb{N}$, $g_i \in A \cup B$ et $\varepsilon_i = \pm 1$, est telle que le produit comporte au moins une expression de la forme tat^{-1}, avec $a \in A$, ou $t^{-1}bt$, avec $b \in B$.

Théorème 2.8.3. *Soit X un espace topologique connexe par arcs, soit $Y \subset X$ un ouvert connexe par arcs, et soit $x_0 \in Y$ un point base. Fixons un homéomorphisme $\varphi : Y \to Y$. Considérons l'espace topologique $Z = (X \sqcup Y \times [0,1]) \,/\, \sim$, où $\forall y \in Y, y \sim (y, 0)$ et $\varphi(y) \sim (y, 1)$. Alors $\pi_1(Z, x_0) \simeq \pi_1(X, x_0)\star_{\pi_1(Y,x_0)}$.*

Exemples.

- Si $\alpha = \mathrm{id}_G$, on a $G\star_A \simeq G \times \mathbb{Z}$ (**Exercice**).
- Si α est un automorphisme de G, on a $G\star_\alpha \simeq G \rtimes_\alpha \mathbb{Z}$ (**Exercice**).
- On retrouve que le groupe fondamental du tore $\mathbb{T}^2$ est $\mathbb{Z}\star_\mathbb{Z} = \langle a, t \mid tat^{-1} = a \rangle \simeq \mathbb{Z}^2$.
- On retrouve que le groupe fondamental de la bouteille de Klein est $\mathbb{Z}\star_{-1} = \langle a, t \mid tat^{-1} = a^{-1} \rangle$.

Théorème 2.8.4 (Higman)**.** *Le groupe de présentation*

$$H = \langle x_1, x_2, x_3, x_4 \mid x_2 x_1 x_2^{-1} = x_1^2, x_3 x_2 x_3^{-1} = x_2^2, x_4 x_3 x_4^{-1} = x_3^2, x_1 x_4 x_1^{-1} = x_4^2 \rangle$$

est infini, et son seul sous-groupe d'indice fini est H.

Démonstration. Montrons tout d'abord que le seul sous-groupe d'indice fini de H est H : supposons par l'absurde que H ait un sous-groupe d'indice fini non trivial. Quitte à considérer l'intersection de ses conjugués, on peut supposer que H ait un sous-groupe d'indice fini distingué non trivial, donc que H ait un quotient fini $\overline{H}$ non trivial. Notons $n_1, \dots, n_4 \in \mathbb{N}$ les ordres de $\overline{x_1}, \dots, \overline{x_4}$ dans $\overline{H}$: comme $\overline{H} \neq \{1\}$, ils ne sont pas tous égaux à 1. Soit $p \geqslant 2$ le plus petit nombre premier divisant l'un des n_i, supposons que p divise n_1.

Alors $\overline{x_1} = \overline{x_2}^{n_2} \overline{x_1} \overline{x_2}^{-n_2} = \overline{x_1}^{2^{n_2}}$, d'où $2^{n_2} \equiv 1[n_1]$, donc $2^{n_2} \equiv 1[p]$. Notons que $p > 2$, ainsi notons N l'ordre de 2 dans $(\mathbb{Z}/p\mathbb{Z})^*$: on a $2 \leqslant N \leqslant p - 1$. Comme $2^{n_2} \equiv 1[p]$, on sait que N divise n_2, donc si q désigne un facteur premier de N, c'est un facteur premier de n_2 qui est plus petit que p : contradiction.

Montrons ensuite que H est infini. Notons $H_{12} = \langle x_1, x_2 \mid x_2 x_1 x_2^{-1} = x_1^2 \rangle$, c'est l'extension HNN de $\mathbb{Z}$ par l'isomorphisme $\alpha : n \mapsto 2n$ entre les sous-groupes $\mathbb{Z}$ et $2\mathbb{Z}$. Notons que H est aussi isomorphe au produit semi-direct $\mathbb{Z}[\frac{1}{2}] \rtimes \mathbb{Z}$, où $\mathbb{Z}$ agit sur $\mathbb{Z}[\frac{1}{2}]$ par $n \mapsto 2n$. Notons que les sous-groupes $H_1 = \langle x_1 \rangle$ et $H_2 = \langle x_2 \rangle$ de H_{12} sont isomorphes à $\mathbb{Z}$.

Maintenant, le groupe $H_{123} = \langle x_1, x_2, x_3 \mid x_2x_1x_2^{-1} = x_1^2, x_3x_2x_3^{-1} = x_2^2\rangle$ est l'amalgame de H_{12} et de H_{23} au-dessus du sous-groupe $H_2 = \langle x_2\rangle$. Notons que le sous-groupe $H_{13} = \langle x_1, x_3 \mid\rangle$ de H_{123} est librement engendré par $\{x_1, x_3\}$. De même, le groupe $H_{341} = \langle x_1, x_3, x_4 \mid x_4x_3x_4^{-1} = x_3^2, x_1x_4x_1^{-1} = x_4^2\rangle$ est l'amalgame de H_{34} et de H_{41} au-dessus du sous-groupe $H_4 = \langle x_4\rangle$. Et H_{341} contient le sous-groupe libre H_{13}.

Enfin, H est l'amalgame des sous-groupes H_{123} et H_{341} au-dessus du sous-groupe H_{13}. En particulier, H contient le sous-groupe $H_{13} \simeq \mathbb{F}_2$ et est donc infini. $\square$

Corollaire 2.8.5. *Il existe un groupe simple infini de type fini.*

Démonstration. Considérons l'ensemble $\mathcal{N}$ des sous-groupes normaux de H distincts de H. Soit $(N_i)_{i\in I}$ une chaîne de $\mathcal{N}$, et posons $N = \cup_{i\in I} N_i$: c'est un sous-groupe normal de H, montrons que $N \neq H$. Si on avait $N = H$, comme H est de type fini, il existerait $i \in I$ tel que les 4 générateurs de H appartiennent à N_i, et donc $N_i = H$, ce qui contredit $N_i \in \mathcal{N}$.

D'après le lemme de Zorn, il existe donc un élément maximal $N \in \mathcal{N}$. Ce sous-groupe normal est tel que le quotient H/N est infini, d'après le théorème 2.8.4. De plus, si N' était un sous-groupe distingué non trivial de H/N, ce serait un sous-groupe distingué de H contenant N et distinct de N et de H, ce qui contredirait la maximalité de N. Ainsi H/N est un groupe simple. $\square$

2.9 Variétés de dimension 4

Théorème 2.9.1. *Soit G un groupe de présentation finie. Alors il existe une variété topologique compacte sans bord orientable, dont le groupe fondamental soit isomorphe à G.*

Démonstration. Notons $G = \langle s_1, \ldots, s_n \mid r_1, \ldots, r_m\rangle$ une présentation finie de G, et effectuons une récurrence sur le nombre $m \geqslant 0$ de relations.

Si $m = 0$, alors $G = \mathbb{F}_n$ est le groupe libre de rang n, c'est le groupe fondamental de la somme connexe de n copies de $\mathbb{S}^1 \times \mathbb{S}^3$, qui est une variété de dimension 4, compacte sans bord.

Supposons que le groupe $G_0 = \langle s_1, \ldots, s_n \mid r_1, \ldots, r_{m-1}\rangle$ soit isomorphe au groupe fondamental d'une variété M_0 de dimension 4 compacte sans bord. Alors la relation r_m définit un lacet $\ell \subset M_0$, que l'on peut supposer simple car M_0 est de dimension au moins 3. Considérons un voisinage tubulaire $V \simeq \mathbb{S}^1 \times \mathbb{B}^3$ (car M_0 est orientable) de ℓ. Notons $M_1 = M \backslash \mathring{V}$, et écrivons $M_0 = M_1 \cup V$: M_1, V et l'intersection $M_1 \cap V = \partial V \simeq \mathbb{S}^1 \times \mathbb{S}^2$ sont connexes par arcs, donc d'après le théorème de Van Kampen on a $\pi_1(M_0) \simeq \pi_1(M_1) \star_{\pi_1(\partial V)} \pi_1(V)$.

Or l'application naturelle $\pi_1(\partial V) \to \pi_1(V)$ est un isomorphisme, donc $\pi_1(M_0) \simeq \pi_1(M_1)$. Et la variété M_1 a une composante de bord $\partial M_1 \simeq \mathbb{S}^1 \times \mathbb{S}^2$.

Considérons la variété $N = \mathbb{S}^2 \times \mathbb{D}^2$, compacte orientable de dimension 4, avec une composante de bord $\partial N \simeq \mathbb{S}^2 \times \mathbb{S}^1 \simeq \partial M_1$. Recollons M_1 et N le long de leur bord : on obtient une variété M de dimension 4 compacte sans bord, et d'après Van Kampen son groupe fondamental est $\pi_1(M) = \pi_1(M_1) \star_{\pi_1(M_1\cap N)} \pi_1(N)$. Or N est simplement connexe, donc $\pi_1(M)$ est le quotient de $\pi_1(M_1)$ par le sous-groupe normal engendré par $\pi_1(M \cap N) = \langle r_m\rangle$. Ainsi $\pi_1(M)$ est isomorphe à G. $\square$

Chapitre 3

Graphes de Cayley, actions de groupes sur les arbres

De bonnes références sont [Ser77] et [dlH00].

3.1 Graphes et arbres

Définition 3.1.1. *Un* ***graphe*** *est la donnée* Γ *d'un ensemble* X *de sommets, d'un ensemble* E *d'arêtes, et de deux applications :*

$$\begin{array}{rcl} E \to X \times X & \quad et \quad & E \to E \\ e \mapsto (o(e), t(e)) & & e \mapsto \overline{e}, \end{array}$$

telles que pour tout $e \in E$*, on a* $\overline{e} \neq e$*,* $\overline{\overline{e}} = e$ *et* $o(e) = t(\overline{e})$*.*

Définition 3.1.2. *La* ***réalisation géométrique*** *du graphe* $\Gamma = (X, E)$ *est l'espace topologique* $|\Gamma|$ *quotient de* $X \sqcup (E \times [0, 1])$*, par la relation d'équivalence engendrée par :*

- *pour toute arête* $e \in E$*, on a* $o(e) \sim (e, 0)$ *et* $t(e) \sim (e, 1)$*,*
- *pour toute arête* $e \in E$ *et pour tout* $t \in [0, 1]$*, on a* $(e, t) \sim (\overline{e}, 1 - t)$*.*

Définition 3.1.3. *Un graphe* ***simplicial*** *est un graphe* (X, E) *tel que pour tous* $x, y \in X$*, il existe au plus une arête* $e \in E$ *telle que* $o(e) = x$ *et* $t(e) = y$*. Dans ce cas, on peut identifier* E *à un sous-ensemble de l'ensemble* $\mathcal{P}(X)$ *des paires d'éléments distincts de* X*.*

Définition 3.1.4. *Soit* $\Gamma = (X, E)$ *un graphe. Pour tout sommet* $x \in X$*, la* ***valence*** *(ou le* ***degré****) de* x *est le nombre d'arêtes d'origine* x*. Si tous les sommets de* Γ *ont la même valence finie* $k \in \mathbb{N}$*, on dit que* Γ *est* k***-régulier****.*

Exemples.

- Pour tout ensemble X, on peut considérer le graphe complet sur X, ayant pour ensemble de sommets X et pour ensemble d'arêtes $\mathcal{P}(X)$. Si X est fini de cardinal k, le graphe complet est $(k-1)$-régulier. Par exemple si $|X| = 3$, la réalisation géométrique de X est un triangle.

- Le graphe de sommets $\mathbb{Z}$, et d'arêtes $\{\{i, i+1\}, i \in \mathbb{Z}\}$ a pour réalisation géométrique la droite $\mathbb{R}$. Ce graphe est 2-régulier.

- Pour tout $n \geqslant 1$, on peut considérer le cycle C_n de longueur n, qui a pour sommets $\mathbb{Z}/n\mathbb{Z}$ et pour arêtes $\{\{i, i+1\}, i \in \mathbb{Z}/n\mathbb{Z}\}$. Ce graphe est 2-régulier.

Définition 3.1.5. *Soit $\Gamma = (X, E)$ un graphe. La* ***subdivision barycentrique*** *de Γ est le graphe $\Gamma' = (X', E')$, avec :*

- *$X' = X \cup \{\{e, \overline{e}\}, e \in E\}$ (les sommets de Γ et les milieux de ses arêtes),*

- *$E' = E \times \{0, 1\}$, avec $\overline{(e, 0)} = (\overline{e}, 1)$, $o((e, 0)) = o(x)$ et $t((e, 0)) = \{e, \overline{e}\}$.*

Exemples.

- Pour tout $n \geqslant 1$, C'_n est isomorphe à C_{2n}.

- Le graphe de sommets $\mathbb{Z}$ et d'arêtes $\{\{i, i+1\}, i \in \mathbb{Z}\}$ est isomorphe à sa subdivision barycentrique.

Proposition 3.1.6. *Si Γ est un graphe, sa subdivision barycentrique Γ' est un graphe simplicial. De plus, sa réalisation géométrique $|\Gamma'|$ est naturellement homéomorphe à $|\Gamma|$.*

Définition 3.1.7. *Soit Γ un graphe. Un* ***cycle*** *de Γ est un sous-graphe de Γ isomorphe à un cycle C_n, pour $n \geqslant 1$. On dit que Γ est* ***connexe*** *si deux sommets quelconques de Γ sont reliés par un chemin fini d'arêtes.*

Définition 3.1.8. *Un* ***arbre*** *est un graphe connexe et sans cycle.*

Exercice 14. *Soit Γ un graphe. Il est connexe (au sens des graphes) si et seulement si sa réalisation géométrique $|\Gamma|$ est connexe (au sens topologique). De plus, Γ est un arbre si et seulement si sa réalisation géométrique $|\Gamma|$ est simplement connexe.*

Exemples.

- Si $|X| \geqslant 3$, le graphe complet sur X est connexe, mais a des cycles.

- Le graphe $(\{1, 2\}, \{\{1, 2\}\})$ est un arbre.

- Le graphe de sommets $\mathbb{Z}$, et d'arêtes $\{\{i, i+1\}, i \in \mathbb{Z}\}$ est un arbre.

- Pour tout $n \geqslant 1$, le cycle C_n est connexe, mais n'est pas un arbre.

3.2 Graphes de Cayley

Définition 3.2.1. *Soit G un groupe engendré par une partie $S \subset G$, qu'on suppose ne contenant pas 1. Le* ***graphe de Cayley*** *de G par rapport à S est le graphe $\mathrm{Cay}(G, S)$ de sommets G, et d'arêtes :*

$$\{(g, gs) \mid g \in G, s \in S \sqcup S^{-1}\}.$$

Exercice 15. *Montrer que si G est engendré par une partie $S \subset G$, alors son graphe de Cayley $\mathrm{Cay}(G, S)$ est connexe. Montrer que si S est finie, alors $\mathrm{Cay}(G, S)$ est régulier.*

Exemples.

- Soit G un groupe quelconque et $S = G\backslash\{e\}$. Alors $\mathrm{Cay}(G,S)$ est le graphe complet sur G.
- Soit $G = \mathbb{Z}$ et $S = \{1\}$. Alors $\mathrm{Cay}(\mathbb{Z},\{1\})$ est le graphe ci-dessus, dont la réalisation géométrique est homéomorphe à la droite $\mathbb{R}$.
- Soit $G = \mathbb{Z}$ et $S = \{2,3\}$. Alors $\mathrm{Cay}(\mathbb{Z},\{2,3\})$ sensiblement différent de $\mathrm{Cay}(\mathbb{Z},\{1\})$, sa réalisation géométrique n'est pas une droite (**Exercice** : le dessiner).
- Soit $G = \mathbb{Z}^2$ et $S = \{(1,0),(0,1)\}$. Alors $\mathrm{Cay}(\mathbb{Z}^2,\{(1,0),(0,1)\})$ a pour réalisation géométrique le "quadrillage" classique du plan $\mathbb{R}^2$.
- Soit $G = \mathbb{F}_2$ et $S = \{a,b\}$. Alors $\mathrm{Cay}(\mathbb{F}_2,\{a,b\})$ est un arbre 4-régulier.
- Soit $G = D_{2\times 3} \simeq \mathfrak{S}_3 = \langle a,b \mid a^2 = b^2 = 1, (ab)^3 = 1\rangle$. Alors $\mathrm{Cay}(G,\{a,b\})$ est un hexagone, de sommets $1, a, ab, aba = bab, ba, b, 1$.

Proposition 3.2.2. *Soit G un groupe, et S une partie de G. Alors son graphe de Cayley $\mathrm{Cay}(G,S)$ est un arbre si et seulement si G est librement engendré par S.*

Démonstration. Supposons que G est librement engendré par S, alors le graphe de Cayley $\Gamma = \mathrm{Cay}(G,S)$ est connexe. Supposons qu'il y ait un cycle dans Γ, et choisissons-le de longueur $n \geqslant 1$ minimale. Ceci correspond à l'existence d'un sommet $g \in G$ et d'une suite d'éléments $s_1,\dots,s_n \in S \cup S^{-1}$ tels que $gs_1\dots s_n = g$, autrement dit $s_1\dots s_n = 1$. Comme le groupe G est libre, on déduit que deux lettres consécutives s_i, s_{i+1} sont inverses l'une de l'autre. Mais dans ce cas, on peut réduire de 2 la longueur du cycle en enlevant l'aller-retour s_is_{i+1} : ceci contredit la minimalité de la longueur du cycle. Donc Γ est un arbre.

Réciproquement, supposons que le graphe de Cayley $\Gamma = \mathrm{Cay}(G,S)$ est un arbre. Alors comme Γ est connexe, la partie S engendre G. Remarquons que comme Γ est sans cycle, on a $S \cap S^{-1} = \emptyset$. Si le groupe G n'était pas librement engendré par G, il existerait un mot réduit $s_1\dots s_n$, avec $s_i \in S \cup S^{-1}$, tel que $s_1\dots s_n = 1$ dans G. Alors le sous-graphe de sommets $\{e, s_1, s_1s_2, \dots, s_1\dots s_n = e\}$ dans Γ est un cycle de longueur n, ce qui contredit le fait que Γ est sans cycle. Donc G est librement engendré par S. □

Théorème 3.2.3. *Soit $\Gamma = (X,E)$ un graphe et $x_0 \in X$. Alors le groupe fondamental $\pi_1(|\Gamma|, x_0)$ est libre.*

Lemme 3.2.4. *Soit $\Gamma = (X,E)$ un graphe, soit $e \in E$ une arête entre deux sommets distincts $x,y \in X$, et soit $\Gamma' = (X',E')$ le graphe obtenu en écrasant l'arête e :*

- *$X' = X\backslash\{y\}$,*
- *$E' = E\backslash\{e,\overline{e}\}$, et pour toute arête $e' \in E'$ telle que $o(e') = y$ (resp. $t(e') = y$), on pose $o'(e') = x$ (resp. $t'(e') = x$).*

Alors l'application continue naturelle $f : |\Gamma| \to |\Gamma'|$ induit un isomorphisme de groupes fondamentaux $f_* : \pi_1(|\Gamma|, x) \to \pi_1(|\Gamma'|, x)$.

Démonstration. Montrons que f_* est surjective : soit ℓ' un lacet dans $|\Gamma'|$ basé en x. Ce lacet ℓ' est homotope à la concaténation d'un nombre fini d'arêtes $e'_1, \dots, e'_n$ de $|\Gamma'|$. Considérons le lacet suivant dans $|\Gamma|$, où pour toute e'_i, si elle appartient déjà à E, on la conserve, et si e'_i n'appartient pas à E, on la concatène si nécessaire avant et après avec l'arête e ou $\overline{e}$. Alors le lacet obtenu ℓ dans $|\Gamma|$ basé en x est tel que $f(\ell)$ est homotope à ℓ', donc $f_*([\ell]) = [\ell']$: f_* est surjective.

Montrons que f_* est injective : soit ℓ un lacet dans $|\Gamma|$ basé en x tel que $f(\ell)$ soit homotope au lacet constant en x. Supposons de plus que le lacet ℓ est homotope à la concaténation d'un nombre fini d'arêtes $e_1, \dots, e_n$ de $|\Gamma|$, avec $n \geqslant 0$ minimal. Alors $f(\ell)$ est homotope à la concaténation des arêtes correspondantes $e'_1, \dots, e'_n$ dans $|\Gamma'|$ (et de chemins constants en x, lorsque $e_i = e$ ou $\overline{e}$). Si $n \geqslant 1$, comme ce lacet est homotope au lacet constant, il existe deux arêtes consécutives e'_i, e'_{i+1} telles que $\overline{e'_i} = e'_{i+1}$. Ainsi les arêtes e_i, e_{i+1} dans ℓ étaient telles que $\overline{e_i} = e_{i+1}$ (en composant éventuellement à gauche et à droite par e ou $\overline{e}$). Donc le lacet ℓ n'était pas de longueur n minimale : on a donc $n = 0$, et le morphisme f_* est injectif. □

Démonstration. On peut supposer que le graphe Γ est connexe. En appliquant succesivement le Lemme 3.2.4 au graphe Γ tant qu'il possède au moins une arête entre deux sommets distincts, on obtient que le groupe fondamental de $|\Gamma|$ est isomorphe au groupe fondamental d'un graphe ayant un seul sommet, c'est-à-dire un bouquet de cercles. Donc son groupe fondamental est libre. □

3.3 Actions de groupes sur les graphes

Définition 3.3.1. *Soit $\Gamma = (X, E)$ un graphe et G un groupe. Une **action** de G sur le graphe Γ est une paire d'actions de G sur X et sur E telle que*

$$\forall g \in G, \forall e \in E, o(g \cdot e) = g \cdot o(e) \ \text{ et } t(g \cdot e) = g \cdot t(e).$$

*L'action est dite **sans inversion** si $\forall g \in G, \forall e \in E, g \cdot e \neq e$.*

*L'action est dite **libre** si elle est sans inversion, et si $\forall g \in G \backslash \{1\}, \forall x \in X, g \cdot x \neq x$.*

*Si G agit sans inversion sur le graphe $\Gamma = (X, E)$, le **graphe quotient** $G \backslash \Gamma$ a pour ensemble de sommets $G \backslash X$ et pour ensemble d'arêtes $G \backslash E$.*

Exemples.

- Soit le groupe $\mathbb{Z}$ agissant par translations sur la droite $\mathrm{Cay}(\mathbb{Z}, \{1\})$, sans inversion et librement. Le graphe quotient est une boucle.
- Plus généralement, si G est un groupe engendré par une partie finie $S \subset G$, alors G a une action sans inversion et libre sur son graphe de Cayley $\mathrm{Cay}(G, S)$. Le quotient est un bouquet de $|S|$ cercles.
- Soit Γ l'arbre $(3, 4)$-régulier. Alors le groupe $G = \mathrm{Aut}(\Gamma)$ agit sans inversion sur Γ (mais pas librement), et a pour quotient une arête.

Remarque. Si G a une action libre sur un graphe Γ, c'est une action continue et libre (au sens classique) sur la réalisation géométrique $|\Gamma|$.

Remarque. Si G agit avec sur un graphe Γ, il agit sans inversion sur sa subdivision barycentrique Γ'.

Théorème 3.3.2. *Tout groupe agissant librement sur un arbre est un groupe libre.*

Démonstration. Soit G un groupe agissant librement sur un arbre $\Gamma = (X, E)$. D'après la remarque précédente, G agit continûment et librement sur la réalisation géométrique $|\Gamma|$. Montrons qu'il s'agit d'une action propre : soit K un compact de $|\Gamma|$. Comme X est discret dans Γ, $K \cap X$ est fini. Pour tout $g \in G$ tel que $g \cdot K \cap K \neq \emptyset$, on a $g \cdot (K \cap X) \cap (K \cap X) \neq \emptyset$, donc il y a au plus $|K \cap X|$ tels éléments $g \in G$: l'action est propre.

Comme $|\Gamma|$ est simplement connexe, séparé et localement connexe par arcs, d'après le théorème 1.2.10, le groupe G est isomorphe au groupe fondamental du quotient $|\Gamma|/G$, qui n'est autre que la réalisation géométrique du graphe quotient Γ/G.

D'après le théorème 3.2.3, le groupe fondamental du graphe Γ/G est libre, donc Γ est un groupe libre. □

Corollaire 3.3.3 (Théorème de Schreier)**.** *Soit F un groupe libre et G un sous-groupe de F. Alors G est un groupe libre.*

Démonstration. Si S engendre librement F, alors F a une action libre et propre sur son graphe de Cayley $\Gamma = \mathrm{Cay}(F, S)$. Donc G a une action libre sur le graphe Γ : d'après le théorème 3.3.2, G est un groupe libre. □

3.4 2-complexes de Cayley

Définition 3.4.1. *Un CW-complexe de dimension 2 est obtenu, à partir de la réalisation géométrique d'un graphe $|\Gamma|$, en recollant des disques $\mathbb{D}^2$ à l'aide d'applications continues $\partial\mathbb{D}^2 = \mathbb{S}^1 \to |\Gamma|$.*

Exemples.

- On peut voir la sphère $\mathbb{S}^2$ comme un CW-complexe de dimension 2 en recollant, sur le graphe $\mathbb{S}^1$ "équatorial", de deux disques "nord" et "sud".
- On peut voir le tore $\mathbb{T}^2$ comme un CW-complexe de dimension 2 en recollant, sur un "quadrillage" tracé sur la surface de tores, un disque sur chaque "carré".

Définition 3.4.2. *Soit $G = \langle S \mid R \rangle$ un groupe de présentation finie. Son **2-complexe de Cayley**, noté $\mathrm{Cay}^2(G, S, R)$, est le CW-complexe de dimension 2 ayant pour 1-squelette le graphe de Cayley $\mathrm{Cay}(G, S)$, et pour 2-cellules les disques dont les bords sont donnés par les mots grg^{-1}, où $g \in \mathbb{F}(S)$ et $r \in R$.*

Théorème 3.4.3. *Soit $G = \langle S \mid R \rangle$ un groupe de présentation finie. Son 2-complexe de Cayley $\mathrm{Cay}^2(G, S, R)$ est simplement connexe, et son quotient par l'action de G est un CW-complexe fini de dimension 2, dont le groupe fondamental est naturellement isomorphe à G.*

Démonstration. Soit ℓ un lacet dans $\mathrm{Cay}^2(G, S, R)$ basé en e. Alors ℓ est homotope à un lacet $s_1 \dots s_n$ du 1-squelette $\mathrm{Cay}(G, S)$, où $s_i \in S \cup S^{-1}$ pour tout $1 \leqslant i \leqslant n$.

Comme c'est un lacet, le mot $s_1 \dots s_n$ évalué dans G est égal à $\overline{s_1 \dots s_n}^G = 1$. Comme G a pour présentation $G = \langle S \mid R \rangle$, il existe un nombre fini de conjugués de R,

$g_1r_1g_1^{-1}, \dots, g_mr_mg_m^{-1}$, où $g_i \in \mathbb{F}(S)$ et $r_i \in R$ pour tout $1 \leqslant i \leqslant m$, tel qu'on ait l'égalité $s_1 \dots s_m = g_1r_1g_1^1g_2r_2g_2^{-1} \dots g_mr_mg_m^{-1}$ dans $\mathbb{F}(S)$.

Grâce aux m 2-cellules dont les bords sont $g_1r_1g_1^1, (g_1r_1g_1^1)g_2r_2g_2^{-1}(g_1r_1g_1^1)^{-1}, \dots,$ $g_1r_1g_1^1g_2r_2g_2^{-1} \dots g_mr_mg_m^{-1}(g_{m-1}r_{m-1}g_{m-1}^{-1})^{-1} \dots (g_1r_1g_1^1)^{-1}$, on en déduit que le lacet ℓ est homotope au lacet trivial.

Comme le 1-squelette $\mathrm{Cay}(G, S)$ est connexe, le 2-complexe $\mathrm{Cay}^2(G, S, R)$ est connexe, il est donc simplement connexe.

Enfin, comme le groupe G agit librement et proprement sur $\mathrm{Cay}^2(G, S, R)$, on en déduit que le quotient $G\backslash \mathrm{Cay}^2(G, S, R)$ a pour groupe fondamental G. De plus, $G\backslash \mathrm{Cay}^2(G, S, R)$ est un 2-complexe fini : il a 1 sommet, $|S|$ arêtes et $|R|$ 2-cellules. $\square$

Exemples.

- Pour $\mathbb{Z}^2 = \langle a, b \mid aba^{-1}b^{-1}\rangle$, le 2-complexe de Cayley est le plan $\mathbb{R}^2$ quadrillé par des carrés. Le quotient $\mathbb{Z}^2\backslash\mathbb{R}^2$ est homéomorphe au tore $\mathbb{T}^2$, qui a bien pour groupe fondamental $\mathbb{Z}^2$.

- Pour $G = \langle a, b \mid aba^{-1}b\rangle$, le 2-complexe de Cayley est aussi le plan $\mathbb{R}^2$ quadrillé par des carrés. Mais l'action du groupe G est différente : le quotient est le quotient d'un carré par des identifications d'arêtes, et est une bouteille de Klein.

- Pour le groupe fondamental d'une surface de genre 2, $G = \langle a, b, c, d \mid aba^{-1}b^{-1}cdc^{-1}d^{-1}\rangle$, le quotient du 2-complexe de Cayley est le quotient d'un octogone par des identifications d'arêtes, et est une surface compacte de genre 2.

3.5 Graphes de groupes

Théorème 3.5.1. *Soit G un groupe opérant sans inversion sur un arbre $\Gamma = (X, E)$, tel que le graphe quotient Γ/G soit une arête entre deux sommet distincts. Soient $x, y \in X$ et $e \in E$ une arête entre x et y, de sorte que $\Gamma/G = (\{G \cdot x, G \cdot y\}, \{G \cdot e, G \cdot \overline{e}\})$. Notons G_x (resp. G_y, G_e) le stabilisateur dans G de x (resp. y, e). Il y a des inclusions naturelles $G_e \to G_x$ et $G_e \to G_y$. Alors G est isomorphe au produit amalgamé*

$$G \simeq G_x \star_{G_e} G_y.$$

Démonstration. Montrons tout d'abord que G est engendré par $G_x \cup G_y$: notons G' le sous-groupe de G engendré par $G_x \cup G_y$. Notons $T = \{\{x, y\}, \{e, \overline{e}\}\}$ le sous-graphe de Γ correpondant à l'arête e. Alors $G' \cdot T$ et $(G\backslash G') \cdot T$ sont des sous-graphes disjoints de Γ, dont la réunion est égale à Γ. Comme le graphe Γ est connexe, on en déduit que $(G\backslash G') \cdot T = \emptyset$ et $G' \cdot T = \Gamma$, d'où $G' = G$.

Considérons le morphisme $f : G_x \star_{G_e} G_y \to G$ associé aux inclusions naturelles de G_x, G_y et G_e dans G. Le morphisme f est surjectif d'après ce qui précède, montrons qu'il est injectif : soit $cg_1 \dots g_n \in \operatorname{Ker} f$, où l'élément est en forme normale : $n \in \mathbb{N}$, $c \in G_e$ et $g_i \in G_x$ ou $g_i \in G_y$. Alors le chemin $e, g_1 \cdot \overline{e}, g_1g_2 \cdot e, \dots, g_1 \dots g_n \cdot e = e$ est un cycle, or le graphe Γ est un arbre et l'élément est en forme normale, donc on déduit que $n = 0$. Ainsi $\operatorname{Ker} f = \{1\}$: f est un isomorphisme de groupes. $\square$

On a une réciproque.

Théorème 3.5.2. *, Soient A, B, C trois groupes, et deux morphismes injectifs $C \to A$ et $C \to B$, dont on note G le produit amalgamé $G = A \star_C B$. Alors il existe un arbre $\Gamma = (X, E)$, une action sans inversion de G sur Γ, et une arête $e \in E$ entre deux sommets distincts $x, y \in X$ tels que $G_x = A$, $G_y = B$ et $G_e = C$.*

Démonstration. Considérons le graphe $\Gamma = (X, E)$, avec :

- $X = G/A \sqcup G/B$,
- $E = G/C \sqcup \overline{G/C}$,
- les applications $o : G/C \to G/A$ et $t : G/C \to G/B$ sont induites par les inclusions $C \to A$ et $C \to B$.

Le groupe G agit sur Γ par translation à gauche, et cette action est bien sans inversion.

Considérons maintenant les sommets $x = A$, $y = B$ et l'arête $e = C$. Alors on a bien $G_x = A$, $G_y = B$ et $G_e = C$. Comme G est engendré par $A \cup B$, le graphe Γ est connexe.

De plus, tout cycle dans le graphe Γ correspond à une écriture sous forme normale de l'élément neutre de G : ainsi le graphe Γ est un arbre. $\square$

Exemples.

- Le groupe diédral infini $D_\infty = \langle a, b \mid a^2 = b^2 = 1\rangle \simeq \mathbb{Z}/2\mathbb{Z} \star \mathbb{Z}/2\mathbb{Z}$ opère sans inversion sur la droite réelle.
- Le groupe $G = \mathbb{Z}/3\mathbb{Z} \star \mathbb{Z}/4\mathbb{Z}$ opère sans inversion sur l'arbre infini birégulier de valences 3 et 4.
- Le groupe $\mathrm{SL}(2, \mathbb{Z})$ est isomorphe au produit amalgamé $\mathbb{Z}/6\mathbb{Z} \star_{\mathbb{Z}/2\mathbb{Z}} \mathbb{Z}/4\mathbb{Z}$, et opère sans inversion sur un arbre 3-régulier (voir plus loin).

Théorème 3.5.3. *Soit G un groupe opérant sans inversion sur un arbre $\Gamma = (X, E)$, tel que le graphe quotient Γ/G soit une boucle. Soient $x, y \in X$ deux sommets distincts et $e \in E$ une arête entre x et y, de sorte que $\Gamma/G = (\{G \cdot x\}, \{G \cdot e, G \cdot \overline{e}\})$. Notons G_x (resp. G_y, G_e) le stabilisateur dans G de x (resp. y, e). Il y a des inclusions naturelles $G_e \to G_x$ et $G_e \to G_y$. Comme G_y est conjugué à G_x, cela fournit un autre morphisme injectif $\alpha : G_e \to G_x$. Alors G est isomorphe à l'extension HNN*

$$G \simeq G_x \star_{G_e} .$$

Démonstration. Soit $t \in G$ un élément tel que $y = t \cdot x$, on a alors $G_y = tG_xt^{-1}$.

Montrons tout d'abord que G est engendré par $G_x \cup \{t\}$: notons G' le sous-groupe de G engendré par $G_x \cup \{t\}$. Notons $T = \{\{x, y\}, \{e, \overline{e}\}\}$ le sous-graphe de Γ correpondant à l'arête e. Alors $G' \cdot T$ et $(G \backslash G') \cdot T$ sont des sous-graphes disjoints de Γ, dont la réunion est égale à Γ. Comme le graphe Γ est connexe, on en déduit que $(G\backslash G') \cdot T = \emptyset$ et $G' \cdot T = \Gamma$, d'où $G' = G$.

Considérons le morphisme $f : G_x \star_{G_e} \to G$ associé aux inclusions naturelles de G_x et $G_y = tG_xt^{-1}$ dans G. Le morphisme f est surjectif d'après ce qui précède, montrons qu'il est injectif : soit $g_0 t^{\varepsilon_1} g_1 t^{\varepsilon_2} \dots t^{\varepsilon_n} g_n \in \operatorname{Ker} f$ un élément en forme normale. Alors le chemin $e, g_0 \cdot \overline{e}, g_0 t^{\varepsilon_1} g_1 \cdot e, \dots, g_0 t^{\varepsilon_1} g_1 t^{\varepsilon_2} \dots t^{\varepsilon_n} g_n \cdot e = e$ est un cycle, or graphe Γ est un arbre et l'élément est en forme normale, donc on déduit que $n = 0$. Ainsi $\operatorname{Ker} f = \{1\}$: f est un isomorphisme de groupes. $\square$

On a une réciproque.

Théorème 3.5.4. *, Soient A, C deux groupes, avec $C \subset A$, et soit $\alpha : C \to A$ un morphisme injectif, dont on note l'extension HNN $G = A\star_C$, et soit $t \in G$ l'élément conjuguant C à $\alpha(C)$. Alors il existe un arbre $\Gamma = (X, E)$, une action sans inversion de G sur Γ, et une arête $e \in E$ entre deux sommets distincts $x, y \in X$ tels que $G_x = A$, $G_y = tAt^{-1}$ et $G_e = C$.*

Démonstration. Considérons le graphe $\Gamma = (X, E)$, avec :

- $X = G/A$,
- $E = G/C \sqcup \overline{G/C}$,
- les applications $o : G/C \to G/A : gC \mapsto gA$ et $t : G/C \to G/A : gC \mapsto gtA$ (qui est bien définie car $tCt^{-1} = \alpha(C) \subset A$).

Le groupe G agit sur Γ par translation à gauche, et cette action est bien sans inversion.

Considérons maintenant les sommets $x = A$, $y = tA$ et l'arête $e = C$. Alors on a bien $G_x = A$, $G_y = tAt^{-1}$ et $G_e = C$. Comme G est engendré par $A \cup \{t\}$, le graphe Γ est connexe.

De plus, tout cycle dans le graphe Γ correspond à une écriture sous forme normale de l'élément neutre de G : ainsi le graphe Γ est un arbre. □

Exemples.

- L'action de $\mathbb{Z}$ par translations sur $\Gamma = \mathrm{Cay}(\mathbb{Z}, \{1\})$ fournit une écriture $\mathbb{Z} \simeq \{1\}\star_{\{1\}}$.
- L'action de $\mathbb{Z}^2$ sur la droite réelle par $(a, b) \cdot x = a + x$ fournit une écriture $\mathbb{Z}^2 \simeq \mathbb{Z}\star_{\{1\}}$.

3.6 Distances dans les graphes et applications

Définition 3.6.1. *Si $\Gamma = (X, E)$ est un graphe connexe, on peut munir sa réalisation géométrique $|\Gamma|$ d'une distance naturelle, en déclarant que chaque arête est de longueur 1, et que la distance entre deux points de $|\Gamma|$ est la longueur du plus court chemin les reliant.*

Proposition 3.6.2. *Si $\Gamma = (X, E)$ est un arbre, pour tous points $x, y \in |\Gamma|$, il existe un unique plus court chemin entre x et y, appelé **géodésique** entre x et y.*

Démonstration. S'il existait deux plus courts chemins entre x et y, il y aurait un cycle dans l'arbre Γ. □

Théorème 3.6.3 (Théorème de point fixe dans un arbre)**.** *Soit G un groupe agissant sans inversion sur un arbre $\Gamma = (X, E)$, tel que l'orbite d'un sommet $x_0 \in X$ soit bornée. Alors il existe un sommet de Γ fixé par tous les éléments de G.*

Démonstration. Fixons notre orbite bornée $B = G \cdot x_0$. Considérons l'application $f : X \to \mathbb{N}$, qui à un sommet $x \in X$ associe la plus grand distance entre x et un point de B. Comme B est borné, f est bien définie. Comme f est à valeurs finies, il existe $x \in X$ minimisant f : notons $m = f(x)$. Supposons par l'absurde qu'il existe $y \in X$ un autre sommet de X minimisant f.

Supposons tout d'abord que x et y ne soient pas adjacents : il existe alors un sommet z sur la géodésique entre x et y. Comme $f(z) \geqslant m$, il existe un point $b \in B$ tel que $d(z, b) = m$. Comme $d(z, x) \leqslant m$, la géodésique de x à b ne passe pas par z. De même, la géodésique de y à b ne passe pas par z. Mais alors, $[xb] \cup [by] \cup [yx]$ contient un cycle de l'arbre Γ : c'est une contradiction.

Ainsi y est adjacent à x. Ceci prouve, comme Γ ne contient pas de triangle, que l'ensemble S des sommets de X minimisant f est soit un singleton, soit deux sommets adjacents. Comme G agit sans inversion, aucun élément de G n'échange x et y. Donc dans tous les cas, le sommet x est fixé par tous les éléments de G. □

Théorème 3.6.4. *Soit G un produit amalgamé $G = A \star_C B$ ou bien une extension HNN $G = A\star_C$. Tout sous-groupe fini de G est conjugué à un sous-groupe fini de A (ou de B dans le cas amalgamé).*

Démonstration. La preuve étant similaire dans les deux cas, traitons celui où G est un produit amalgamé. Soit F un sous-groupe fini de G. Comme G est un produit amalgamé, d'après le théorème 3.5.2, G agit sur un arbre $\Gamma = (X, E)$ sans inversion, avec des sommets x, y reliés par une arête e tels que $G_x = A$, $G_y = B$ et $G_e = C$. Comme F est un groupe fini, l'orbite par F de tout sommet est borné. D'après le théorème 3.6.3, F fixe un sommet de Γ, donc F est conjugué à un sous-groupe de A ou de B. □

Exercice 16. *Soit $g \in A \star B$ un élément d'ordre fini, montrer que g est conjugué à un élément de A ou de B.*

Proposition 3.6.5. *Soit Γ un arbre, et g un automorphisme sans inversion de Γ. Alors il y a deux possibilités, mutuellement exclusives :*

- *soit g a un point fixe dans Γ (g est appelé **elliptique**),*
- *soit il existe une unique droite géodésique $T \subset \Gamma$ telle que g préserve T et agisse sur $T \simeq \mathbb{R}$ par translation d'un nombre entier non nul (g est appelé **loxodromique**).*

Démonstration. Définissons la fonction distance de translation

$$\begin{aligned} \delta_g : X &\to \mathbb{N} \\ x &\mapsto d(x, g \cdot x). \end{aligned}$$

Soit $x \in X$ réalisant le minimum $\delta \in \mathbb{N}$ de la fonction δ_g.

Si g a un point fixe, alors $\delta = 0$. Supposons que g est sans point fixe, et donc que $\delta \geqslant 1$.

Montrons que $g \cdot x$ est sur la géodésique entre x et $g^2 \cdot x$. Si ce n'est pas le cas, la concaténation des géodésiques $[x, g \cdot x] \cup [g \cdot x, g^2 \cdot x]$ n'est pas géodésique : les sommets adjacents à $g \cdot x$ sur les arêtes $[x, g \cdot x]$ et $[g \cdot x, g^2 \cdot x]$ coïncident : appelons ce sommet y. Par translation par g, le sommet gy est donc adjacent à $g^2 \cdot x$ sur la géodésique $[g \cdot x, g^2 \cdot x]$. En particulier, $d(y, g \cdot y) \leqslant d(g \cdot x, g^2 \cdot x) - 2 = \delta - 2$. Ceci contredit la minimalité de δ.

Ainsi $g \cdot x$ est sur la géodésique entre x et $g^2 \cdot x$. Cet argument montre que pour tout $n \in \mathbb{N}$, la géodésique $[g^{-n-1} \cdot x, g^{n+1} \cdot x]$ contient la géodésique $[g^{-n} \cdot x, g^n \cdot x]$. Ainsi la réunion $T = \bigcup_{n \in \mathbb{N}} [g^{-n-1} \cdot x, g^{n+1} \cdot x]$ est une droite géodésique, sur laquelle g agit par translation de δ.

Montrons que T est unique : supposons que $y \in X$ soit un sommet tel que $\delta_g(y) = \delta$, nous allons montrer que $y \in T$. Soit $z \in T$ l'unique sommet de T le plus proche de y. Alors

$g \cdot z$ est l'unique sommet de T le plus proche de $g \cdot y$, donc la réunion $[z, y] \cup [y, g \cdot y] \cup [g \cdot y, g \cdot z]$ est une géodésique. En particulier, $d(z, g \cdot z) = 2d(z, y) + d(y, g \cdot y)$, soit $\delta = 2d(z, y) + \delta$. Ainsi $d(z, y) = 0$, donc $y \in T$: T est bien unique. $\square$

3.7 Propriété (FA)

Définition 3.7.1. *On dit qu'un groupe G a la* ***propriété (FA)*** *si, pour tout arbre Γ et pour toute action de G sur Γ sans inversion, cette action a un point fixe.*

Exemple. Nous avons vu, avec le théorème 3.6.3, que tout groupe fini a la propriété (FA).

Théorème 3.7.2. *Soit G un groupe de type fini. Alors G a la propriété (FA) si et seulement si les deux conditions suivantes sont vérifiées :*

- *G n'est pas un produit amalgamé, et*
- *G n'a pas de quotient isomorphe à $\mathbb{Z}$.*

Lemme 3.7.3. *Soit G un groupe agissant sans inversion sur un arbre Γ, tel que le quotient $G \backslash \Gamma$ soit un arbre. Alors il existe un sous-arbre $T \subset \Gamma$ tel que G soit engendré par les stabilisateurs des sommets de T.*

Démonstration. Notons $\Gamma = (X, E)$. Choisissons un sous-arbre $T \subset \Gamma$ tel que $T \simeq G \backslash \Gamma$. Notons H le sous-groupe de G engendré par les stablisateurs des sommets de T. Supposons par l'absurde que $G \neq H$, et considérons un tel élément $g \in G \backslash H$ tel que $\min_{x \in X} d(x, g \cdot x) = n \geqslant 1$ soit minimale. Choisissons $x_0 \in X$ tel que $d(x_0, g \cdot x_0) = n$, on peut même choisir $x_0 \in T$.

Notons $e_1, \ldots, e_n \in E$ les arêtes de la géodésique de x_0 à $g \cdot x_0$, et notons les sommets $x_0, x_1, \ldots, x_n = g \cdot x_0$. Quitte à multiplier g à gauche par un élément de G_{x_0}, on peut supposer que $x_1 \in T$. Dans le quotient $G \backslash \Gamma$, on obtient un lacet $Ge_1, \ldots, Ge_n$ dans un arbre. Quitte à changer x_0 en un autre sommet parmi $x_0, x_1, \ldots, x_n$, on peut supposer que $Ge_1 = G\overline{e_2}$. Il existe donc $h \in G_{x_1}$ tel que $h \cdot x_2 = x_0$. Ainsi $d(gh \cdot x_2, x_2) = d(x_n, x_2) = n - 2 < n$. Par minimalité de n, on a $gh \in H$. Or $h \in H$, donc $g \in H$: contradiction. Ainsi $G = H$. $\square$

Lemme 3.7.4. *Soit G un groupe agissant sans inversion sur un arbre $\Gamma = (X, E)$, et soit $x_0 \in X$. Alors il existe un morphisme naturel surjectif de G sur $\pi_1(G \backslash \Gamma, Gx_0)$.*

Démonstration. Soit $g \in G$, et considérons le chemin géodésique $[x_0, g \cdot x_0]$ de x_0 à $g \cdot x_0$. Dans le quotient $G \backslash \Gamma$, cela définit un lacet basé en Gx_0. Notons $\phi(g) = [G[x_0, g \cdot x_0]]$ sa classe d'homotopie dans $\pi_1(G \backslash \Gamma, Gx_0)$.

Montrons tout d'abord que $\phi : G \to \pi_1(G \backslash \Gamma, Gx_0)$ est bien un morphisme. Soient $g, h \in G$. Il existe un unique sommet $m \in X$ tel que $m \in [x_0, g \cdot x_0] \cap [g \cdot x_0, gh \cdot x_0] \cap [x_0, gh \cdot x_0]$. Alors $\phi(g)\phi(h)$ est la classe d'homotopie de la composition des lacets $G[x_0, g \cdot x_0]$ et $G[x_0, h \cdot x_0]$. Or $[x_0, g \cdot x_0] = [x_0, m] \cup [m, g \cdot x_0]$ et $g[x_0, h \cdot x_0] = [g \cdot x_0, gh \cdot x_0] = [g \cdot x_0, m] \cup g[m, gh \cdot x_0]$. Donc $\phi(g)\phi(h)$ est la classe d'homotopie de la composition des chemins $G[x_0, m]$, $G[m, g \cdot x_0]$, $G[g \cdot x_0, m]$ et $G[m, gh \cdot x_0]$: c'est donc la classe d'homotopie du lacet $G[x_0, gh \cdot x_0]$, d'où $\phi(g)\phi(h) = \phi(gh)$.

Montrons ensuite que ϕ est surjectif : soit ℓ un lacet dans $G \backslash \Gamma$ basé en Gx_0. Ce lacet se relève en un chemin ℓ' dans Γ de x_0 à un sommet $y \in Gx_0$. Notons $g \in G$ tel que $y = g \cdot x_0$.

Par unicité des chemins (à homotopie près) dans un arbre, on sait que $\ell' = [x_0, g \cdot x_0]$, d'où $\phi(g)$ est la classe d'homotopie du lacet ℓ. Ainsi ϕ est surjective. $\square$

Démonstration. Soit G un groupe de type fini ayant la propriété (FA).

Supposons que G est un produit amalgamé non trivial $G = A \star_C B$, donc d'après le théorème 3.5.2, G a une action sur un arbre, avec deux orbites de sommets. Comme G a un point fixe pour cette action, c'est une contradiction.

Supposons que G a un quotient $\phi : G \to \mathbb{Z}$ isomorphe à $\mathbb{Z}$. Alors l'action par translation de $\mathbb{Z}$ sur la droite $\Gamma = \mathrm{Cay}(\mathbb{Z}, \{1\})$ définit une action de G sur Γ sans point fixe, ce qui contredit la propriété (FA).

Réciproquement, supposons que G vérifie les deux propriétés, et considérons une action de G sur un arbre Γ. Si le quotient $G\backslash\Gamma$ n'est pas un arbre, alors d'après le lemme 3.7.4, il existe un morphisme surjectif de G vers un groupe libre non trivial. En particulier, G a un morphisme surjectif vers $\mathbb{Z}$, ce qui contredit la deuxième hypothèse sur G.

Donc le quotient $G\backslash\Gamma$ est un arbre : d'après le lemme 3.7.3, il existe un sous-arbre $T \subset \Gamma$ tel que G soit engendré par les stabilisateurs des sommets de T. Comme G est de type fini, il existe un sous-arbre fini $T' \subset T$ tel que G soit engendré par les stabilisateurs des sommets de T'. Choisissons un tel sous-arbre fini T' minimal.

Si T' est réduit à un seul sommet x, alors G fixe x. Sinon, considérons un sommet terminale x de T', notons e l'unique arête de T' d'origine x, et considérons le sous-arbre $T'' = T' \backslash \{x\}$.

Considérons l'arbre Γ obtenu à partir de Γ en écrasant toutes les arêtes autre que $G \cdot e$: le groupe G agit encore sans inversion sur l'arbre Γ', et a pour quotient une arête entre deux sommets distincts. D'après le théorème 3.5.1, le groupe G est donc le produit amalgamé $G = G_x \star_{G_e} H$, où H désigne le sous-groupe de G engendré par les stabilisateurs de sommets de T''. Par minimalité de T', on a $H \neq G$, donc G est un produit amalgamé non trivial. Ceci contredit la première hypothèse sur G. $\square$

Proposition 3.7.5. *Soit G un groupe ayant la propriété (FA). Si G est contenu dans un amalgame $A \star_C B$, alors G est contenu dans un conjugué de A ou de B.*

Proposition 3.7.6 (Admis)**.** *Soit G un groupe ayant la propriété (FA), et $\phi : G \to \mathrm{GL}(2, \mathbb{K})$ une représentation, où $\mathbb{K}$ est un corps commutatif. Pour tout $g \in G$, les valeurs propres de $\phi(g)$ sont entières sur $\mathbb{Z}$.*

Exercice 17. *Montrer que le groupe du trèfle $G_\clubsuit = \langle xy \mid x^2 = y^3 \rangle$ n'a pas la propriété (FA).*

Exercice 18. *Montrer que le groupe $G = \langle a, b, c \mid abca = bcac, bcc = aca \rangle$ n'a pas la propriété (FA).*

3.8 Propriété (FA) pour $\mathrm{SL}(3, \mathbb{Z})$

L'objectif de cette partie est de montrer le théorème suivant :

Théorème 3.8.1 (Serre-Margulis-Tits)**.** *Le groupe $\mathrm{SL}(3, \mathbb{Z})$ a la propriété (FA).*

Il a le corollaire suivant :

Corollaire 3.8.2. *Le groupe* $\mathrm{SL}(3, \mathbb{Z})$ *n'est pas un amalgame, et n'a pas de quotient isomorphe à* $\mathbb{Z}$*.*

Lemme 3.8.3. *Soit* Γ *un arbre, et soit* G *un groupe agissant sans inversion sur* Γ*. Alors le sous-graphe* Γ_G *des points fixes est un arbre.*

Démonstration. Soient $x, y \in \Gamma_G$, alors par unicité de la géodésique, pour tout $g \in G$, on a $g \cdot [x, y] = [g \cdot x, g \cdot y] = [x, y]$. En particulier, la géodésique $[x, y]$ est incluse dans Γ_G. Ainsi Γ_G est un sous-graphe connexe de l'arbre Γ, c'est donc un arbre. □

Lemme 3.8.4. *Soit* $\Gamma = (X, E)$ *un arbre, et* g *un automorphisme de* Γ *elliptique. Alors pour tout sommet* $x \in X$*, le milieu de la géodésique* $[x, g \cdot x]$ *est fixé par* g*.*

Démonstration. Notons Γ_g le sous-arbre de Γ fixé par g. Notons $y \in \Gamma_g$ l'unique sommet le plus proche de x. Alors si z désigne le sommet de la géodésique $[y, x]$ à distance 1 de y, on a $g \cdot z \neq z$, comme $z \notin \Gamma_g$. Ainsi le chemin $[x, y] \cup [y, g \cdot x]$ est une géodésique. En particulier, le milieu y de la géodésique $[x, g \cdot x]$ est fixé par g. □

Proposition 3.8.5. *Soit* G *un groupe engendré par des éléments* $(a_i)_{i \in I}$ *et* $(b_j)_{j \in J}$*, et notons* A *et* B *les sous-groupes engendrés par les* $(a_i)_{i \in I}$ *et par les* $(b_j)_{j \in J}$ *respectivement. Supposons que* G *agisse sans inversion sur un arbre* Γ*, tel que* A *et* B *aient des points fixes, et tel que pour tout couple* $(i, j) \in I \times J$*,* $a_i b_j$ *ait un point fixe. Alors* G *a un point fixe.*

Démonstration. Notons Γ_A et Γ_B les sous-arbres de Γ fixés par A et B respectivement. Si $\Gamma_A \cap \Gamma_B \neq \emptyset$, alors G fixe l'intersection.

Supposons par l'absurde que $\Gamma_A \cap \Gamma_B = \emptyset$. Il existe un unique chemin géodésique le plus court entre Γ_A et Γ_B : notons-le $[x, y]$, avec $x \in \Gamma_A$ et $y \in \Gamma_B$. Soit $z \in [x, y]$ le sommet à distance 1 de x : comme $z \notin \Gamma_A$, il existe $i \in I$ tel que $a_i \cdot z \neq z$. Alors le chemin $[y, x] \cup [x, a_i \cdot y]$ est une géodésique.

Pour tout $j \in J$, comme $a_i b_j$ a un point fixe, d'après le lemme 3.8.4, et comme $a_i b_j \cdot y = a_i \cdot y$, on sait que $a_i b_j$ fixe le milieu x de $[y, a_i \cdot y]$. Ainsi x est fixé par tous les $(b_j)_{j \in J}$, donc est fixé par B : ceci contredit l'hypothèse $x \notin \Gamma_B$. □

Corollaire 3.8.6. *Soit* G *un groupe agissant sans inversion sur un arbre* Γ*, et supposons que* G *est engendré par des éléments* $s_1, \ldots, s_n$ *tels que chaque* s_i *soit elliptique, et tels que chaque produit* $s_i s_j$ *soit elliptique. Alors* G *a un point fixe.*

Démonstration. On peut appliquer la proposition 3.8.5 récursivement, en posant $a_1 = s_1, \ldots, a_{n-1} = s_{n-1}$ et $b_1 = s_n$. □

Exercice 19. *Montrer que le groupe* $G = \langle a, b, c \mid a^2, b^2, c^2, (ab)^3, (bc)^3, (ac)^3 \rangle$ *a la propriété (FA). (Admis : il est infini)*

Proposition 3.8.7. *Soit* G *un groupe nilpotent de type fini agissant sans inversion sur un arbre* Γ*. Alors il y a deux possiblités, mutuellement exclusives :*

- *soit* G *a un point fixe,*
- *soit il existe une unique droite géodésique* $T \subset \Gamma$ *invariante par* G*, telle que* G *agisse sur* T *par translations au moyen d'un morphisme non trivial* $G \to \mathbb{Z}$*.*

Démonstration. Choisissons une suite de sous-groupes normaux de G, $\{1\} = G_0 \subset G_1 \subset \cdots \subset G_n = G$ telle que, pour tout $0 \leqslant i \leqslant n-1$, le quotient G_{i+1}/G_i soit monogène. Effectuons une récurrence sur $n \in \mathbb{N}$. Le cas $n = 0$ est trivial.

Supposons donc que $n \geqslant 1$, et supposons par récurrence que le groupe $H = G_{n-1}$ satisfasse la conclusion de la proposition.

Si H a un point fixe, considérons le sous-arbre Γ_H constitué des points fixes de H. Alors le groupe monogène G/H agit sur cet arbre Γ_H, notons $gH \in G/H$ un générateur de ce groupe.

- Si gH a un point fixe dans Γ_H, c'est un point fixe pour G/H, et donc un point fixe pour G.

- Si gH n'a pas de point fixe dans Γ_H, d'après le lemme 3.6.5, gH est loxodromique, donc il existe une unique droite géodésique $T \subset \Gamma_H$ translatée par gH. Ainsi T est invariante par G, et translatée au moyen du morphisme $G \to G/H \simeq \mathbb{Z}$.

Si H n'a pas de point fixe, considérons la droite géodésique $T \subset \Gamma$ translatée par H. Comme H est distingué dans G et que T est unique, G stabilise la droite T. L'image de G dans $\mathrm{Aut}(T)$ est alors soit $\mathbb{Z}$, soit le groupe diédral infini $D_{2\times\infty}$. Or ce groupe $D_{2\times\infty}$ n'est pas nilpotent (**Exercice**), donc ce ne peut pas être le quotient du groupe nilpotent G. Ainsi l'image de G dans $\mathrm{Aut}(T)$ est $\mathbb{Z}$: le groupe G agit sur T par translations au moyen d'un morphisme non trivial $G \to \mathbb{Z}$. □

Corollaire 3.8.8. *Soit G un groupe nilpotent de type fini agissant sans inversion sur un arbre Γ. Si G est engendré par des éléments ayant un point fixe, alors G a un point fixe.*

Démonstration. Par l'absurde, supposons que G n'ait pas de point fixe. D'après la proposition 3.8.7, il existe une droite géodésique $T \subset \Gamma$ invariante par G, telle que G agisse sur T par translations au moyen d'un morphisme $\phi : G \to \mathbb{Z}$. Si $g \in G$ a un point fixe, alors $\phi(g) = 0$. Ainsi $\phi = 0$, donc G a donc un point fixe : ceci contredit l'hypothèse. □

Corollaire 3.8.9. *Soit G un groupe nilpotent de type fini agissant sans inversion sur un arbre Γ. Si g appartient au sous-groupe dérivé G' de G, alors g a un point fixe.*

Démonstration. Si G a un point fixe, alors g aussi. Sinon, d'après la proposition 3.8.7, il existe une droite géodésique $T \subset \Gamma$ invariante par G, telle que G agisse sur T par translations au moyen d'un morphisme $\phi : G \to \mathbb{Z}$. Alors $\phi(g) = 0$, donc g a un point fixe. □

Démonstration. [$\mathrm{SL}(3,\mathbb{Z})$ a la propriété (FA)] Si $i, j \in \{1, 2, 3\}$, notons e_{ij} la matrice élémentaire avec des zéros partout, et un 1 en ligne i et colonne j. On sait que $\mathrm{SL}(3,\mathbb{Z})$ est engendré par les $\{1 + e_{ij}, i \neq j\}$.

Notons $g_0 = 1+e_{12}$, $g_1 = 1+e_{13}$, $g_2 = 1+e_{23}$, $g_3 = 1+e_{21}$, $g_4 = 1+e_{31}$ et $g_5 = 1+e_{32}$ (et $g_6 = g_0$). On a les propriétés suivantes :

- Pour tout i, g_i commute avec g_{i+1} et g_{i-1}.

- Le commutateur de g_{i+1} et de g_{i-1} est égal à g_i ou à g_i^{-1}.

Ainsi $\mathrm{SL}(3,\mathbb{Z})$ est engendré par g_1, g_3 et g_5. De plus, pour tout i, les éléments g_{i-1} et g_{i+1} engendrent un groupe nilpotent B_i.

Supposons que $\mathrm{SL}(3,\mathbb{Z})$ agisse sans inversion sur un arbre Γ. Pour tout i, d'après le corollaire 3.8.9, g_i a un point fixe dans Γ. Donc d'après le corollaire 3.8.8, comme B_i est engendré par g_{i-1} et g_{i+1} qui ont des points fixes, B_i a un point fixe. En particulier, $g_{i-1}g_{i+1}$ et $g_{i+1}g_{i-1}$ ont des points fixes.

Ainsi $\mathrm{SL}(3,\mathbb{Z})$ est engendré par g_1, g_3, g_5, et ces éléments et leurs produits ont des points fixes, donc d'après le corollaire 3.8.6, $\mathrm{SL}(3,\mathbb{Z})$ a un point fixe. Ainsi $\mathrm{SL}(3,\mathbb{Z})$ a la proriété (FA). $\square$

Remarque. Comme $\mathrm{SL}(2,\mathbb{Z}) \simeq \mathbb{Z}/4\mathbb{Z} \star_{\mathbb{Z}/2\mathbb{Z}} \mathbb{Z}/6\mathbb{Z}$, $\mathrm{SL}(2,\mathbb{Z})$ n'a pas la propriété (FA).

Théorème 3.8.10. *Pour tout $n \geqslant 3$, le groupe $\mathrm{SL}(n,\mathbb{Z})$ a la propriété (FA).*

Exercice 20. *Montrer que $\mathrm{SL}(4,\mathbb{Z})$ a la propriété (FA).*

3.9 Théorème de Grushko

Lemme 3.9.1 (Higgins)**.** *Soitent $G = A\star B$ et $G' = A'\star B'$ deux groupes, et soit $\phi : G \to G'$ un morphisme surjectif tel que $\phi(A) = A'$ et $\phi(B) = B'$. Alors pour tout sous-groupe H de G tel que $\phi(H) = G'$, il existe deux sous-groupes $A_H, B_H \subset H$ tels que $H = A_H \star B_H$, $\phi(A_H) = A'$ et $\phi(B_H) = B'$.*

Démonstration. Considérons un arbre Γ, tel que le groupe $G = A\star B$ agisse sans inversion sur Γ, avec pour quotient une arête entre deux sommets distincts. Remarquons que G agit librement sur les arêtes de Γ. De même, considérons un arbre Γ', tel que le groupe $G' = A' \star B'$ agisse sans inversion sur Γ', avec pour quotient une arête entre deux sommets distincts.

Remarquons que H agit sur Γ et sur Γ'. Considérons l'ensemble $\mathcal{T}$ des arbres T munis d'une action sans inversion de H, tel que l'action de H sur les arêtes de T soit libre, et tel qu'il existe des morphismes surjectifs d'arbres $\Gamma \to T \to \Gamma'$ équivariants pour l'action de H. Par exemple, $\Gamma \in \mathcal{T}$.

Alors $\mathcal{T}$ est naturellement muni d'une relation d'ordre, où on déclare que $T \geqslant T'$ s'il existe un morphisme surjectif H-équivariant $T \to T'$. L'ensemble $\mathcal{T}$ est alors inductif : d'après le lemme de Zorn, considérons un élément minimal T.

Nous allons montrer que l'application quotient $H\backslash T \to H\backslash \Gamma'$ est un isomorphisme : si ce n'est pas le cas, alors T a au moins deux H-orbites d'arêtes. Considérons ainsi deux arêtes e, e' de T ayant la même origine, et telles que $H \cdot e \neq H \cdot e'$. Considérons le graphe T' obtenu à partir de T en recollant chaque paire d'arêtes $(h \cdot e, h \cdot e')$, pour $h \in H$. Alors T' est un arbre, et on a $T' \in \mathcal{H}$, ce qui contredit la minimalité de T.

Ainsi l'application quotient $H\backslash T \to H\backslash \Gamma'$ est un isomorphisme. En particulier, $H\backslash T$ a une seule arête, donc il existe deux sous-groupes $A_H, B_H \subset H$ tels que $H = A_H \star B_H$. De plus, comme A_H est le stabilisateur d'un sommet de T, $\phi(A_H)$ est contenu dans le stabilisateur d'un sommet de Γ', donc $\phi(A_H) \subset A$ ou $\phi(A_H) \subset B$. Quitte à les renommer, on peut supposer que $\phi(A_H) \subset A$ et $\phi(B_H) \subset B$. Comme $\phi(H) = G' = A' \star B'$, on en déduit que $\phi(A_H) = A'$ et $\phi(B_H) = B'$. $\square$

Lemme 3.9.2. *Soit F un groupe libre, A et B deux groupes, et $\phi : F \to A \star B$ un morphisme surjectif. Alors il existe des sous-groupes A', B' de F tels que $F \simeq A' \star B'$, et tels que $\phi(A') = A$ et $\phi(B') = B$.*

Démonstration. Notons $S \subset F$ tel que F soit librement engendré par S. Pour tout $s \in S$, écrivons $\phi(s) = a_{s,1}b_{s,1} \dots a_{s,n_s}b_{s,n_s}$ sous la forme d'un mot réduit dans $A \star B$ (éventuellement $a_{s,1} = 1$ ou $b_{s,n_s} = 1$). Soit G le groupe librement engendré par $T = \{a_{s,i}, b_{s,i} \mid s \in S, 1 \leqslant i \leqslant n_s\}$. Notons que le morphisme naturel $F \to G$ qui à $s \in S$ associe $a_{s,1}b_{s,1} \dots a_{s,n_s}b_{s,n_s}$ nous permet de considérer F comme un sous-groupe de G. Par ailleurs, on a un morphisme naturel $G \to A \star B$ qui étend ϕ. Notons A_G (resp. B_G) le sous-groupe de G (librement) engendré par les $\{a_{s,i} \mid s \in S, 1 \leqslant i \leqslant n_s\}$ (resp. par les $\{b_{s,i} \mid s \in S, 1 \leqslant i \leqslant n_s\}$). Alors on a $G = G_A \star G_B$, et de plus $\phi(G_A) \subset A$ et $\phi(G_B) \subset B$. Comme $\phi : G \to A \star B$ est surjectif, on a donc $\phi(G_A) = A$ et $\phi(G_B) = B$.

D'après le lemme précédent appliqué au sous-groupe $F \subset G$, il existe donc deux sous-groupes A', B' de F tels que $F \simeq A' \star B'$, et tels que $\phi(A') = A$ et $\phi(B') = B$. □

Définition 3.9.3. *Si G est un groupe de type fini, son* ***rang*** $\mathrm{rg}(G)$ *est le cardinal minimal d'une partie génératrice de G.*

Théorème 3.9.4 (Grushko)**.** *Soient A, B deux groupes de type fini. Alors* $\mathrm{rg}(A \star B) = \mathrm{rg}(A) + \mathrm{rg}(B)$.

Démonstration. Il est immédiat que $\mathrm{rg}(A \star B) \leqslant rg(A) + \mathrm{rg}(B)$. Réciproquement, considérons F le groupe libre de rang $\mathrm{rg}(A \star B)$. Alors il existe un morphisme surjectif naturel $\phi : F \to A \star B$. D'après le lemme précédent, il existe des sous-groupes A', B' de F tels que $F \simeq A' \star B'$, et tels que $\phi(A') = A$ et $\phi(B') = B$. Comme F est un groupe libre, on a $\mathrm{rg}(F) = \mathrm{rg}(A') + \mathrm{rg}(B')$, donc $\mathrm{rg}(A \star B) = \mathrm{rg}(F) = \mathrm{rg}(A') + \mathrm{rg}(B') \geqslant \mathrm{rg}(A) + \mathrm{rg}(B)$. □

Définition 3.9.5. *On dit qu'un groupe G est* ***librement indécomposable*** *si, pour tous sous-groupes A, B de G tels que $G = A \star B$, on a $A = \{1\}$ ou $B = \{1\}$.*

Exercice 21. *Sont librement indécomposables :*

- *les groupes finis,*
- *les groupes simples,*
- *les groupes ayant un centre non trivial,*
- *les produits directs...*

Théorème 3.9.6 (Décomposition de Grushko)**.** *Soit G un groupe de type fini. Alors G a une décomposition en produit libre $G = G_1 \star \cdots \star G_n \star F$, qui est unique à permutation et conjugaison des facteurs G_i près, telle que chaque groupe G_i est librement indécomposable, et le groupe F est libre.*

Démonstration. On itère le processus de remplacer un groupe non librement indécomposable par un produit libre. Grâce au théorème de Grushko, comme G est de type fini, ce processus s'arrête. Nous admettons l'unicité. □

3.10 Bouts d'un groupe et théorème de Stallings

Définition 3.10.1. *Soit X un espace topologique connexe par arcs, dénombrable à l'infini. Le* ***nombre de bouts*** *de X est la borne supérieure du nombre de composantes connexes par arcs non relativement compactes parmi les complémentaires $X \backslash K$, où K est un compact de X. On le note $e(X) \in \mathbb{N} \cup \{\infty\}$.*

Exemples.

- Si X est compact, alors $e(X) = 0$.
- On a $e([0, +\infty[) = 1$.
- On a $e(\mathbb{R}) = 2$.
- On a $e(\mathbb{R}^2) = 1$.
- Si X est la réunion de p demi-droites attachées en leur origine commune, on a $e(X) = p$.
- Si X est un arbre 3-régulier, alors $e(X) = \infty$.

Définition 3.10.2. *Soit G un groupe de type fini. Si S est un partie génératrice de G, alors le nombre $e(\mathrm{Cay}(G, S))$ ne dépend pas de S : on le note $e(G)$.*

Démonstration. Soit S' une autre partie génératrice finie de G. Supposons que $e(\mathrm{Cay}(G, S')) = e$ est fini, et montrons que $e(\mathrm{Cay}(G, S)) \leqslant e$. Considérons un compact $K' \subset \mathrm{Cay}(G, S)$ tel que $\mathrm{Cay}(G, S') \backslash K'$ ait e composantes connexes non relativement compactes. Pour simplifier, on peut supposer que K' est contenu dans l'ensemble G des sommets de $\mathrm{Cay}(G, S)$.

Comme S' engendre G et que S est finie, il existe un entier $p \geqslant 0$ tel que tout $s \in S$ s'écrive comme produit d'au plus p éléments de $S' \cup S'^{-1}$.

Considérons un ensemble fini $K' \subset K$ de sommets de $\mathrm{Cay}(G, S)$ tel que tout sommet de $G \backslash K$ soit à distance au moins $p + 1$ de K' dans $\mathrm{Cay}(G, S)$.

Considérons une composante connexe par arcs non relativement compacte C de $\mathrm{Cay}(G, S) \backslash K$. Soient x, y deux sommets de C. Nous allons montrer que x et y sont dans la même composante connexe de $\mathrm{Cay}(G, S') \backslash K$. Par définition, il existe $s_1, \ldots, s_n \in S \cup S^{-1}$ tels que $y = xs_1s_2 \ldots s_n$, où pour tout $0 \leqslant i \leqslant n$, on a $x_i = xs_1s_2 \ldots s_i \in C$. Comme la distance entre x_i et x_{i+1} est au plus p dans $\mathrm{Cay}(G, S')$, on en déduit que x_i et x_{i+1} sont dans la même composante connexe de $\mathrm{Cay}(G, S') \backslash K'$. Ainsi x et y sont dans la même composante connexe de $\mathrm{Cay}(G, S') \backslash K'$.

En conclusion, l'espace $\mathrm{Cay}(G, S) \backslash K$ a au plus autant de composantes connexes non bornées que $\mathrm{Cay}(G, S') \backslash K'$. Ainsi $e(\mathrm{Cay}(G, S)) \leqslant e(\mathrm{Cay}(G, S')) = e$. Par symétrie, on a donc $e(\mathrm{Cay}(G, S)) = e(\mathrm{Cay}(G, S'))$. $\square$

Exemples.

- G est un groupe fini si et seulement si $e(G) = 0$.
- On a $e(\mathbb{Z}) = 2$.
- On a $e(\mathbb{Z}^2) = 1$.
- On a $e(\mathbb{F}_2) = \infty$.

Exercice 22. *Soit G un groupe de type fini, et $H < G$ un sous-groupe d'indice fini. Alors $e(G) = e(H)$.*

Remarque. Le nombre $e(G)$ est même un invariant de quasi-isométrie (voir plus loin).

Définition 3.10.3. *On dit qu'un groupe G se* ***décompose*** *au-dessus d'un sous-groupe $F \subset G$ si G est isomorphe à un produit amalgamé $A \star_F B$ ou à un extension HNN $A\star_F$ au-dessus de F.*

Théorème 3.10.4 (Stallings, admis)**.** *Soit G un groupe de type fini. Alors $e(G) \in \{0, 1, 2, \infty\}$. De plus :*

- *$e(G) \geqslant 2$ si et seulement si G se décompose au-dessus d'un groupe fini.*
- *$e(G) = 2$ si et seulement si G a un sous-groupe d'indice fini isomorphe à $\mathbb{Z}$.*

Démonstration. [Sens facile] Supposons que G se décompose au-dessus d'un sous-groupe fini. Pour simplifier, considérons le cas d'un produit amalgamé $G = A \star_F B$. Alors G a une action sans inversion sur un arbre Γ, avec pour quotient une arête. De plus, chaque stabilisateur d'arête est conjugué à F, donc est fini. Considérons une partie génératrice $S = S_A \cup S_B$ de G formée de la réunion de parties génératrices de A et de B. Comme F est fini, nous pouvons de plus supposer que S contient F. Considérons une arête e de Γ dont le stabilisateur soit F. Soient e' et e'' deux arêtes de Γ n'appartenant pas à la même composante connexe de $\Gamma \backslash e$. Soient $g', g'' \in G$ tels que $g' \cdot e = e'$ et $g'' \cdot e = e''$: écrivons $g''^{-1} g' = s_1 \dots s_n$ comme un mot en $S \cup S^{-1}$, avec $n \geqslant 1$ minimal. Alors pour tout $0 \leqslant i \leqslant n-1$, les arêtes $s_1 \dots s_i \cdot e$ et $s_1 \dots s_{i+1} \cdot e$ sont adjacentes, donc il existe $0 \leqslant i \leqslant n-1$ tel que $g'' s_1 \dots s_i \cdot e = e$. Ceci signifie que $g'' s_1 \dots s_i \in F$, donc toute géodésique dans $\mathrm{Cay}(G, S)$ de g' à g'' passe à distance au plus 1 de l'élément neutre de G. En particulier, le complémentaire de la boule de rayon 1 n'est pas connexe : $e(G) \geqslant 2$.

Supposons que G a un sous-groupe d'indice fini isomorphe à $\mathbb{Z}$. Alors comme G et $\mathbb{Z}$ ont le même nombre de bouts, on a $e(G) = e(\mathbb{Z}) = 2$. $\square$

Exemples.

- On a $e(\mathbb{Z}) = 2$, et en effet $\mathbb{Z} \simeq \{1\} \star_{\{1\}}$.
- On a $e(\mathbb{F}_2) = \infty$, et en effet $\mathbb{F}_2 \simeq \mathbb{Z} \star \mathbb{Z}$.
- On a $\mathrm{SL}(2, \mathbb{Z}) \simeq \mathbb{Z}/6\mathbb{Z} \star_{\mathbb{Z}/2\mathbb{Z}} \mathbb{Z}/4\mathbb{Z}$, donc $e(\mathrm{SL}(2, \mathbb{Z})) = \infty$ car $\mathrm{SL}(2, \mathbb{Z})$ n'a pas de sous-groupe d'indice fini isomorphe à $\mathbb{Z}$.
- Si $g \geqslant 1$, alors le groupe fondamental d'une surface de genre g a un bout.

Corollaire 3.10.5. *Si un groupe de type fini G a la propriété (FA), alors G a au plus un bout.*

Démonstration. Si G a la propriété (FA), alors G ne se décompose pas de manière non triviale. Ainsi, d'après le théorème de Stallings, G a au plus un bout. $\square$

Exemple. $\mathrm{SL}(3, \mathbb{Z})$ a un bout.

Définition 3.10.6. *On dit qu'un groupe de type fini avec au plus un bout est 0-**accessible**. De plus, si un groupe G se décompose au-dessus d'un sous-groupe fini avec des facteurs qui sont n-accessibles, on dit que G est $(n+1)$-accessible. On dit que G est* ***accessible*** *s'il est n-accessible pour un entier $n \geqslant 0$.*

Théorème 3.10.7 (Dunwoody, admis)**.** *Un groupe de présentation finie est accessible.*

Chapitre 4

Sous-groupes libres, alternative de Tits

De bonnes références sont [Ben97], [dlH00] et [Löh11].

Dans ce chapitre, on va s'intéresser à la construction de sous-groupes libres, avec en vue le résultat suivant.

Théorème 4.0.8 (Alternative de Tits)**.** *Soit $\mathbb{K}$ un corps de caractéristique nulle, et soit G un sous-groupe de $\mathrm{GL}(n, \mathbb{K})$. Alors :*

- *ou bien G contient un sous-groupe résoluble d'indice fini*
- *ou bien G contient un sous-groupe libre de rang 2.*

4.1 Lemme du ping-pong classique

L'objet de cette partie est de présenter le principal outil géométrique permettant de montrer qu'un groupe est libre, il est dû à Tits :

Lemme 4.1.1 (Lemme du ping-pong)**.** *Soit G un groupe engendré par deux éléments $a, b \in G$. Supposons que G agisse sur un ensemble X, et qu'il existe deux sous-ensembles disjoints non vides $A, B \subset X$ tels que :*

$$\forall n \in \mathbb{Z}\backslash\{0\}, a^n \cdot B \subset A \text{ et } b^n \cdot A \subset B.$$

Alors G est librement engendré par $\{a, b\}$.

Démonstration. Supposons par l'absurde qu'il existe un mot $w \in \mathbb{F}(a, b)$ non vide tel que $\overline{w}^G = 1$. Ecrivons w sous forme normale : $w = a^{n_1} b^{m_1} a^{n_2} \dots b^{m_p}$.

Quitte à conjuguer w par une puissance de a ou de b, on peut supposer que $n_1 \neq 0$ et $m_p \neq 0$. Choisissons alors $x \in A$. Nous avons $b^{m_p} \cdot x \in B$, puis $a^{n_p} b^{m_p} \cdot x \in A$, etc. Par une récurrence immédiate, on obtient $w \cdot x = a^{n_1} b^{m_1} a^{n_2} \dots b^{m_p} \cdot x \in A$. Or on devrait avoir $w \cdot x = x \in B$, ce qui contredit le fait que A et B sont disjoints.

Ainsi G est librement engendré par $\{a, b\}$. □

Exemple. Considérons le sous-groupe G de $\mathrm{SL}(2,\mathbb{R})$ engendré par $a = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ et $b = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$. Alors G est librement engendré par $\{a,b\}$.

Pour voir cela, considérons l'action linéaire de $\mathrm{SL}(2,\mathbb{R})$ sur $X = \mathbb{R}^2$, et considérons les sous-ensembles disjoints

$$A = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in X \ \mid \ |x| > |y| \right\} \text{ et } B = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in X \ \mid \ |x| < |y| \right\}.$$

Alors, pour tout $n \in \mathbb{Z}\backslash\{0\}$, on a bien $a^n \cdot B \subset A$ et $b^n \cdot A \subset B$.

D'après le lemme du ping-pong, G est librement engendré par $\{a,b\}$.

Exercice 23. *Soit $z \in \mathbb{C}$ et G_z le sous-groupe de* $\mathrm{SL}(2,\mathbb{C})$ *engendré par* $a = \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix}$ *et* $b = \begin{pmatrix} 1 & 0 \\ z & 1 \end{pmatrix}$.

Montrer que si $|z| \geqslant 2$, alors G_z est librement engendré par $\{a,b\}$.

Montrer que si z est transcendant, alors G_z est librement engendré par $\{a,b\}$.

On peut déduire de ce lemme du ping-pong un critère pour montrer qu'un produit est libre. Nous en laissons la preuve en **Exercice**.

Lemme 4.1.2 (Lemme du ping pong pour les produits libres)**.** *Soit G un groupe engendré par deux sous-groupes A, B. Supposons que G agisse sur un ensemble X, et qu'il existe deux sous-ensembles disjoints non vides $X_A, X_B \subset X$ tels que :*

$$\forall a \in A\backslash\{1\}, a \cdot X_B \subset X_A \text{ et } \forall b \in B\backslash\{1\}, b \cdot X_A \subset X_B.$$

Alors G est le produit libre de A et B.

Corollaire 4.1.3. *Le groupe* $\mathrm{PSL}(2,\mathbb{Z})$ *est isomorphe au produit libre* $\mathbb{Z}/2\mathbb{Z} \star \mathbb{Z}/3\mathbb{Z}$.

Démonstration. Considérons l'action de $\mathrm{PSL}(2,\mathbb{Z})$ sur $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$ par homographies :

$$\forall g = \left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right] \in \mathrm{PSL}(2,\mathbb{Z}), \forall z \in \mathbb{P}^1(\mathbb{Q}), g \cdot z = \frac{az+b}{cz+d}.$$

Considérons les classes d'homothéties a et b des matrices $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $\begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$. Notons $c = ba = \left[\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right] \in G$.

Première étape : Montrons que $\mathrm{PSL}(2,\mathbb{Z})$ est engendré par $\{a,b\}$. Notons G le sous-groupe de $\mathrm{PSL}(2,\mathbb{Z})$ engendré par $\{a,b\}$, et supposons par l'absurde qu'il existe $g \in \mathrm{PSL}(2,\mathbb{Z})\backslash G$. Supposons de plus que $g \in \mathrm{PSL}(2,\mathbb{Z})\backslash G$ soit tel que $g \cdot 0 = \frac{p}{q} \in \mathbb{P}^1(\mathbb{Q})$ soit tel que $|q|$ soit minimal et non nul. Notons qu'on peut supposer $g \cdot 0 \neq \infty$ grâce à l'action de a. Nous allons montrer que $g \cdot 0 = 0$. Supposons donc que $p \neq 0$.

Si $|q| > |p|$, alors $ag \cdot 0 = \frac{-q}{p}$ a un dénominateur de valeur absolue inférieure, ce qui contredit la minimalité de $|q|$. On a donc $|q| \leqslant |p|$.

Comme $p \neq 0$, considérons $n \in \mathbb{Z}$ tel que $|p+nq| < |q|$. Alors $ac^n g \cdot 0 = \frac{-q}{p+nq}$, ce qui contredit la minimalité de $|q|$.

En conclusion, on a $p = 0$, d'où $g \cdot 0 = 0$. Ainsi g a pour coefficients $g = \left[\begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix}\right]$, où $x \in \mathbb{Z}$. Or $aga = c^{-x}$, donc $g \in H$. Ceci prouve que $\mathrm{PSL}(2,\mathbb{Z}) = G$ est engendré par $\{a, b\}$.

Deuxième étape : Montrons que $\mathrm{PSL}(2,\mathbb{Z})$ est le produit libre des sous-groupes A et B engendrés par a et b. Notons que $a^2 = b^3 = 1$, donc $A \simeq \mathbb{Z}/2\mathbb{Z}$ et $B \simeq \mathbb{Z}/3\mathbb{Z}$.

Considérons l'ensemble $X = \mathbb{P}^1(\mathbb{Q})$, et les sous-ensembles disjoints $X_A = \mathbb{Q} \cap]-\infty, 0[$ et $X_B = \mathbb{Q} \cap]0, +\infty[$. Alors, pour tout $z \in X_B$, on a $z > 0$ donc $a \cdot z = \frac{-1}{z} \in X_A$. Et si $z \in X_A$, alors $z < 0$ donc $b \cdot z = 1 - \frac{1}{z} > 1$ donc $b \cdot z \in X_A$. Enfin si $z \in X_A$, alors $z < 0$ donc $b^2 \cdot z = \frac{-1}{z-1} > 0$ donc $b^2 \cdot z \in X_B$.

D'après le lemme du ping-pong pour les produits libres, on en déduit que $\mathrm{PSL}(2,\mathbb{Z}) \simeq A \star B \simeq \mathbb{Z}/2\mathbb{Z} \star \mathbb{Z}/3\mathbb{Z}$. □

Corollaire 4.1.4. *Le groupe* $\mathrm{PSL}(2,\mathbb{Z})$ *agit sans inversion sur un arbre* $(2,3)$*-birégulier, avec pour quotient une arête.*

4.2 Lemme du ping-pong dynamique

Pour obtenir des éléments a et b auxquels on pourra appliquer le lemme du ping-pong, on a souvent recours à un critère dynamique.

Définition 4.2.1. *Soit g un homéomorphisme d'un espace métrisable compact X. On dit que g a une* ***dynamique Nord-Sud*** *s'il existe un point attractif $x_g^+ \in X$ et un bassin d'attraction ouvert $B_g^+ \subset X$ tels que*

$$\forall x \in B_g^+, \lim_{n \to +\infty} g^n \cdot x = x_g^+.$$

Lemme 4.2.2. *Soit $g \in \mathrm{SL}(2,\mathbb{R})$ diagonalisable sur $\mathbb{R}$, avec des valeurs propres λ, λ^{-1} telles que $\lambda > 1$. Alors l'action de g par homographies sur $\mathbb{P}^1(\mathbb{R}) = \mathbb{R} \cup \{\infty\}$ a une dynamique Nord-Sud.*

Démonstration. Notons $v^+, v^- \in \mathbb{R}^2$ des vecteurs propres associés aux valeurs propres λ, λ^{-1}. Alors v^+, v^- définissent d'uniques points $x_g^+, x_g^- \in \mathbb{P}^1(\mathbb{R})$. Montrons que g a pour point attractif x_g^+ et pour bassin d'attraction $B_g^+ = \mathbb{P}^1(\mathbb{R}) \setminus \{x_g^-\}$. Soit $x \in B_g^+$. Alors x représente un vecteur $v \in \mathbb{R}^2$ non colinéaire à v^-. Ecrivons $v = av^+ + bv^-$, où $a, b \in \mathbb{R}$ avec $a \neq 0$. Dans ce cas, on a $g^n \cdot v = a\lambda^n v^+ + b\lambda^{-n} v^-$, donc on déduit que $g^n \cdot x \to_{n \to +\infty} x_g^+$. □

Lemme 4.2.3 (Lemme du ping-pong dynamique)**.** *Soit G un groupe contenant deux éléments $a, b \in G$. Supposons que G agisse par homéomorphismes sur un espace métrisable compact X tel que, si on note $S = \{a, b, a^{-1}, b^{-1}\}$, alors :*

- *pour tout $g \in S$, g a une dynamique Nord-Sud avec un point attractif $x_g^+ \in X$ et un bassin d'attraction B_g^+,*
- *les points $\{x_g^+, g \in S\}$ sont distincts et l'intersection $\bigcap_{g \in S} B_g^+$ est non vide,*

- *pour tous $g, h \in S$ tel que $g \neq h^{-1}$, $x_h^+ \in B_g^+$.*

Alors il existe un entier $p > 0$ tel que le groupe engendré par $\{a^p, b^p\}$ soit libre.

Démonstration. Fixons un point $x \in \bigcap_{g \in S} B_g^+$, qu'on peut supposer distinct des $\{x_g^+, g \in S\}$. Pour tout $g \in S$, choisissons un voisinage compact K_g^+ de x_g^+ ne contenant pas x tel que, si $h \neq g^{-1}$, alors $K_g^+ \subset B_h^+$. On peut de plus supposer les K_g^+ disjoints, pour $g \in S$.

Notons $A = K_a^+ \cup K_{a^{-1}}^+$ et $B = K_b^+ \cup K_{b^{-1}}^+$. Comme A est compact et inclus dans K_b^+, il existe un entier $p_b > 0$ tel que $\forall n \geqslant p_b, b^n \cdot A \subset K_b^+$. On peut donc trouver un entier $p > 0$ tel que, pour tout $n \in \mathbb{Z}$ tel que $|n| \geqslant p$, on a $b^n \cdot A \subset B$ et $a^n \cdot B \subset A$.

On peut alors appliquer le lemme du ping-pong au sous-groupe de G engendré par a^p et b^p, pour montrer que le groupe engendré par $\{a^p, b^p\}$ est libre. $\square$

Corollaire 4.2.4. *Soit G un sous-groupe de $\mathrm{SL}(2, \mathbb{R})$ engendré par deux matrices a, b diagonalisables sur $\mathbb{R}$, de valeurs propres différentes de ± 1, tel que G ne stabilise pas de droite de $\mathbb{R}^2$. Alors il existe un entier $p > 0$ tel que le sous-groupe engendré par a^p et b^p soit libre.*

Démonstration. On considère l'action de G par homographies sur $\mathbb{P}^1(\mathbb{R})$. D'après le lemme, $a^{\pm}$ et $b^{\pm}$ ont des dynamiques Nord-Sud, avec des points d'attractions distincts car G ne stabilise pas de droite de $\mathbb{R}^2$. De plus, l'intersection des bassins d'attractions est $\mathbb{P}^1(\mathbb{R})$ privé de 4 points donc est non vide. Ainsi, d'après le lemme du ping-pong dynamique, il existe un entier $p > 0$ tel que le sous-groupe engendré par a^p et b^p soit libre. $\square$

4.3 Lemme de Selberg

Définition 4.3.1. *Soit P une propriété. On dit qu'un groupe G est **virtuellement** P si G a un sous-groupe d'indice fini qui est P.*

L'objet de cette partie est de montrer le résultat suivant, dont les arguments serviront également dans la preuve de l'alternative de Tits.

Théorème 4.3.2 (Lemme de Selberg). *Soit $\mathbb{K}$ un corps de caractéristique nulle, et $n \geqslant 1$. Tout sous-groupe de type fini de $\mathrm{GL}(n, \mathbb{K})$ est virtuellement sans torsion.*

Définition 4.3.3. *Un élément $g \in \mathrm{GL}(n, \mathbb{K})$ est dit **unipotent** si sa seule valeur propre est 1. Il est dit **virtuellement unipotent** s'il existe $k \in \mathbb{N}^*$ tel que g^k soit unipotent.*

Le Lemme de Selberg découle du résultat suivant.

Proposition 4.3.4. *Soit $\mathbb{K}$ un corps de caractéristique nulle, et $n \geqslant 1$. Soit G un sous-groupe de type fini de $\mathrm{GL}(n, \mathbb{K})$. Alors G contient un sous-groupe d'indice fini G' tel que tout élément de G' qui est virtuellement nilpotent est nilpotent.*

Démonstration. [Proposition implique Lemme de Selberg] Soit G un sous-groupe de type fini de $\mathrm{GL}(n, \mathbb{K})$. Soit G' le sous-groupe d'indice fini de G donné par la proposition précédente. Soit $g \in G'$ un élément d'ordre fini : il existe $k \in \mathbb{N}^*$ tel que $g^k = 1$, donc g est virtuellement unipotent. Par hypothèse sur G', g' est nilpotent. Ainsi g' est diagonalisable, et sa seule valeur propre est 1 : $g = 1$. Donc G' est sans torsion. $\square$

Démonstration. [Proposition 4.3.4]

- Premier cas : $\mathbb{K} = \mathbb{Q}$. Soit $E \subset \mathbb{N}^*$ une partie finie contenant les dénominateurs des coefficients des éléments d'une partie génératice finie de G et de leurs inverses. Soit $s \in \mathbb{N}^*$ le produit des éléments de E, et $A = \mathbb{Z}[\frac{1}{s}]$. Alors G est inclus dans le groupe $G_0 = \mathrm{GL}(n, A)$: on va montrer le résultat pour G_0.

  Soit p un nombre premier supérieur à $2n$ et à s. Le morphisme surjectif $A \to \mathbb{Z}/p\mathbb{Z}$ induit un morphisme de groupes $G_0 \to \mathrm{GL}(n, \mathbb{Z}/p\mathbb{Z})$. Notons G_0' le noyau de ce morphisme, il est d'indice fini dans G_0, nous allons montrer qu'il convient.

  Soit $g \in G_0'$ un élément virtuellement unipotent. Etudions la trace de g :

  - $\mathrm{tr}(g)$ est une somme de racines n èmes de l'unité, c'est donc un entier algébrique de A. Or les seuls entiers algébriques de $A = \mathbb{Z}[\frac{1}{s}]$ sont $\mathbb{Z}$, donc $\mathrm{tr}(g) \in \mathbb{Z}$.
  - $\mathrm{tr}(g)$ est une somme de n racines de l'unité, donc $|\,\mathrm{tr}(g)| \leqslant n$.
  - $\mathrm{tr}(g) - n = \mathrm{tr}(g - 1)$ est un multiple de p dans A. Donc $\mathrm{tr}(g) \in n + p\mathbb{Z}$.

  Ainsi $\mathrm{tr}(g) = n$: toutes les valeurs propres de g sont égales à 1, donc g est unipotent.

- Deuxième cas : $\mathbb{K} = \mathbb{Q}(X_1, \ldots, x_r)$. On procède de même : il existe un polynôme non nul $s \in \mathbb{Z}[X_1, \ldots, X_r]$ tel que G est inclus dans $G_0 = \mathrm{GL}(n, A)$, où $A = \mathbb{Z}[X_1, \ldots, X_r, s^{-1}]$. Soit p un nombre premier tel que $p > 2n$ et $s \not\equiv 0[p]$. Notons $\overline{\mathbb{Z}/p\mathbb{Z}}$ la clôture algébrique de $\mathbb{Z}/p\mathbb{Z}$, et soit $(a_1, \ldots, a_r) \in \overline{\mathbb{Z}/p\mathbb{Z}}^r$ tel que $s(a_1, \ldots, a_r) \neq 0$. La surjection de A sur le corps fini $A_p = \overline{\mathbb{Z}/p\mathbb{Z}}[a_1, \ldots, a_r]$ qui à X_i associe a_i induit un morphisme de groupes de G_0 sur $\mathrm{GL}(n, A_p)$: notons G_0' son noyau, il est d'indice fini. Comme ci-dessus, on montre que G_0' convient.

- Soient $y_1, \ldots, y_d$ les coefficients d'une famille finie de générateurs de G. On a $G \subset \mathrm{GL}(n, \mathbb{Q}(y_1, \ldots, y_d))$, on peut donc supposer que $\mathbb{K}$ est de type fini. Soit $(x_1, \ldots, x_r)$ une famille maximale algébriquement indépendante de $\mathbb{K}$. Alors $\mathbb{K}$ est une extension finie de degré d du corps $\mathbb{F} = \mathbb{Q}(x_1, \ldots, x_r)$. Comme $\mathbb{K}^n$ est un espace vectoriel de dimension n sur $\mathbb{K}$, c'est aussi un espace vectoriel de dimension dn sur $\mathbb{F}$, d'où $G \subset \mathrm{GL}(nd, \mathbb{F})$. Le cas précédent permet de conclure.

□

Proposition 4.3.5. *Soit $\mathbb{K}$ un corps de caractéristique nulle, et $n \geqslant 1$. Soit G un sous-groupe de type fini de $\mathrm{GL}(n, \mathbb{K})$ tel que tout élément de G est virtuellement unipotent. Alors G est virtuellement nilpotent.*

Démonstration. D'après la proposition 4.3.4, considérons un tel sous-groupe G' d'indice fini. Alors tous les éléments de G' sont unipotents. D'apès le théorème d'Engel, dans une base adaptée de $\mathbb{K}^n$, tous les éléments de G' sont triangulaires supérieurs. Or les seuls éléments triangulaires supérieurs unipotents ont des 1 sur la diagonale. Ainsi G' est nilpotent. □

4.4 Corps locaux

Définition 4.4.1. *Soit $\mathbb{K}$ un corps, on dit que $|\cdot| : \mathbb{K} \to \mathbb{R}_+$ est une valeur absolue si*

- $\forall x \in \mathbb{K}, |x| = 0 \Longrightarrow x = 0,$

- *$\forall x, y \in \mathbb{K}, |xy| = |x||y|$ et*
- *$\forall x, y \in \mathbb{K}, |x+y| \leqslant |x| + |y|$.*

*On appelle $(\mathbb{K}, \|\cdot\|)$ un **corps valué**.*

*On dit que $\mathbb{K}$ est un **corps local** s'il est localement compact et complet pour cette valeur absolue.*

Exemples.

- $(\mathbb{R}, |\cdot|)$ et $(\mathbb{C}, |\cdot|)$ sont des corps locaux, appelés corps locaux archimédiens.
- Soit p un nombre premier. Alors $\mathbb{Q}_p = \{\sum_{n \geqslant n_0} a_n p^n, n_0 \in \mathbb{Z}, a_n \in \{0, 1, \ldots, p-1\}\}$ est un corps de caractéristique 0, et $|\sum_{n \geqslant n_0} a_n p^n| = p^{-n_0}$ (si n_0 est maximal) définit une valeur absolue qui en fait un corps local, appelé ultramétrique.
- Soit p un nombre premier. Alors $\mathbb{F}_p((t)) = \{\sum_{n \geqslant n_0} a_n t^n, n_0 \in \mathbb{Z}, a_n \in \mathbb{Z}/p\mathbb{Z}\}$ est un corps de caractéristique p, et $|\sum_{n \geqslant n_0} a_n t^n| = p^{-n_0}$ (si n_0 est maximal) définit une valeur absolue qui en fait un corps local, appelé ultramétrique.

Proposition 4.4.2. *Soit $\mathbb{K}$ une extension de type fini de $\mathbb{Q}$ et $\alpha \in \mathbb{K}$ qui n'est pas une racine de l'unité. Alors il existe un corps local $\mathbb{K}'$ et un morphisme de corps injectif $\mathbb{K} \to \mathbb{K}'$ tel que $|\alpha| > 1$.*

Démonstration. [Cas particulier] Si $\mathbb{K} = \mathbb{Q}(\alpha)$, avec α transcendant sur $\mathbb{Q}$, il existe un morphisme injectif f de $\mathbb{K}$ dans $\mathbb{C}$ avec $|f(\alpha)| > 1$. $\square$

4.5 Elements proximaux

Définition 4.5.1. *Soit $\mathbb{K}$ un corps valué, V un espace vectoriel sur $\mathbb{K}$, et $g \in GL(V)$. On dit que g est **proximal** sur V si g a une unique valeur propre de valeur absolue maximale, de multiplicité 1.*

Lemme 4.5.2. *Notons V_g^+ la somme des sous-espaces caractéristiques de V associés aux valeurs propres de g valeur absolue maximale. Soit V_g^- la somme des sous-espaces caractéristiques de V associés aux autres valeurs propres de g.*

L'élément g est proximal sur V si et seulement si g a une dynamique Nord-Sud sur $\mathbb{P}(V)$, avec point attractif $x_g^+ = V_g^+$ et pour bassin d'attraction $B_g^+ = \mathbb{P}(V) \setminus V_g^-$.

Démonstration. Supposons g proximal. Soit $x \in B_g^+$. Alors x représente un vecteur $v \in V \setminus V_g^-$. Ecrivons $v = v_g^+ + v_g^-$, où $v_g^+ \in V_g^+ \setminus \{0\}$ et $v_g^- \in V_g^-$. Dans ce cas, on a $g^n \cdot v = \alpha^n v_g^+ + w_n$, avec $w_n = o(\alpha^n)$. Ainsi $g^n \cdot x \to_{n \to +\infty} x_g^+$, donc g a une dynamique Nord-Sud.

Réciproquement, si g a une dynamique Nord-Sud, montrons que $\dim V_g^+ = 1$. Sinon, considérons un vecteur propre $v \in V_g^+ \cap B_g^+$ non colinéaire à x_g^+. Alors $g^n \cdot \mathbb{K}v = \mathbb{K}v$ ne converge pas vers x_g^+ lorsque n tend vers $+\infty$: contradiction. $\square$

Lemme 4.5.3. *Soit $g \in \mathrm{GL}(V)$, notons $p = \dim V_g^+$. Alors l'élément $\Lambda^p g$ est proximal sur $\Lambda^p V$.*

Démonstration. Si $\lambda_1, \ldots, \lambda_n$ sont les n valeurs propres de g (avec multiplicité), alors les valeurs propres de $\Lambda^p g$ sont les $\prod_{i \in E} \lambda_i$, où E est un sous-ensemble de $\{1, \ldots, n\}$ de cardinalité p. Ainsi $\Lambda^p g$ a une unique valeur propre de valeur absolue maximale. $\square$

Lemme 4.5.4. *Soit $g \in \mathrm{GL}(V)$. Alors g est proximal sur V si et seulement s'il existe une suite $(c_n)_{n\in\mathbb{N}} \in \mathbb{K}^{\mathbb{N}}$ telle que la suite $(c_n g^n)_{n\in\mathbb{N}}$ converge dans $\mathrm{End}(V)$ vers un projecteur π de rang 1.*

Démonstration. Supposons g proximal, de valeur propre maximale α. Alors $\frac{1}{\alpha^n} g^n$ converge vers le projecteur de rang 1 sur V_g^+ parallèlement à V_g^-.

Réciproquement, supposons que $(c_n g^n)_{n\in\mathbb{N}}$ converge dans $\mathrm{End}(V)$ vers un projecteur π de rang 1. Soit $v \in V$ un vecteur propre de g associé à une valeur propre α de valeur absolue maximale. Alors $c_n g^n(v) = c_n \alpha^n v \to \pi(v)$. Ainsi $c_n \alpha^n \to 1$, et $v \in \mathrm{Im}\,\pi$. Ainsi $\dim V_g^+ = 1$, g est proximal. $\square$

Proposition 4.5.5. *Soit V un $\mathbb{K}$-espace vectoriel de dimension au moins 2. Soit G un sous-groupe irréductible de $\mathrm{GL}(V)$ qui contient un élément proximal dans V.*

- *Il existe $\gamma \in G$ tel que γ et γ^{-1} sont proximaux dans V.*
- *G contient un sous-groupe libre à deux générateurs.*

Démonstration.

- Soit $g \in G$ un élément proximal. Soient $(c_n)_{n\in\mathbb{N}} \in \mathbb{K}^{\mathbb{N}}$, $(d_n)_{n\in\mathbb{N}} \in \mathbb{K}^{\mathbb{N}}$ deux suites telles que $c_n g^n \to \pi$ un projecteur de rang 1, et $d_n g^{-n} \to \sigma$, où σ est un endomorphisme non nul de V.

  Par irréducibilité, considérons $h \in G$ tel que $h(\mathrm{Im}\,\sigma) \not\subset \mathrm{Ker}\,\pi$ et $h^{-1}(\mathrm{Im}\,\sigma) \not\subset \mathrm{Ker}\,\pi$.

  Soit $g_n = g^n h g^{-n}$. Alors $c_n d_n g_n \to \pi h \sigma$, qui est un endomorphisme de rang au plus 1. Or $h\sigma(\mathrm{Im}\,\pi) \subsetneq \mathrm{Ker}\,\pi$, donc cet endomorphisme est non nul : c'est un multiple d'un projecteur de rang 1. Ainsi, si n est assez grand, g_n est proximal dans V. De même, g_n^{-1} est proximal. Posons, pour n assez grand, $\gamma = g_n$.

- Par irréducibilité, il existe $f \in G$ tel que $f^{\pm 1} \cdot V_{\gamma^{\pm 1}}^+ \not\subset V_{\gamma^{\pm 1}}^-$. D'après le lemme du ping-pong dynamique, il existe un entier $p > 0$ tel que γ^p et $f\gamma^p f^{-1}$ engendrent un sous-groupe libre de G.

$\square$

4.6 L'alternative de Tits

L'objet de cette partie est de donner une preuve du résultat suivant.

Théorème 4.6.1 (Alternative de Tits)**.** *Soit $\mathbb{K}$ un corps de caractéristique nulle, et soit G un sous-groupe de $\mathrm{GL}(n, \mathbb{K})$. Alors :*

- *ou bien G est virtuellement résoluble,*
- *ou bien G contient un sous-groupe libre de rang 2.*

Remarquons tout d'abord que les deux possibilités sont mutuellement exclusives : si G contient un sous-groupe d'indice fini résoluble G_0 et un sous-groupe libre de rang 2 F, alors $F \cap G_0$ est un groupe libre non abélien résoluble, ce qui n'existe pas.

Nous allons supposer que G ne contient pas de sous-groupe résoluble d'indice fini, et en déduire que G contient un sous-groupe libre de rang 2.

On peut supposer que G est de type fini. On peut donc également supposer que $\mathbb{K}$ est une extension de type fini de $\mathbb{Q}$.

On peut supposer que l'action de G sur $\mathbb{K}^n$ est irréductible. Alors l'action du sous-groupe dérivé $D(G)$ sur $V = \mathbb{K}^n$ est aussi irréductible.

Comme $D(G)$ n'est pas virtuellement résoluble, il n'est pas virtuellement nilpotent, donc d'après la Proposition 4.3.5, il existe $g \in D(G)$ qui ne soit pas virtuellement unipotent. Ainsi il existe une valeur propre $\alpha \in \overline{\mathbb{K}}$ de g qui n'est pas une racine de l'unité.

D'après la Proposition 4.4.2, il existe une injection de $\mathbb{K}$ dans un corps local $\mathbb{K}'$ muni d'une valeur absolue $|\cdot|$ telle que $|\alpha| > 1$. Remplaçons alors $\mathbb{K}$ par $\mathbb{K}'$.

D'après le Lemme 4.5.3, si on note $p \geqslant 1$ la multiplicité des valeurs propres de g de valeur absolue maximale, alors l'élément $\Lambda^p g$ a une action proximale sur $W = \Lambda^p V$. Quitte à remplacer W par un sous-quotient G-invariant, on peut supposer que l'action de G sur W est irréductible, et que $\Lambda^p g$ a une unique valeur propre de valeur absolue maximale, $|\alpha|^p$.

Comme $\Lambda^p g$ a une valeur propre de valeur absolue supérieure à 1, et que $g \in D(G)$ donc $\Lambda^p g$ est de déterminant 1, on déduit que $\dim W \geqslant 2$. D'après la Proposition 4.5.5, on conclut que G contient un sous-groupe libre de rang 2.

Chapitre 5

Les groupes hyperboliques

Dans partie, nous allons donner une introduction aux groupes hyperboliques au sens de Gromov. De bonnes références sont [GdlH90], [BH99], [Löh11] et [CdV97].

5.1 Le plan hyperbolique réel

Dans cette section, nous commençons par décrire brièvement le plan hyperbolique réel, à travers le modèle du demi-plan de Poincaré.

Définition 5.1.1. *Le plan hyperbolique réel $\mathbb{H}^2$ est, à isométrie près, la seule surface simplement connexe munie d'une métrique riemannienne de courbure sectionnelle constante égale à -1.*

Définition 5.1.2 (Modèle du demi-plan supérieur)**.** *Notons $\mathbb{H}^2 = \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$ le **demi-plan de Poincaré**. Si $f : [0,1] \to \mathbb{H}^2$ est une fonction C^1 par morceaux, posons*

$$\ell(f) = \int_0^1 \frac{|f'(t)|}{\mathrm{Im}(f(t))} dt.$$

Si $z, w \in \mathbb{H}^2$, notons

$$d(z,w) = \inf_{f \mid f(0)=z, f(1)=w} \ell(f).$$

Alors $(\mathbb{H}^2, d)$ est le plan hyperbolique réel.

Proposition 5.1.3. *Si $z, w \in \mathbb{H}^2$, il existe un unique chemin de z à w de longueur minimale, on l'appelle **segment géodésique**. Ce sont des segments de **droites géodésiques**, qui sont :*

- *les demi-droites perpendiculaires à l'axe réel et*
- *les demi-cercles perpendiculaires à l'axe réel.*

Définition 5.1.4. *Le **bord à l'infini** de $\mathbb{H}^2$ est le cercle $\partial\mathbb{H}^2 = \mathbb{R} \cup \{\infty\}$.*

Proposition 5.1.5. *Soient $z, w \in \mathbb{H}^2$ distincts, et considérons la droite géodésique passant par z et w : ses extrémités sont $\alpha, \beta \in \mathbb{R} \cup \{\infty\}$. Alors*

$$d(z,w) = |\log([z : w : \alpha : \beta])|.$$

Proposition 5.1.6. *Soient $u, v, w \in \mathbb{H}^2$. Alors tout point de la géodésique $[u, w]$ est à distance au plus* $\log(2)$ *d'un point de $[u, v] \cup [v, w]$.*

Proposition 5.1.7. *Soient $r, r' : [0, +\infty[\to \mathbb{H}^2$ deux rayons géodésiques de même extrémité dans $\partial\mathbb{H}^2$. Alors $\lim\limits_{t\to+\infty} d(r(t), r') = 0$.*

Théorème 5.1.8. *Le groupe des isométries préservant l'orientation de $\mathbb{H}^2$ est* $\mathrm{PSL}(2, \mathbb{R})$*, agissant sur $\mathbb{H}^2$ par homographies. Soit $g \in \mathrm{PSL}(2, \mathbb{R})\backslash\{1\}$, alors il y a 3 possibilités, mutuellement exclusives :*

- *soit g a un unique point fixe $z \in \mathbb{H}^2$. Dans ce cas, $|\operatorname{tr}(g)| < 2$, g est conjugué à $\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$, et g est une rotation autour de z. g est appelé **elliptique**.*
- *soit g a un unique point fixe $\alpha \in \partial\mathbb{H}^2$. Dans ce cas, $|\operatorname{tr}(g)| = 2$ et g est conjugué à $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$. g est appelé **parabolique**.*
- *soit g a deux points fixes $\alpha^-, \alpha^+ \in \partial\mathbb{H}^2$. Dans ce cas, $|\operatorname{tr}(g)| > 2$, g est conjugué à $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$ et g translate la géodésique de α^- à α^+ de la longueur $2\log\lambda$. g est appelé **loxodromique**.*

Remarque. On peut définir de même l'espace hyperbolique réel de dimension 3, avec pour modèle $\mathbb{H}^3 = \mathbb{C} \times \mathbb{R}_+^*$, pour bord $\partial\mathbb{H}^3 = \mathbb{C} \cup \{\infty\}$ et pour groupes d'isométries $\mathrm{PSL}(2, \mathbb{C})$.

5.2 Espaces Gromov-hyperboliques, quasigéodésiques

Définition 5.2.1. *Soit X un espace métrique géodésique. On dit que X est **Gromov-hyperbolique** s'il existe un réel $\delta \geqslant 0$ tel que, pour tous $x, y, z \in X$ et pour tous segments géodésiques $[x, y], [y, z], [x, z]$, on ait que tout point de $[x, z]$ soit à distance au plus δ d'un point de $[x, y] \cup [y, z]$.*

Exemples.

- La droite $\mathbb{R}$ est Gromov-hyperbolique.
- Le plan hyperbolique réel est Gromov-hyperbolique.
- L'espace hyperbolique réel est Gromov-hyperbolique.
- Tout arbre est Gromov-hyperbolique (avec $\delta = 0$).
- Tout espace borné est Gromov-hyperbolique.

Définition 5.2.2. *Soient (X, d_X) et (Y, d_Y) deux espaces métriques. Une application $f : X \to Y$ est appelée **plongement quasi-isométrique** s'il existe des constantes $K \geqslant 1, C \geqslant 0$ telles que*

$$\forall x, x' \in X, \frac{1}{K} d_X(x, x') - C \leqslant d_Y(f(x), f(x')) \leqslant K d_X(x, x') + C.$$

*Une telle application f est appelée **quasi-isométrie** si de plus*

$$\forall y \in Y, \exists x \in X, d_Y(y, f(x)) \leqslant C.$$

Exercice 24. *Si X est quasi-isométrique à Y, alors Y est quasi-isométrique à X.*

Exemples.

- L'inclusion $\mathbb{Z} \to \mathbb{R}$ est une quasi-isométrie.
- L'inclusion $\mathbb{Z} \to \mathbb{R}^2$ est un plongement quasi-isométrique.
- Une géodésique dans un arbre ou dans le plan hyperbolique, vue comme application $\mathbb{R} \to X$, est un plongement quasi-isométrique.
- Si X et Y sont bornés, alors X et Y sont quasi-isométriques.
- Soit G un groupe de type fini, et soient S, S' deux parties génératrices finies. Alors $\mathrm{Cay}(G, S)$ et $\mathrm{Cay}(G, S')$ sont quasi-isométriques. On peut donc parler de la classe de quasi-isométrie de G.
- Si H est un sous-groupe d'indice fini de G, ou bien un quotient de noyau fini de G, alors G est Gromov-hyperbolique si et seulement si H est Gromov-hyperbolique.

Définition 5.2.3. *Soit X un espace métrique. Une (K, C)-**quasi-géodésique** de X est un plongement (K, C)-quasi-isométrique d'un intervalle de $\mathbb{R}$.*

Théorème 5.2.4. *Soit X un espace métrique géodésique δ-hyperbolique. Pour tous (K, C), il existe une constante $D \geqslant 0$ telle que tout segment (K, C)-quasi-géodésique soit à distance de Hausdorff au plus D d'un segment géodésique.*

Exemples.

- Dans un arbre, une quasi-géodésique reste à distance bornée d'une géodésique.
- Dans $\mathbb{R}^2$, l'application $f : \mathbb{R}^+ \to \mathbb{R}^2$ qui à t associe $f(t) = (t, \sqrt{t})$ est une $(\sqrt{2}, 1)$-quasi-géodésique qui n'est pas à distance bornée d'une demi-droite.

Corollaire 5.2.5. *Soient X, Y deux espaces métriques géodésiques qui sont quasi-isométriques. Si X est Gromov-hyperbolique, alors Y est Gromov-hyperbolique.*

Démonstration. Considérons un triangle géodésique $[a, b], [b, c], [a, c]$ dans Y, et soit $d \in [a, c]$. Considérons $f : Y \to X$ une (K, C)-quasi-isométrie. Soient $x, y, z \in X$ tels que $d(x, f(a)) \leqslant C$, $d(y, f(b)) \leqslant C$ et $d(z, f(c)) \leqslant C$.

Comme l'image par f de $[a, c]$ est une quasi-géodésique, il existe $u \in [x, z]$ tel que $d(f(d), u) \leqslant D$. Comme X est hyperbolique, il existe $v \in [x, y] \cup [y, z]$ tel que $d(v, u) \leqslant \delta$, par exemple $v \in [x, y]$.

Comme l'image par f de $[a, b]$ est une quasi-géodésique, il existe $e \in [a, b]$ tel que $d(v, f(e)) \leqslant D$. Alors $d(d, e) \leqslant Kd(f(d), d(e)) + KC \leqslant K(2D + d(u, v)) + KC \leqslant K(2D + \delta) + KC = \delta'$. Donc Y est δ'-hyperbolique. □

5.3 Groupes Gromov-hyperboliques

Définition 5.3.1. *Soit G un groupe de type fini. On dit que G est un **groupe Gromov-hyperbolique** si un graphe de Cayley de G est Gromov-hyperbolique.*

Exemples.

- Tout groupe libre est un groupe Gromov-hyperbolique.
- Si H est un sous-groupe d'indice fini de G, ou bien un quotient de noyau fini de G, alors G est Gromov-hyperbolique si et seulement si H est Gromov-hyperbolique.
- Tout groupe fini, ou virtuellement $\mathbb{Z}$, est Gromov-hyperbolique.

Théorème 5.3.2 (Lemme de Svarcz-Milnor)**.** *Soit X un espace métrique géodésique propre, et soit G un groupe discret agissant proprement par isométries sur X, tel que le quotient X/G soit compact. Alors G est de type fini, et tout graphe de Cayley de G est quasi-isométrique à X.*

Démonstration. Fixons $x_0 \in X$, et soit $D \geqslant 0$ tel que $K = B(x_0, D)$ vérifie $G \cdot K = X$. Fixons $S = \{g \in G \mid d(g \cdot x_0, x_0) \leqslant 3D\}$. Par propreté de l'action, S est fini, montrons qu'il engendre G.

Soit $g \in G$, et considérons une géodésique discrète $x_0, x_1, \ldots, x_n = g \cdot x_0$ telle que, pour tout $0 \leqslant i \leqslant n-2$, on ait $d(x_i, x_{i+1} = D$ et $d(x_{n-1}, x_n) \leqslant D$. On a donc $(n-1)D \leqslant d(g \cdot x_0, x_0) \leqslant nD$.

Pour tout $0 \leqslant i \leqslant n$, soit $g_i \in G$ tel que $x_i \in g_i \cdot K$. Alors, pour tout $0 \leqslant i \leqslant n$, on a $d(g_i \cdot x_0, g_{i+1} \cdot x_0) \leqslant 2D + d(x_i, x_{i+1}) \leqslant 3D$. Ainsi $g_i^{-1} g_{i+1} \in S$, donc g est un produit d'au plus n éléments de S. Ainsi G est engendré par S, et de plus $d_S(e, g) \leqslant n \leqslant \frac{1}{D} d(x_0, g \cdot x_0) + 1$.

Montrons l'autre inégalité : soit $g \in G$ tel que $d_S(e, g) = n$, et écrivons $g = s_1 \ldots s_n$, avec $s_i \in S \cup S^{-1}$. Alors, pour tout $0 \leqslant i \leqslant n-1$, on a $d(s_1 \ldots s_I \cdot x_0, s_1 \ldots s_{i+1} \cdot x_0) = d(x_0, s_{i+1} \cdot x_0) \leqslant 3D$. Ainsi $d(x_0, g \cdot x_0) \leqslant 3nD = 3D d_S(e, g)$.

Ainsi $g \in S \mapsto g \cdot x_0 \in X$ est un plongement quasi-isométrique. Comme il est quasi-surjectif, on déduit que G et X sont quasi-isométrique. □

Corollaire 5.3.3. *Si $g \geqslant 2$, le groupe fondamental de la surface compacte de genre g est Gromov-hyperbolique.*

Démonstration. [Idée] On peut munir la surface S_g de genre $g \geqslant 2$ d'une métrique riemannienne à courbure sectionnelle constante égale à -1 (par exemple en recollant les côtés d'un $4g$-gone régulier hyperbolique à angles droits). Le revêtement universel de S_g est alors $\mathbb{H}^2$, et $\pi_1(S_g)$ agit proprement et cocompactement dessus. Ainsi $\pi_1(S_g)$ est quasi-isométrique à $\mathbb{H}^2$, donc est Gromov-hyperboliqe. □

Proposition 5.3.4. *Soient A, B, C trois groupes finis, et $\alpha : C \to A$, $\beta : C \to B$ deux morphismes injectifs. Alors $G = A \star_C B$ est Gromov-hyperbolique.*

Démonstration. D'après le théorème de Bass-Serre, il existe un arbre X sur lequel G agit sans inversion, avec pour quotient une arête, les stabilisateurs de sommets étant conjugués à A ou à B. Les stabilisateurs de sommets étant finis, l'action de G sur X est propre. Comme elle est cocompacte, G est quasi-isométrique à X. Comme X est un arbre, X est Gromov-hyperbolique, donc G est Gromov-hyperbolique. □

Exercice 25. *Montrer que* $\mathrm{GL}(2, \mathbb{Z})$ *est Gromov-hyperbolique.*

5.4 Propriétés des groupes hyperboliques

Nous allons ici donner une liste de propriétés algébriques élémentaires vérifiées par les groupes hyperboliques.

Théorème 5.4.1. *Tout groupe hyperbolique est de présentation finie.*

Lemme 5.4.2. *Soit X un espace métrique géodésique δ-hyperbolique, et soient $c, c' : [0,T] \to X$ deux géodésiques avec $c(0) = c'(0)$. Si $K = d(c(T), c'(T))$, alors pour tout $t \in [0,T]$ on a $d(c(t), c'(t)) \leqslant 2(K+\delta)$.*

Démonstration. Si $c(t)$ est δ-proche d'un point $c'(t')$, alors on a $d(c(t), c'(t)) \leqslant 2\delta$. Donc dans le triangle δ-fin de côtés $c([0,T])$ et $c'([0,T])$, on a $d(c(t), c(T)) \leqslant K + \delta$ et $d(c(t), c'(T)) \leqslant K + \delta$. D'où $|T - t| \leqslant K + \delta$. Ainsi $d(c(t), c'(t)) \leqslant d(c(t), c'(T)) + d(c'(T), c'(t)) \leqslant 2(K+\delta)$. $\square$

Démonstration. Soit G un groupe hyperbolique, et S une partie génératrice finie de G. Soit $\delta \geqslant 0$ tel que $X = \mathrm{Cay}(G,S)$ soit δ-hyperbolique. Soit R l'ensemble des mots de $\mathbb{F}(S)$ de longueur au plus $10+4\delta$ qui représentent l'élément neutre de G. Soit $w = s_1 \dots s_n \in \mathbb{F}(S)$ un mot représentant l'élément neutre de G. Notons $x_0 = 1, x_1 = s_1, \dots, x_n = s_1 \dots s_n = 1$ la suite de sommets de X. Pour tout $0 \leqslant i \leqslant n$, notons c_i un rayon géodésique de 1 à x_i dans X. D'après le lemme, pour tout t, on a $d(c_i(t), c_{i+1}(t)) \leqslant 2(2+\delta) = 4 + 2\delta$. Ainsi on peut écrire w comme un produit de conjugués de mots représentant l'élément neutre de G de longueurs au plus $2(4+2\delta)+2 = 10+4\delta$. Autrement dit, w appartient au sous-groupe normal de $\mathbb{F}(S)$ engendré par R. Ainsi $G = \langle S \mid R \rangle$ est une présentation finie de G. $\square$

Théorème 5.4.3. *Tout groupe hyperbolique a un nombre fini de classes de conjugaison de sous-groupes finis.*

Lemme 5.4.4. *Soit X un espace métrique géodésique δ-hyperbolique, et soit $Y \subset X$ une partie bornée. Soit $r = \inf\{r \geqslant 0 \mid \exists x \in X, Y \subset B(x,r)\}$. Pour tout $\varepsilon > 0$, l'ensemble $C_\varepsilon(Y) = \{x \in X \mid Y \subset B(x, r+\varepsilon)\}$ est de diamètre au plus $4\delta + 2\varepsilon$.*

Démonstration. Soient $x, x' \in C_\varepsilon(Y)$, et soit m le milieu du segment $[x,x']$. Il existe $y \in Y$ tel que $d(y,m) \geqslant r$. Dans le triangle δ-fin de sommets x, x', y, il existe par exemple $p \in [x,y]$ tel que $d(p,m) \leqslant \delta$. Alors $d(p,x) \geqslant d(x,m) - d(m,p) \geqslant d(x,m) - \delta$. D'où $d(y,p) = d(y,x) - d(p,x) \leqslant d(y,x) + \delta - \frac{d(x,x')}{2}$. Ainsi $r \leqslant d(y,m) \leqslant d(y,p) + d(p,m) \leqslant d(y,x) + 2\delta - \frac{d(x,x')}{2} \leqslant r + \varepsilon + 2\delta - \frac{d(x,x')}{2}$. Donc $d(x,x') \leqslant 4\delta + 2\varepsilon$. $\square$

Démonstration. Soit G un groupe hyperbolique, et S une partie génératrice finie de G. Soit $\delta \geqslant 0$ tel que $X = \mathrm{Cay}(G,S)$ soit δ-hyperbolique. Soit H un sous-groupe fini de G. Considérons $C_1(H) \subset X$: c'est une partie de X contenant au moins un sommet. L'action de H sur X préserve l'ensemble des sommets de $C_1(H)$. Si g est un sommet de $C_1(H)$, alors $g^{-1}Hg$ préserve l'ensemble des sommets de $g^{-1}C_1(H)$. Comme $g^{-1}C_1(H)$ contient 1 et est de diamètre au plus $4\delta + 2$, on déduit que $g^{-1}Hg \cdot 1 = g^{-1}Hg$ est inclus dans $g^{-1}C_1(H)$, et donc est inclus dans $B(1, 4\delta + 2)$. Ainsi tout sous-groupe fini de G est conjugué à une partie finie de $B(1, 4\delta+2)$. $\square$

Bibliographie

[Bau93] G. Baumslag – **Topics in combinatorial group theory** , Lectures in Mathematics ETH Zürich, Birkhäuser Verlag, Basel, 1993.

[Ben97] Y. Benoist – « Sous-groupes discrets des groupes de Lie », (1997), Cours à l'Ecole Européenne de théorie des groupes, http ://www.math.u-psud.fr/~benoist/prepubli/0097luminy.pdf.

[BH99] M. R. Bridson & A. Haefliger – Grund. math. Wiss., **Metric spaces of non-positive curvature 319** , Springer, 1999.

[Bow06] B. H. Bowditch – MSJ Memoirs, **A course on geometric group theory 16** , Mathematical Society of Japan, Tokyo, 2006.

[CdV97] Y. Colin de Verdiï¿½re – « Un exemple de gï¿½omï¿½trie non euclidienne : la gï¿½omï¿½trie hyperbolique en dimension 2 », **Repï¿½res - IREM 27** (1997).

[dlH00] P. de la Harpe – **Topics in geometric group theory** , Chicago Lectures in Mathematics, University of Chicago Press, Chicago, IL, 2000.

[GdlH90] É. Ghys & P. de la Harpe – « Panorama », Progr. Math., in **Sur les groupes hyperboliques d'après Mikhael Gromov (Bern, 1988) 83** , Birkhäuser Boston, Boston, MA, 1990, p. 1–25.

[God71] C. Godbillon – **Éléments de topologie algébrique**, Hermann, Paris, 1971.

[Hat02] A. Hatcher – **Algebraic topology**, Cambridge Univ. Press, 2002.

[Haï15] P. Haïssinsky – **Quelques aspects de la théorie géométrique des groupes**, 2015, http ://www.math.univ-toulouse.fr/~phaissin/Enseignement/M2/.

[Löh11] C. Löh – **Geometric group theory, an introduction**, 2011, http ://www.mathematik.uni-regensburg.de/loeh/teaching/ggt_ws1011/lecture_notes.pdf.

[Pau10] F. Paulin – **Topologie algébrique élémentaire**, 2010, http ://www.math.u-psud.fr/~paulin/notescours/cours_topoalg.pdf.

[Ser77] J.-P. Serre – **Arbres, amalgames,** SL_2, Société Mathématique de France, Paris, 1977, Avec un sommaire anglais, Rédigé avec la collaboration de Hyman Bass, Astérisque, No. 46.

[SW79] P. Scott & T. Wall – « Topological methods in group theory », London Math. Soc. Lecture Note Ser., in **Homological group theory (Proc. Sympos., Durham, 1977) 36** , Cambridge Univ. Press, Cambridge-New York, 1979, p. 137–203.