

Groupes, algorithmique et combinatoire: cours 2015

Laurent HAYEZ

Date de création: 30 septembre 2015

Dernière modification: 7 janvier 2016

Table des matières

I. Objets	4
0. Motivations	5
0.1. Algorithmes et combinatoire ?	5
0.2. Problèmes de Dehn	6
0.2.1. Problème de l'égalité (PE)	6
0.2.2. Problème des mots (PM)	6
1. Groupes libres	7
1.1. Propriété universelle du groupe libre (PU)	8
2. Présentations de groupes	9
3. Problèmes de Dehn	10
3.1. Les problèmes de Dehn pour les groupes libres	10
3.1.1. Problème de conjugaison pour les groupes libres	11
3.1.2. Problème de l'isomorphisme pour les groupes libres	11
4. Propriétés du groupe libre	13
4.1. Observations	14
4.2. Groupes libres dans la nature	14
5. Introduction à la topologie algébrique	17
5.1. Groupe fondamental d'un espace topologique	17
5.1.1. Lacets	17
5.1.2. Groupe fondamental	18
5.1.3. Propriétés du groupe fondamental	19
5.2. Produits libres	22
5.3. Théorème de Van Kampen (version simple)	22
5.4. Revêtements	24
6. Transformations de Tietze	29
6.1. Algorithme de Todd-Coxeter (1936) (Coset enumeration)	31
6.1.1. Version basique	31
6.1.2. Version générale	33

6.2. Algorithme de Todd-Coxeter pour les graphes	35
6.2.1. $H = \{1\}$	35
6.2.2. $H \neq \{1\}$ et $ G:H < \infty$	36
7. Graphes de Cayley (groupes comme espaces métriques)	38
7.1. Quasi-isométries	41
7.2. Actions propres	41
7.3. Théorème fondamental de la théorie géométrique des groupes	43
8. Propriétés géométriques	46
8.1. Croissance des groupes	47
9. Croissance et langages (formels)	54

Première partie .

Objets

Chapitre 0.

Motivations

Définition 0.1. Soit G un groupe muni d'une loi " \cdot ". G est un **groupe** si

1. il existe un élément neutre $e \in G$;
2. pour chaque élément $g \in G$, il existe un inverse g^{-1} ;
3. \cdot est associative : $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.

Exemples 0.2. 1. $G = \{e\}$.

2. $G = (\mathbb{Z}, +)$.

3. $G = \mathbb{Z}/n\mathbb{Z}$.

4. $G = S_3$ le groupe des symétries d'un triangle.

5. $G = D_4$ le groupe des symétries d'un carré.



0.1. Algorithmes et combinatoire ?

Chaque groupe G admet une présentation

$$G = \langle X | R \rangle$$

où $X \subset G$ est une partie génératrice et R est un ensemble de relations.

Exemples 0.3. 1. $\mathbb{Z} = \langle a \mid a^{-1}a = 1 \rangle$.

2. $S_3 = \langle t_1, t_2 \mid t_1^2 = e = t_2^2, (t_1 t_2)^3 = e \rangle$.

3. $D_4 = \langle x, y \mid x^2 = y^4 = (xy)^2 = e \rangle$.

4. $\mathbb{Z}/7\mathbb{Z} = \langle x \mid x^7 = e \rangle$.



Attention : la présentation n'est pas unique, car par exemple $\mathbb{Z} = \langle a, b \mid b = 1 \rangle$.

0.2. Problèmes de Dehn

0.2.1. Problème de l'égalité (PE)

Existe-t-il un algorithme permettant de décider pour tout couple de mots (u, v) sur X (pour un groupe $G = \langle X | R \rangle$) s'ils représentent le même élément du groupe ($u =_G v$) ?

Par exemple, soit $G = \langle x, y, z | x^2 y x^{-1} z = x^3 y^3 \rangle$. Est-ce que $xyx^{-1}z =_G zx^2y^{-1}z$? Ou par exemple dans S_3 , est-ce que $t_1 t_2 t_1^3 t_2 =_{S_3} t_2 t_1$? En fait, oui car

$$\begin{aligned} t_1 t_2 t_1^3 t_2 &= t_1 t_2 t_1 t_1^2 t_2 \\ &= t_1 t_2 t_1 t_2 \\ &= t_2^{-1} t_1^{-1} \\ &= t_2 t_1. \end{aligned} \qquad \begin{aligned} t_1^2 &= e \\ (t_1 t_2)^3 &= e \\ t_1 &= t_1^{-1}, \quad t_2 = t_2^{-1} \end{aligned}$$

0.2.2. Problème des mots (PM)

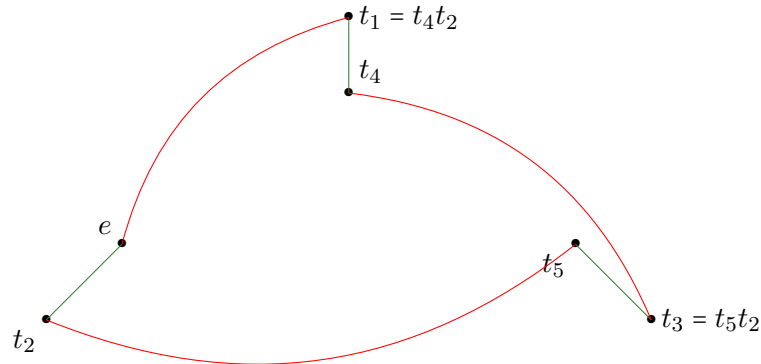
Existe-t-il un algorithme permettant de décider pour tout mot w sur X si $w =_G e$?

Si $G = \langle X | R \rangle$, on peut dessiner son graphe de Cayley, qui est un espace métrique. Les sommets de ce graphe sont $\{g \in G\}$ et les arêtes sont $\{(g, gx) : g \in G, x \in X\}$.

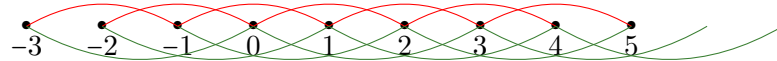
Exemples 0.4. 1. Considérons par exemple

$$S_3 = \{e, (12) = t_1, (23) = t_2, (13) = t_3, (123) = t_4, (132) = t_5\}.$$

On a $X = \{t_1, t_2\}$. Le graphe de Cayley est



2. Considérons $\mathbb{Z} = \langle 2, 3 | 2 + 2 + 2 = 3 + 3 \rangle$. Dessinons son graphe de Cayley.



En fait on dit que ce groupe est quasi-isométrique à $\mathbb{Z} = \langle 1 | - \rangle$.



Chapitre 1.

Groupes libres

Soit A un alphabet, fini ou infini.

- On considère l'ensemble des mots de longueur finie sur $A \cup A^{-1}$ (on introduit pour chaque nouvelle lettre $a \in A$ une nouvelle lettre a^{-1}).
- Un mot est **réduit** s'il ne contient aucune expression de la forme aa^{-1} ou $a^{-1}a$, $a \in A$.
- Le **mot vide** est réduit et se note 1 (ou ε ou e, \dots).

Définition 1.1. Le **groupe libre** sur A , noté $\mathbb{F}(A)$ est l'ensemble des mots réduits sur $A \cup A^{-1}$. Ceci définit $\mathbb{F}(A)$ comme ensemble. Pour avoir un groupe il faut définir le produit : c'est la concaténation/réduction. On écrit deux mots réduits bouts à bouts, puis on réduit en supprimant les apparitions de aa^{-1} ou $a^{-1}a$. Avec ce produit, $\mathbb{F}(A)$ est un groupe.

Si $A = \{a_1, \dots, a_n\}$, on note $\mathbb{F}_n = \mathbb{F}(A)$ et on parle du **groupe libre de rang n** .

Exercice 1.1. Montrer que $\mathbb{F}_1 = \mathbb{Z}$. En fait, on a $A = \{a\}$, donc les mots sont $aaa \dots a^{-1}$, c'est-à-dire a^n ou a^{-n} . ♣

Remarque 1.2. $\mathbb{F}_1 = \mathbb{Z}$ et \mathbb{F}_n ($n > 1$) ont des propriétés très différentes. ♣

Définition 1.3. Soit X un alphabet fini. Le **monoïde libre** sur X , noté $M(X)$, est l'ensemble des mots sur X avec le produit donné par la concaténation. Soit $X = A \cup A^{-1}$. Nous pouvons poser sur $M(X)$ la relation d'équivalence suivante : $w_1 \sim w_2 \iff$ après réduction, $w_1 = w_2$. Le quotient $M(X)/\sim$ est le **groupe libre** $\mathbb{F}(A)$, où l'inverse de la classe d'équivalence de $x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n}$ est la classe d'équivalence de $x_n^{-\varepsilon_n} \dots x_1^{-\varepsilon_1}$ avec $\varepsilon_i \in \mathbb{Z}$ pour tout i . L'opération est la concaténation (la réduction est implicite).

On fait souvent l'abus de langage suivant : on va identifier un mot réduit avec sa classe d'équivalence.

Proposition 1.4. 1. $\mathbb{F}(A)$ est un groupe (von Dyck, 1882).
 2. La définition 1.1 est équivalente à la définition 1.3.

- Preuve.** 1. • Le neutre est le mot vide, noté ε ou $1_{\mathbb{F}(A)}$.
 • L'inverse de $a_1^{\varepsilon_1} \dots a_n^{\varepsilon_n}$ est $a_n^{-\varepsilon_n} \dots a_1^{-\varepsilon_1}$.
 • L'opération de concaténation et réduction est associative (exercice)
 2. Exercice. □

Question : pourquoi dit-on que $\mathbb{F}(A)$ est libre sur A ?

Réponse : car tout mot réduit sur A représentant l'élément neutre est le mot vide (exercice). Alors il n'y a pas de relation entre les lettres dans A , et $\mathbb{F}(A)$ à la présentation $\langle a_1, a_2, \dots, a_n \mid - \rangle$.

1.1. Propriété universelle du groupe libre (PU)

Soit G un groupe et $f : A \rightarrow G$ une application. Alors il existe un unique homomorphisme φ tel que le diagramme suivant commute.

$$\begin{array}{ccc} A & \xrightarrow{i} & \mathbb{F}(A) \\ & \searrow f & \swarrow !\varphi \\ & G & \end{array}$$

Ceci signifie que toute application $f : A \rightarrow G$ s'étend en un unique homomorphisme $\varphi : \mathbb{F}(A) \rightarrow G$ où pour $w = a_{i_1}^{\varepsilon_1} \dots a_{i_n}^{\varepsilon_n}$ on pose $\varphi(w) = f(a_{i_1})^{\varepsilon_1} \dots f(a_{i_n})^{\varepsilon_n}$ avec $\varepsilon_i \in \mathbb{Z}$. En particulier, si A est une partie génératrice de G (par exemple $A = G$), on voit que $\mathbb{F}(A)$ se surjecte sur G et ceci nous donne le théorème suivant, qui est très important.

Théorème 1.5. *Tout groupe est quotient d'un groupe libre.*

Preuve. Si A est une partie génératrice d'un groupe G , par le premier théorème d'isomorphisme, il existe un isomorphisme tel que $\varphi : \mathbb{F}(A) \rightarrow G$ implique que $\mathbb{F}(A)/\ker \varphi \cong \text{Im} \varphi = G$. □

Chapitre 2.

Présentations de groupes

Soit $R \subset \mathbb{F}(A)$. La **fermeture normale** $N(R)$ ou $\triangleleft R \triangleright$ ou $gp_{\mathbb{F}(A)}(R)$ dans $\mathbb{F}(A)$ est définie par

$$\bigcap_{\substack{N \triangleleft \mathbb{F}(A) \\ R \subset N}} N.$$

Il faut vérifier que

- $N(R) \triangleleft \mathbb{F}(A)$;
- $N(R) = \left\{ \prod_{r_{ij} \in R} w_{ij} r_{ij}^{\varepsilon_j} w_{ij}^{-1} \right\}$ où $\varepsilon_j = \pm 1$, $r_{ij} \in R$ et $w_{ij} \in \mathbb{F}(A)$.

C'est en fait le plus petit sous-groupe normal contenant R .

Si G a une partie génératrice A , d'après la PU on a $G \cong \mathbb{F}(A)/\ker \varphi$ où $\varphi : \mathbb{F}(A) \xrightarrow{\text{surj.}} G$. Alors si $\ker \varphi = \triangleleft R \triangleright$, on dit que G est donné par la présentation $\langle A | R \rangle$. Les éléments de A sont les **générateurs** et les éléments de R sont les **relateurs**.

- Remarques 2.1.**
1. Si $|A| < +\infty$, on dit que G est **finiment engendré**.
 2. Si $|A| < +\infty$ et $|R| < +\infty$, on dit que G est **finiment présenté**.



- Remarques 2.2.**
1. Si S est un ensemble et $R \subset \mathbb{F}(S)$, la présentation $\langle S | R \rangle$ définit un **unique groupe** (à isomorphisme près), le groupe $G = \mathbb{F}(S)/\triangleleft R \triangleright$.
 2. Un groupe admet une infinité de présentations.



- Exemples 2.3.**
1. Le groupe trivial : $T = \langle x | x = 1 \rangle$, $T = \langle a, b | a = b = 1 \rangle$.
 2. $(\mathbb{Z}^2, +) = \langle a, b | ab = ba \rangle$ où $a = (1, 0)$ et $b = (0, 1)$.
 3. $F_2 = \langle a, b | - \rangle$.
 4. $\mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/s\mathbb{Z} = C_r \times C_s = \langle x, y | x^r = 1, y^s = 1, xy = yx \rangle = \mathbb{F}(x, y)/\triangleleft x^r, y^s, [x, y] \triangleright$ où $[x, y] = xyx^{-1}y^{-1} = 1$ est le commutateur.
 5. $G = \langle X | R \rangle$, $H = \langle Y | S \rangle$, $G \times H = \langle X \cup Y | R \cup S, xy = yx, x \in X, y \in Y \rangle$.



Chapitre 3.

Problèmes de Dehn

Supposons que G soit donné par une présentation finie $\langle S|R \rangle$.

- (1) (PM) Problème des mots : soit $w \in \mathbb{F}(S)$. Est-ce que $w =_G 1$?
- (1') (PE) Problème de l'égalité des mots : soient $w_1, w_2 \in \mathbb{F}(S)$, est-ce que $w_1 =_G w_2 \iff w_1 w_2^{-1} =_G 1$?
- (2) (PC) Problème de conjugaison : soient $w, v \in \mathbb{F}(S)$. Est-ce qu'il existe $g \in \mathbb{F}(S)$ tel que $g^{-1}wg =_G v$?
- (3) (PI) Problème de l'isomorphisme : soit $G_1 = \langle S_1|R_1 \rangle$ et $G_2 = \langle S_2|R_2 \rangle$ des présentations finies. Est-ce que $G_1 \cong G_2$?

La réponse à ces trois problèmes est qu'ils sont insolubles : il n'existe pas d'algorithme pour décider s'il y a une solution pour les trois questions (Adyan, Novikov-Boone, 1950-1960).

Exemple 3.1. Soit $G = \langle x, y | x^2 y^3 = x^3 y^4 = 1 \rangle$. On a que $x^3 y^4 = 1 = x(x^2 y^3)y = xy$, donc $x = y^{-1}$ et $y = x^{-1}$. Ainsi $x^2 y^3 = x^2 (x^{-1})^3 = x^{-1} = 1$, d'où $x = y = -1$. Ainsi G est le groupe trivial! ★

Proposition 3.2. *Le problème des mots et le problème de conjugaison sont des invariants algébriques, ie pour deux présentations finies $\langle S_1|R_1 \rangle, \langle S_2|R_2 \rangle$ d'un même groupe G , on a que les problème des mots pour $\langle S_1|R_1 \rangle$ est résoluble ssi le problème des mots pour $\langle S_2|R_2 \rangle$ est résoluble (pour PE aussi).*

Preuve. Exercice. L'idée est que si on peut exprimer un mot dans S_1 , on peut aussi l'exprimer dans S_2 . □

3.1. Les problèmes de Dehn pour les groupes libres

Soit $A = \{a, b, c, \dots\}$, et $\mathbb{F}(A)$ le groupe libre sur A .

- 1. Problème des mots : soit $w =_{\mathbb{F}(A)} 1 \iff$ après réductions, w est le mot vide.
 $caa^{-1}b^{-2}b^2c^{-1} = 1$ (ou ε) par réductions.
- (1') Problème d'égalité : w_1, w_2 deviennent w'_1, w'_2 après réduction et on a que $w_1 =_{\mathbb{F}(A)} w_2 \iff w'_1 \equiv w'_2$.

3.1.1. Problème de conjugaison pour les groupes libres

Définition 3.3. Si $w \in \mathbb{F}(A)$ et $w = av a^{-1}$ avec $a \in A$ et $v \in \mathbb{F}(A)$, l'opération $w \xrightarrow{\text{c. réd.}} v$ (enlever les a et a^{-1}) s'appelle **réduction cyclique** de w .

Exemple 3.4. $w = a^{-1}bca^2b^{-1}a \xrightarrow{\text{c.}} bca^2b^{-1} \xrightarrow{\text{c.}} ca^2$. ★

Définition 3.5. Un mot w est **cycliquement réduit** s'il n'a pas une forme $w = av a^{-1}$, $a \in A, v \in \mathbb{F}(A)$.

Définition 3.6. Deux mots v, w sont **conjugués cycliques** s'il existe des mots α et β tels que $w = \alpha\beta$ et $v = \beta\alpha$.

Exemple 3.7. $w = aab^{-1}c$. Un conjugué cyclique est $ab^{-1}ca$, en continuant on a $b^{-1}ca^2$, etc... ★

L'algorithme pour résoudre le problème de conjugaison est le suivant. Soient w_1 et w_2 deux mots. On commence par faire la réduction cyclique des deux mots pour obtenir w'_1 et w'_2 . w'_1 et w'_2 sont donc cycliquement réduits. Si w'_1 et w'_2 sont conjugués cycliques, alors il existe g tel que $gw_1g^{-1} = w_2$.

Exemple 3.8. Soient $w_1 = abc^{-1}$ et $w_2 = abbab^{-1}a^{-1}$. On effectue la réduction cyclique :

$$w_1 \xrightarrow{\text{c.}} ab, \quad w_2 \xrightarrow{\text{c.}} bbab^{-1} \xrightarrow{\text{c.}} ba.$$

ab et ba sont conjugués cycliques, donc w_1 et w_2 sont conjugués. À la fin on obtient que

$$w_1 = (cab^{-1}a^{-1})w_2(cab^{-1}a^{-1})^{-1},$$

ainsi $g = cab^{-1}a^{-1}$. ★

3.1.2. Problème de l'isomorphisme pour les groupes libres

Pour deux présentations $\langle X_1 | R_1 \rangle$ et $\langle X_2 | R_2 \rangle$, il n'y a pas d'algorithme pour résoudre le problème de l'isomorphisme.

Mais ici on sait qu'on a deux groupes libres.

Théorème 3.9. Soient X, Y deux ensembles (finis ou infinis). On a que $\mathbb{F}(X) \cong \mathbb{F}(Y) \iff |X| = |Y|$ ($|X| = |Y|$ s'il y a une bijection $f : X \rightarrow Y$).

Preuve. " \Rightarrow " : Supposons qu'on ait une bijection $f : X \rightarrow Y$. Alors il existe $g = f^{-1} : Y \rightarrow X$. Par la propriété universelle, on a $\tilde{f} : X \rightarrow \mathbb{F}(Y)$, $i_X : X \hookrightarrow \mathbb{F}(X)$ et il existe un unique homomorphisme $\varphi : \mathbb{F}(X) \rightarrow \mathbb{F}(Y)$. Même chose pour Y on prend \tilde{g} , i_Y et ψ .

$$\begin{array}{ccccc}
 X & \xrightarrow{\tilde{f}} & \mathbb{F}(Y) & & X & \xrightarrow{\tilde{g}} & \mathbb{F}(X) & & X & \xrightarrow{i_X} & \mathbb{F}(X) \\
 \searrow i_X & & \nearrow \varphi & & \searrow i_Y & & \nearrow \psi & & \searrow i_X & & \nearrow !\alpha=id_{\mathbb{F}(X)} \\
 & & \mathbb{F}(X) & & & & \mathbb{F}(Y) & & & & \mathbb{F}(X)
 \end{array}$$

Alors $\psi \circ \varphi : \mathbb{F}(X) \rightarrow \mathbb{F}(X)$ est une extension de i_X . Par l'unicité dans la propriété universelle, $\psi \circ \varphi = id_{\mathbb{F}(X)}$.

De même $\varphi \circ \psi : \mathbb{F}(Y) \rightarrow \mathbb{F}(Y)$ est égal à $id_{\mathbb{F}(Y)}$. Donc φ et ψ sont des isomorphismes et ainsi $\mathbb{F}(X) \cong \mathbb{F}(Y)$.

" \Leftarrow " : Si $\mathbb{F}(X) \cong \mathbb{F}(Y)$, alors $|X| = |Y|$. Soit $N(X) = \langle g^2 | g \in \mathbb{F}(X) \rangle$. Montrons que $N(X)$ est un sous-groupe normal. La partie sous-groupe est claire, il reste donc à montrer qu'il est normal. $gh^2g^{-1} = (ghg^{-1})(ghg^{-1}) = (ghg^{-1})^2 \in N(x)$ (ce n'est pas la preuve complète, mais c'est l'idée). Ainsi $N(x) \triangleleft \mathbb{F}(X)$ et $\mathbb{F}(X)/N(X)$ est un groupe abélien, un 2-groupe, ie $x^2 = 1 \forall x \in \mathbb{F}(X)/N(X)$.

1. $(gN)^2 = gNgN = g^2N = N$ ce qui montre que c'est un 2-groupe.
2. $(xy)^2 = 1 \implies xyxy = 1 \implies xy = y^{-1}x^{-1} = yx$ car les éléments sont d'ordre 2, ce qui montre que $\mathbb{F}(X)/N(X)$ est abélien.

Notons $V(X) = \mathbb{F}(X)/N(X) = \underbrace{\mathbb{Z}/2\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/2\mathbb{Z}}_{|X|}$ car chaque élément engendre

un groupe cyclique d'ordre 2. Ainsi V est $\mathbb{Z}/2\mathbb{Z}$ -espace vectoriel avec base X et de dimension $|X|$.

Comme $\mathbb{F}(X) \cong \mathbb{F}(Y)$ on a que $\mathbb{F}(X)/N(X) \cong \mathbb{F}(Y)/N(Y) \implies V(X) \cong V(Y) \implies |X| = |Y|$ car deux espaces vectoriels isomorphes ont des bases de mêmes cardinalités.

□

Chapitre 4.

Propriétés du groupe libre

Proposition 4.1. *Si $|A| \geq 2$, le centre de $\mathbb{F}(A)$ est trivial (ex), $Z(G) = \{g \in G | gh = hg \forall h \in G\}$.*

Preuve. " \supset " : Cette inclusion est triviale, car l'élément neutre commute avec tout élément et ainsi $\{1\} \subset Z(\mathbb{F}(A))$.

" \subset " : On va montrer la contraposée, c'est-à-dire que si $g \in \mathbb{F}(A)$ avec $g \neq 1$, $g \notin Z(\mathbb{F}(A))$. Si $g = a_{i_1}^{\varepsilon_1} \dots a_{i_n}^{\varepsilon_n}$, avec $\varepsilon_i \neq -\varepsilon_{n+1-i}$ pour tout i , et $\varepsilon_1 \neq -\varepsilon_{n-2}$ (pour qu'il n'y ait pas de réductions possible dans g). On pose

$$h = a_{i_n}^{-\varepsilon_n} a_{i_{n-1}}^{-\varepsilon_{n-1}} a_{i_1}^{\varepsilon_1} \dots a_{i_{n-1}}^{\varepsilon_{n-1}}.$$

Ainsi, on a

$$gh = a_{i_1}^{\varepsilon_1} \dots a_{i_n}^{\varepsilon_n} a_{i_n}^{-\varepsilon_n} a_{i_{n-1}}^{-\varepsilon_{n-1}} a_{i_1}^{\varepsilon_1} \dots a_{i_{n-2}}^{\varepsilon_{n-2}} = a_{i_1}^{\varepsilon_1} \dots a_{i_{n-2}}^{\varepsilon_{n-2}} a_{i_1}^{\varepsilon_1} \dots a_{i_{n-2}}^{\varepsilon_{n-2}} = (a_{i_1}^{\varepsilon_1} \dots a_{i_{n-2}}^{\varepsilon_{n-2}})^2,$$

$$hg = a_{i_n}^{-\varepsilon_n} a_{i_{n-1}}^{-\varepsilon_{n-1}} a_{i_1}^{\varepsilon_1} \dots a_{i_{n-2}}^{\varepsilon_{n-2}} a_{i_1}^{\varepsilon_1} \dots a_{i_n}^{\varepsilon_n}$$

et $hg \neq gh$ car h et g sont irréductibles, et ne se réduisent quand on les multiplie car $\varepsilon_1 \neq -\varepsilon_{n-2}$ par hypothèse. □

Proposition 4.2. *Si $|A| \geq 2$, $\mathbb{F}(A)$ est sans torsion (ex), (torsion : $\exists g \in G, n \geq 2 \in \mathbb{N}$ tq $g^n = 1$).*

Preuve. Exercice □

Théorème 4.3 (DE NIELSEN-SCHREIER, 1927). *Tout sous-groupe d'un groupe libre est libre.*

Théorème 4.4 (VERSION QUANTITATIVE DE NIELSEN-SCHREIER). *si H est un sous-groupe d'indice k de \mathbb{F}_n , alors $H \cong \mathbb{F}_{k(n-1)+1}$.*

4.1. Observations

1. $\mathbb{F}_2 \hookrightarrow \mathbb{F}_n$, $n \geq 2$. Par exemple $\mathbb{F}_2 = \langle a, b \rangle \hookrightarrow \langle a_1, a_2, \dots, a_n \rangle$.
2. L'autre direction "fonctionne" aussi, ie $\mathbb{F}_n \hookrightarrow F_2$, $n \geq 2$. Ainsi \mathbb{F}_2 contient les groupes libres de rang n pour chaque $n \in \mathbb{N}$.

Exemple 4.5. Soit $\mathbb{F}_2 = \langle a, b \rangle$ et $\mathbb{F}_n = \langle a_1, a_2, \dots, a_n \rangle$ et

$$f : \mathbb{F}_n \rightarrow \mathbb{F}_2, a_i \mapsto a^{-i} b a^i.$$

Alors f est un homomorphisme. On doit montrer que f est injective, c'est-à-dire pour chaque mot réduit $a_{i_1}^{r_1} \dots a_{i_m}^{r_m}$ dans \mathbb{F}_n où $a_{i_j} \in \{a_1, \dots, a_n\}$, $r_i \in \mathbb{Z}$, $i_j \neq i_{j+1}$. On va montrer que $f(a_{i_1}^{r_1} \dots a_{i_m}^{r_m}) \neq_{\mathbb{F}_2} 1$.

On a que

$$f(a_{i_1}^{r_1} \dots a_{i_m}^{r_m}) = a^{-i_1} b^{r_1} a^{i_1} a^{-i_2} b^{r_2} a^{i_2} \dots a^{i_m} \neq_{\mathbb{F}_2} 1$$

car, par exemple, $i_1 \neq i_2$ ainsi il y a des réductions, mais ça ne se réduit pas au mot vide. ★

4.2. Groupes libres dans la nature

Il y a des groupes libres partout !

Proposition 4.6. *Le sous-groupe de $SL_2(\mathbb{Z})$ engendré par $l = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$ et $r = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ est libre de rang 2.*

La preuve utilise le Lemme du Ping-Pong.

Lemme 4.7 (DU PING-PONG, KLEIN, 1880). *Soit G un groupe, $\alpha, \beta \in G$. On suppose que G agit sur un ensemble E ayant deux parties $X, Y \neq \emptyset$, tq $X \cap Y = \emptyset$ et*

- $\forall m \in \mathbb{Z} \setminus \{0\}, \alpha^m \cdot y \in X$ pour tout $y \in Y$,
- $\forall m \in \mathbb{Z} \setminus \{0\}, \beta^m \cdot x \in Y$ pour tout $x \in X$.

Alors $\langle \alpha, \beta \rangle \cong \mathbb{F}_2$.

Preuve (DU LEMME DU PING-PONG). Soit m un mot réduit sur α, β . m est de la forme

1. $m = \alpha^{h_1} \beta^{k_1} \dots \beta^{k_{n-1}} \alpha^{h_n}$ avec $h_i, k_i \in \mathbb{Z} \setminus \{0\}$. Alors supposons que $m =_G 1$. Ainsi

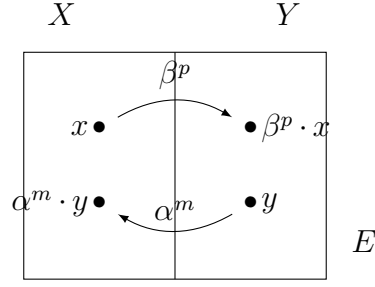


FIGURE 4.1. – Illustration du Lemme du Ping-Pong

$$m \cdot Y = Y.$$

$$\alpha^{h_1} \dots \beta^{k_{n-1}} \alpha^{h_n} \cdot Y \subseteq \alpha^{h_1} \dots \beta^{k_{n-1}} \cdot X \subseteq \alpha^{h_1} \dots \alpha^{k_{n-1}} \cdot Y \subset \dots \subseteq \alpha^{h_1} \cdot Y \subset X,$$

ainsi $m \cdot Y \subset X$, ce qui est une contradiction.

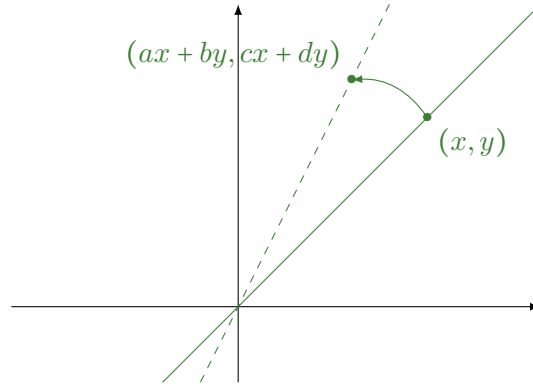
2. $m = \beta^{k_1} \dots \beta^{k_n}$, donc $\alpha^{-h_1} m \alpha^{h_1}$ est comme au point 1 et ainsi $\alpha^{-h_1} m \alpha^{h_1} \neq_G 1$ ainsi $m \neq_G 1$.
3. Si $m = \alpha^{h_1} \dots \beta^{k_n}$, pour $h_0 \neq h_1$ on regarde $\alpha^{-h_0} (\alpha^{h_1} \dots \beta^{k_n}) \alpha^{h_0}$ qui est comme au point 1. Donc $m \neq_G 1$.
4. $m = \beta^{k_1} \dots \alpha^{h_n}$ et on fait la même preuve qu'au point 3.

Ainsi $m \neq 1$ et $\langle \alpha, \beta \rangle \cong \mathbb{F}_2$. □

Preuve (DE 4.6). Exercice.

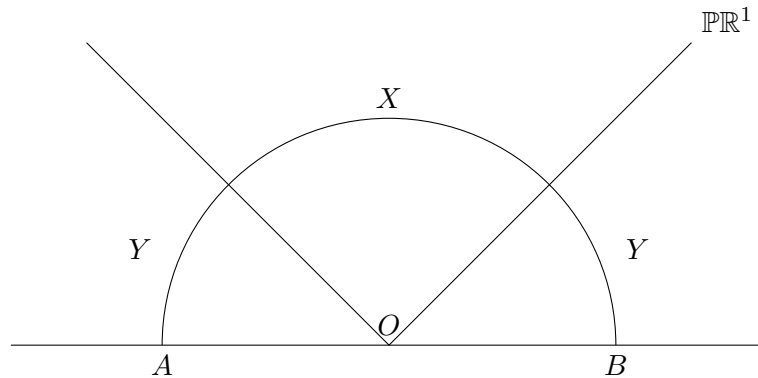
Début de la preuve : on regarde $E = \mathbb{R}^2$ et on regarde l'action de $SL_2(\mathbb{Z})$ sur \mathbb{R}^2 .

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}$$



où \cdot représente l'action (on prend simplement la multiplication). On ne va pas utiliser seulement des points, mais des droites vectorielles. On prend la droite qui passe par l'origine et $(x, y) \in \mathbb{R}^2$ et on regarde l'image de cette droite par l'action, qui est aussi une droite vectorielle. On peut considérer l'action sur l'ensemble des

droites vectorielles dans \mathbb{R}^2 qui est l'espace projectif de dimension 1, $\mathbb{P}\mathbb{R}^1$ (une droite projective peut être vue comme “demi-cercle” où $A = B$). Il faut donc montrer que X et Y satisfont l'hypothèse du Lemme du Ping-Pong.



□

Remarque 4.8. On trouve des groupes libres très souvent dans les groupes linéaires. ♣

Théorème 4.9 (“ALTERNATIVE DE TIETZE”, 1971). *Soit G un groupe linéaire, c’est-à-dire un sous-groupe de $GL_n(\mathbb{C})$ pour un certain $n \geq 1$. On a l’alternative :*

- ou bien G est virtuellement résoluble ;
- ou bien G contient \mathbb{F}_2 comme sous-groupe.

Exemple 4.10. Considérons $\text{Homeo}(\mathbb{R}) = \{\varphi : \mathbb{R} \rightarrow \mathbb{R} \mid \varphi \text{ est continue et bijective}\}$. $\text{Homeo}(\mathbb{R})$ contient beaucoup de groupes libres.

$$\begin{cases} f(x) &= x^p, \text{ } p \text{ premier impair,} \\ g(x) &= x + 1. \end{cases}$$

Alors $\langle f(x), g(x) \rangle \cong \mathbb{F}_2$ (la preuve est très difficile).



Chapitre 5.

Introduction à la topologie algébrique

À tout espace topologique X raisonnable, on associe des groupes.

Une propriété fondamentale est qu'à toute application continue $f : X \rightarrow Y$ correspond un homomorphisme de groupes $f_* : F(X) \rightarrow F(Y)$.

5.1. Groupe fondamental d'un espace topologique

5.1.1. Lacets

Définition 5.1. Soit X un espace topologique. Un **arc** dans X est une application continue $\gamma : [0, 1] \rightarrow X$, $t \mapsto \gamma(t)$, où $\gamma(0)$ est l'**origine** de γ et $\gamma(1)$ est l'**extrémité** de γ .

Un arc peut être inversé :

$$\check{\gamma}(t) = \gamma(1 - t).$$

Deux arcs γ, δ peuvent être composés si l'origine de δ est l'extrémité de γ .

$$(\gamma\delta)(t) = \begin{cases} \gamma(2t) & \text{si } 0 \leq t \leq \frac{1}{2}, \\ \delta(2t - 1) & \text{si } \frac{1}{2} \leq t \leq 1. \end{cases}$$

Pour avoir une composition toujours bien définie, on se restreint aux **lacets**, c'est-à-dire les arcs tels que $\gamma(0) = \gamma(1) = x_0$. Si $x_0 = \gamma(0) = \gamma(1)$, on dit que γ est **basée en** x_0 .

En 1901, POINCARÉ (1854-1912) a eu l'idée que, si on regarde les lacets à déformation continue près, on obtient un groupe, qui détecte la présence de “trous” dans X .

Définition 5.2. Soient γ_0, γ_1 deux lacets basés en x_0 . Une **homotopie** de γ_0 à γ_1 est une application continue

$$F : [0, 1] \times [0, 1] \rightarrow X$$

telle que

$$\begin{cases} F(0, t) = \gamma_0(t), & \forall t \in [0, 1], \\ F(s, 0) = F(s, 1) = x_0, & \forall s \in [0, 1], \\ F(1, t) = \gamma_1(t), & \forall t \in [0, 1]. \end{cases}$$

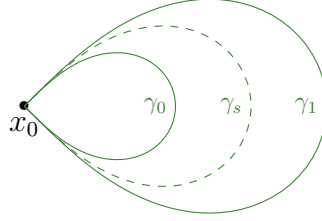


FIGURE 5.1. – Exemple d'homotopie

Si on pose $\gamma_s(t) = F(s, t)$, on voit que $(\gamma_s)_{s \in [0, 1]}$ est une famille continue de lacets qui interpole entre γ_0 et γ_1 .

Définition 5.3. Deux lacets γ_0 et γ_1 (basés en x_0) sont **homotopes** s'il existe une homotopie de γ_0 à γ_1 , et dans ce cas on écrit $\gamma_0 \sim \gamma_1$. On écrit le lacet trivial basé en x_0 ε_{x_0} . Si $\gamma \sim \varepsilon_{x_0}$, on dit que γ est homotope à zéro.

Proposition 5.4. Pour les lacets basés en $x_0 \in X$, la relation “être homotope” est une relation d'équivalence. On note $[\gamma]$ la classe d'équivalence de γ .

Preuve. Exercice. □

5.1.2. Groupe fondamental

Théorème 5.5 (-DÉFINITION). On note $\Pi_1(X, x_0)$ l'ensemble des classes d'homotopie des lacets de X basés en x_0 . Avec la multiplication $[\gamma][\delta] = [\gamma\delta]$, $\Pi_1(X, x_0)$ est un groupe, appelé **groupe fondamental** de X (en x_0).

L'élément neutre est $[\varepsilon_{x_0}]$ et l'inverse de $[\gamma]$ est $[\check{\gamma}]$.

Preuve. On vérifie d'abord que, si $\gamma_0 \sim \gamma_1$, $\delta_0 \sim \delta_1$ alors $\gamma_0\delta_0 \sim \gamma_1\delta_1$, c'est-à-dire que la multiplication est bien définie. On a donc que $[\gamma_0] = [\gamma_1]$ et $[\delta_0 = \delta_1] \Rightarrow [\gamma_0\delta_0] = [\gamma_1\delta_1]$.

Soient F et G deux homotopies de γ_0 à γ_1 et de δ_0 à δ_1 respectivement. Une homotopie de $\gamma_0\delta_0$ à $\gamma_1\delta_1$ est donnée par

$$H(s, t) = \begin{cases} F(s, 2t) & \text{si } 0 \leq t \leq \frac{1}{2}, \quad s \in [0, 1] \\ G(s, 2t - 1) & \text{si } \frac{1}{2} \leq t \leq 1, \quad s \in [0, 1] \end{cases}$$

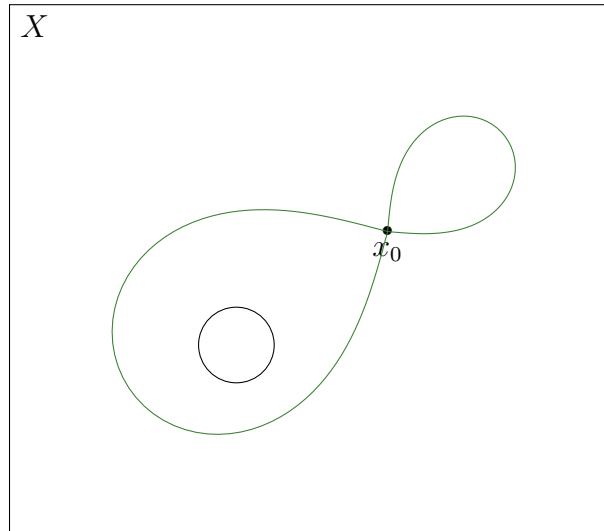


FIGURE 5.2. – Exemple d’homotopies ayant des classes d’équivalence différentes (le rond est un “trou”)

(à vérifier).

Il faut encore montrer que :

- $\varepsilon_{x_0} \gamma \sim \gamma \sim \gamma \varepsilon_{x_0}$;
- $\gamma \tilde{\gamma} \sim \varepsilon_{x_0}$;
- associativité : si $\gamma_0, \gamma_1, \gamma_2$ sont trois lacets basés en x_0 , $\gamma_0(\gamma_1\gamma_2) \sim (\gamma_0\gamma_1)\gamma_2$.

□

5.1.3. Propriétés du groupe fondamental

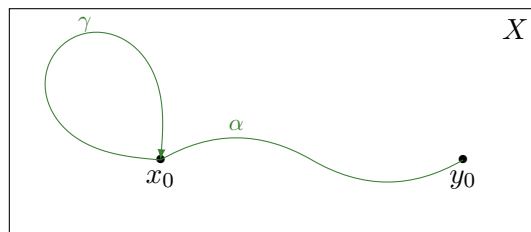
Rappel : Un espace est **connexe par arcs** si deux points peuvent être joints par un arc.

Proposition 5.6. *Si X est connexe par arc, alors*

$$\Pi_1(X, x_0) \cong \Pi_1(X, y_0) \quad \forall x_0, y_0 \in X.$$

Conséquence 5.7. *Si X est connexe par arcs, on peut parler du **groupe fondamental de X** , noté $\Pi_1(X)$.*

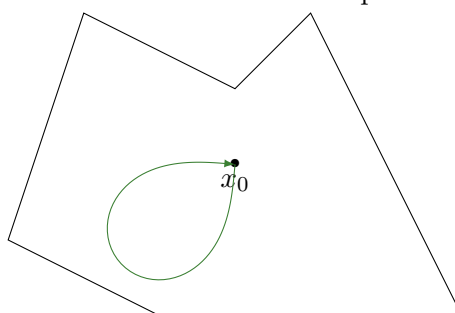
Preuve. Exercice. Dessin de l’idée de la preuve :



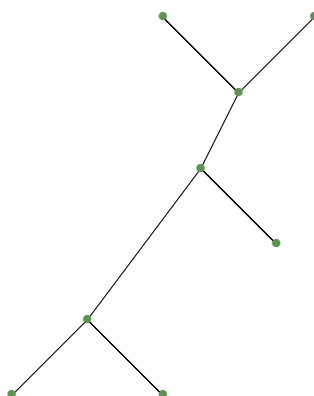
Ainsi pour passer de $\gamma \in \Pi_1(X, x_0)$ à un élément de $\Pi_1(X, y_0)$, on prend $\alpha\gamma\alpha$. \square

Définition 5.8. Un espace X (connexe par arcs) est **simplement connexe** si $\Pi_1(X) = 0$ (ou $\{1\}$). C'est-à-dire que tout lacet dans X est homotope à ε_{x_0} .

Exemples 5.9. 1. Un tel ensemble de \mathbb{R}^n est simplement connexe :



2. Les arbres sont simplement connexes :



3. L'ensemble suivant est homéomorphe à $[0, 1] \times [0, 1]$.



4. Pour $n \geq 2$, la sphère \mathbb{S}^n est simplement connexe (S^1 n'est pas simplement connexe).



Proposition 5.10. Soit $f : X \rightarrow Y$ une application continue, avec $y_0 = f(x_0)$. On pose $f_* : \Pi_1(X, x_0) \rightarrow \Pi_1(Y, y_0), [\gamma] \mapsto [f \circ \gamma]$. Alors f_* est un homomorphisme de groupes.

De plus,

1. si $f : X \rightarrow Y$, $g : Y \rightarrow Z$ sont continues avec $y_0 = f(x_0)$ et $z_0 = g(y_0)$, alors $(g \circ f)_* = g_* \circ f_*$;
2. $id_X : X \rightarrow X$, alors $(id_X)_* = Id_{\Pi_1(X, x_0)}$.

Preuve. Exercice.



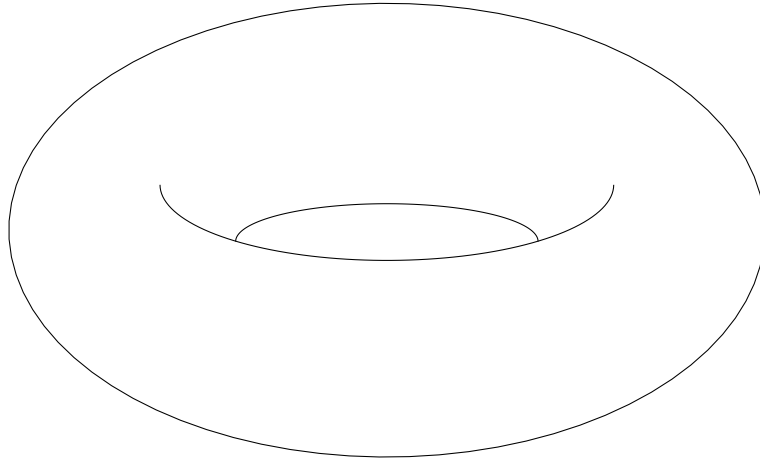
Théorème 5.11. On a que

$$\Pi_1(S^1) \cong \mathbb{Z}$$

Preuve. Difficile, et long.



Exemples 5.12. 1. Soit Π^2 le tore. En découpant le long de a_1 et a_2 , on obtient un carré. Ceci montre que $[a_1 a_2 a_1^{-1} a_2^{-1}] = 1$ dans $\Pi_1(\Pi^2)$. Ainsi $\Pi_1(\Pi^2) = \mathbb{Z}^2$. Si on enlève à Π^2 un petit disque ouvert D , le bord de D est $a_1 a_2 a_1^{-1} a_2^{-1}$ dans $\Pi_1(X)$, où $X = \Pi^2 \setminus D$. En fait, $\Pi_1(X) \cong \mathbb{F}_2 = \langle a_1, a_2 \rangle$ (\mathbb{F}_2 est le groupe libre).



2. On a que $\Pi_1(\Sigma_2) = \langle a_1, a_2, b_1, b_2 | [a_1, a_2][b_1, b_2] = 1 \rangle$.



5.2. Produits libres

Définition 5.13. Soient A et B deux groupes. Le **produit libre**, noté $G = A * B$ est l'ensemble des mots de la forme

$$a_1 b_1 a_2 b_2 \cdots a_k b_k, \quad k \in \mathbb{N}, \quad a_i \in A, \quad b_i \in B$$

et $a_2, \dots, a_k \neq \varepsilon_A$ et $b_1, \dots, b_{k-1} \neq \varepsilon_B$.

Donc G est l'ensemble des mots obtenus en alternant un élément non trivial d'un groupe, un élément non trivial de l'autre, etc.

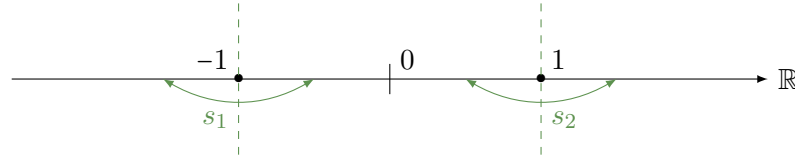
Exemple 5.14. 1. $\mathbb{Z} * \mathbb{Z} = \mathbb{F}_2 = \langle a, b \rangle$.

2. En général, $\mathbb{F}_k * \mathbb{F}_m \cong \mathbb{F}_{k+m}$.

3. Soit D_∞ le groupe diédral infini, c'est le sous-groupe des isométries de \mathbb{R} engendré par deux symétries centrales. Alors

$$D_\infty \cong \mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/2\mathbb{Z}$$

où $\mathbb{Z}/2\mathbb{Z} = \langle s_1 \rangle$ et $\mathbb{Z}/2\mathbb{Z} = \langle s_2 \rangle$. En effet, prenons



On voit que pour tout $s_{i_1} \cdots s_{i_k}$ avec $i_j \neq i_{j+1}$, on a $s_{i_1} \cdots s_{i_k} \neq 0$, ainsi $s_{i_1} \cdots s_{i_k} \neq \varepsilon_{D_\infty}$.



Lemme 5.15 (DU PING-PONG, 2ÈME VERSION). Soient G_1, G_2 des sous-groupes de $\text{Sym}(X)$. On suppose que $|G_1| \geq 2$, $|G_2| \geq 3$. S'il existe deux parties $A_1, A_2 \subset X$ telles que $A_i \neq \emptyset$, $A_1 \not\subset A_2$ avec

- $g_1(A_1) \subseteq A_2 \forall g_1 \in G_1 \setminus \{id\}$;
- $g_2(A_2) \subseteq A_1 \forall g_2 \in G_2 \setminus \{id\}$,

alors le sous-groupe engendré par $G_1 \cup G_2$ dans $\text{Sym}(X)$ est isomorphe à $G_1 * G_2$.

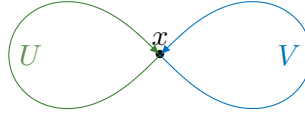
5.3. Théorème de Van Kampen (version simple)

Théorème 5.16 (DE VAN KAMPEN). Soit X un espace connexe par arcs. On suppose que $X = U \cup V$ où

- U et V sont des ouverts connexes par arcs ;
- $U \cap V$ est simplement connexe et non vide.

Alors $\Pi_1(X) \cong \Pi_1(U) * \Pi_1(V)$ (produit libre des groupes fondamentaux).

Exemples 5.17. 1. Le bouquet à deux cercles. Si $X = U \cup V$, on a $U \cap V = \{x\}$.



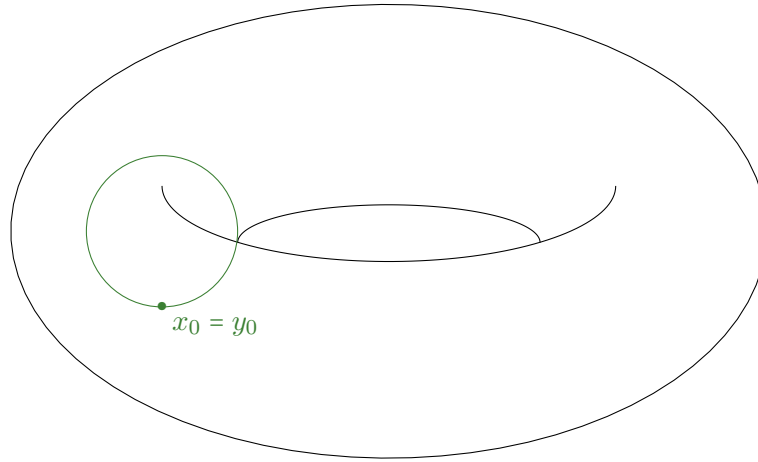
Le groupe fondamental est

$$\Pi_1(X) = \Pi_1(U) * \Pi_1(V) = \mathbb{Z} * \mathbb{Z} = \mathbb{F}_2.$$

2. Si (X, x_0) et (Y, Y_0) sont deux espaces pointés (car on a donné des points), le **wedge** ou **joint** de X et Y est $X \wedge Y = X \cup Y / x_0 = y_0$. Si x_0, y_0 possèdent des voisinages simplement connexes, alors

$$\Pi_1(X \wedge Y) = \Pi_1(X, x_0) * \Pi_1(Y, y_0).$$

Par exemple si on prend $X = S^1$ et $Y = \Pi^2$, on obtient la chose suivante pour $X \wedge Y$.



3. On appelle B_n le bouquet de n cercles. Alors

$$\Pi_1(B_n) = \mathbb{F}_n = \langle a_1, \dots, a_n \rangle.$$

Plus généralement, si $X = (V, E)$ est un graphe connexe avec $n = |V|$, $m = |E|$ vu comme espace topologique en identifiant chaque arête à une copie de $[0, 1]$, alors

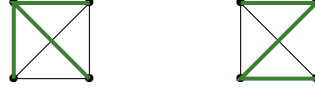
$$\Pi_1(X) \cong \mathbb{F}_{m-n+1}.$$

Par exemple si G est le graphe suivant :



$$\Pi_1(G) = \mathbb{F}_{6-4+1} = \mathbb{F}_3.$$

En effet, soit \mathcal{T} un **arbre maximal** de X (un **arbre maximal** est un sous-graphe de X , sans circuit passant par tous les sommets). En contractant \mathcal{T} sur un point, on obtient un bouquet à $m - n + 1$ cercles, car \mathcal{T} a $n - 1$ arêtes.



Ci-dessus on a des arbres maximaux, car il reste 3 arêtes quand on contracte les arêtes vertes (on obtient donc un bouquet à 3 arêtes, dont le Π_1 est \mathbb{F}_3).



5.4. Revêtements

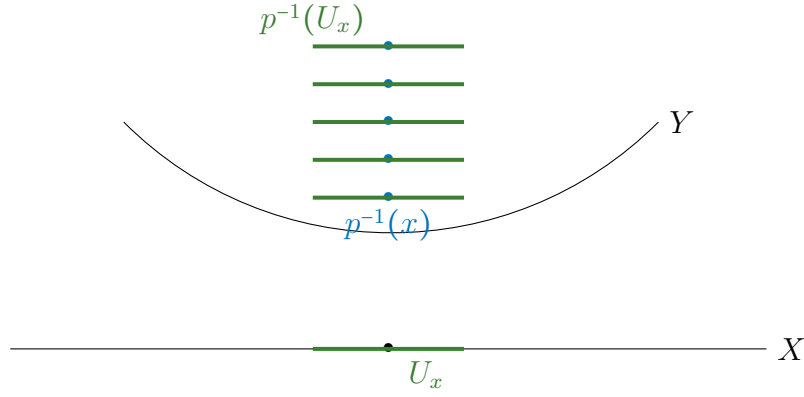
Tous les espaces sont supposés connexes par arcs et localement connexes par arcs.

Définition 5.18. Un triplet (X, Y, p) , noté $\begin{smallmatrix} Y \\ \downarrow p \\ X \end{smallmatrix}$ est un **revêtement** de X si :

- p est une application continue surjective $Y \rightarrow X$.
- Pour tout $x \in X$, $p^{-1}(x)$ est discret dans Y .
- Tout $x \in X$ possède un **voisinage trivialisant** U_x , c'est-à-dire un voisinage connexe par arcs tel que $p^{-1}(U_x)$ est homéomorphe à $p^{-1}(x) \times U_x$, par un homéomorphisme $h_x : p^{-1}(U_x) \rightarrow p^{-1}(x) \times U_x$ tel que le diagramme suivant commute (où p_2 est la projection sur le 2ème facteur).

$$\begin{array}{ccc} p^{-1}(U_x) & \xrightarrow{h_x} & p^{-1}(x) \times U_x \\ & \searrow & \swarrow p_2 \\ p|_{p^{-1}(U_x)} & & U_x \end{array}$$

L'image mentale d'un revêtement est celle de la "pile d'assiettes".

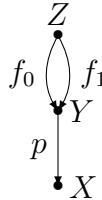


On dira que $\downarrow_X^Y p$ est un **revêtement à n feuillets** si $\#p^{-1}(x) = n$, et a **une infinité de feuillets** si $\#p^{-1}(x) = \infty$.

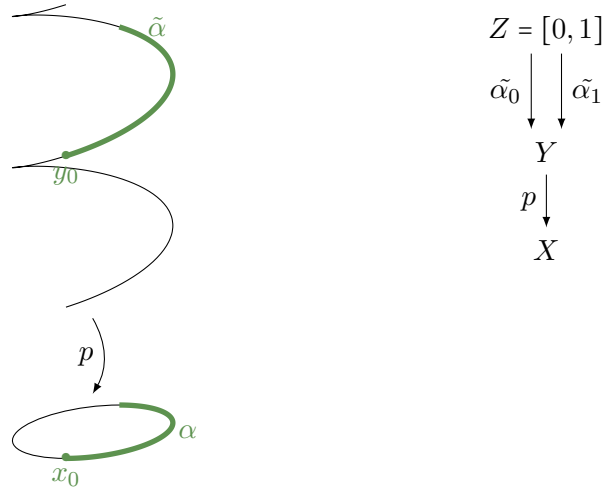
- Exemples 5.19.**
1. Soit $X = \{z \in \mathbb{C} \mid |z| = 1\}$. Alors l'espace Y peut être représenté par une hélice, mais $Y = \mathbb{R}$. Alors $p: \mathbb{R} \rightarrow \mathbb{S}^1$ est défini par $p(t) = e^{2\pi i t}$ et $\downarrow_X^Y p$ est un revêtement car p est surjective. Si $z = e^{2\pi i \varphi}$, alors $p^{-1}(z) = \varphi + \mathbb{Z}$ est discret dans \mathbb{R} . Enfin, si $z = e^{2\pi i \varphi} \in S^1$, $U_z = S^1 \setminus \{-z\}$ (tout le cercle sauf le point opposé à z) est un voisinage de z , et $p^{-1}(U_z) = \mathbb{R} \setminus \{\varphi + (2k+1)\pi, k \in \mathbb{Z}\} \cong \mathbb{Z} \times U_z$ car $\mathbb{Z} = p^{-1}(z)$. On ne prend pas les multiples impairs de π car on ne veut pas $z + \pi, z - \pi, z + 3\pi, \dots$ dans le revêtement.
 2. Soit $X = S^1$, $Y = S^1$ et $p: S^1 \rightarrow S^1$, $z \mapsto z^n$ avec $n > 0$ et un revêtement à n feuillets. On parcourt le cercle n fois, et on arête au même point qu'on a commencé.
 3. Si x est un bouquet à deux boucles, alors $Y_{1,n}$ défini comme suit est un revêtement à n feuillets. $Y_{1,\infty}$ a une infinité de feuillets. Y_2 vu comme \mathbb{Z}^2 (le réseau à coordonnées entières) est aussi un revêtement à une infinité de feuillets.



Lemme 5.20. Soit $\downarrow_X^Y p$ un revêtement. Soit Z un espace connexe et soient $f_0, f_1: Z \rightarrow Y$ deux applications continues avec $p \circ f_0 = p \circ f_1$. Alors $\{z \in Z \mid f_0(z) = f_1(z)\} = \emptyset$ ou Z .



Preuve. Exercice.



□

Lemme 5.21 (RELÈVEMENT DES CHEMINS). Soient $x_0 \in X$, $y_0 \in p^{-1}(x_0)$. Pour tout chemin $\alpha : [0, 1] \rightarrow X$ avec $\alpha(0) = x_0$, il existe un unique chemin $\tilde{\alpha} : [0, 1] \rightarrow Y$ avec $\tilde{\alpha}(0) = y_0$ et $p \circ \tilde{\alpha} = \alpha$. On appelle $\tilde{\alpha}$ le **relèvement** de α .

Preuve. Commençons par montrer l'unicité. Elle résulte du Lemme 5.20. Supposons que $Z = [0, 1]$ et que $\tilde{\alpha}_0$ et $\tilde{\alpha}_1$ sont deux relèvements de α , $\tilde{\alpha}_0, \tilde{\alpha}_1 : Z = [0, 1] \rightarrow Y$ avec $\tilde{\alpha}_0(0) = \tilde{\alpha}_1(0) = y_0$. Alors par le Lemme 5.20, on a que $\tilde{\alpha}_0(z) = \tilde{\alpha}_1(z)$ pour tout $z \in Z$.

La partie existence est en exercice.

□

Lemme 5.22 (RELÈVEMENT DES HOMOTOPIES). Soient $\alpha_0, \alpha_1 : [0, 1] \rightarrow X$ avec $\alpha_0(0) = \alpha_1(0) = x_0$ et $\alpha_0(1) = \alpha_1(1)$. Soient $\tilde{\alpha}_0, \tilde{\alpha}_1$ les relevés par y_0 . Si $\alpha_0 \sim \alpha_1$ dans X , alors $\tilde{\alpha}_0 \sim \tilde{\alpha}_1$ et ont la même extrémité.

Preuve. cf. feuille annexe.

□

Théorème 5.23. Soient $\begin{smallmatrix} Y \\ \downarrow p \\ X \end{smallmatrix}$ un revêtement, $y_0 \in p^{-1}(x_0)$. Alors

$$p_* : \Pi_1(Y, y_0) \rightarrow \Pi_1(X, x_0)$$

est injective (si $f : X \rightarrow Y$, on définit $f_* : \Pi_1(X, x_0) \rightarrow \Pi_1(Y, y_0)$ par $[\gamma] \rightarrow [f \circ \gamma]$). Ainsi $p_*(\Pi_1(Y, y_0))$ est un sous-groupe de $\Pi_1(X, x_0)$.

Preuve. Soit $[\tilde{\alpha}] \in \Pi_1(Y, y_0)$ avec $p_*[\tilde{\alpha}] = [\varepsilon_{x_0}]$. Par le Lemme 5.21, $\tilde{\alpha}$ est l'unique relèvement de $\alpha = p \circ \tilde{\alpha}$ (et ε_{y_0} est l'unique relèvement de ε_{x_0}). Par le Lemme 5.22, une homotopie entre α et ε_{x_0} se relève en une homotopie entre $\tilde{\alpha}$ et ε_{y_0} , donc $[\tilde{\alpha}] = [\varepsilon_{y_0}]$, ce qui montre que p_* est injective. \square

Ce théorème nous dit qu'un revêtement de X nous donne un sous-groupe de $\Pi_1(X)$. On a aussi une réciproque qui est le théorème suivant.

Théorème 5.24. *Soit X connexe par arcs, localement connexe par arcs (graphe). Alors pour H un sous-groupe de $\Pi_1(X, x_0)$, il y a un revêtement $\begin{smallmatrix} X_H \\ \downarrow p \\ X \end{smallmatrix}$ tel que*

$$p_*(\Pi_1(X_H, \tilde{x}_0)) \cong H.$$

Ceci veut dire que pour un sous-groupe de $\Pi_1(X)$, on peut trouver un revêtement de X .

Remarque 5.25. 1. X_H est unique à isomorphisme près!

2. On a donc un dictionnaire entre revêtements et sous-groupes de $\Pi_1(X)$. \clubsuit

Théorème 5.26 (DE NIELSEN-SCHREIER). *Soit F_n le groupe libre avec n générateurs, et soit H un sous-groupe de F_n . Alors*

1. H est libre ;
2. si $[F_n : H] = k$ (index de H dans F_n), alors $H \cong F_{k(n-1)+1}$, c'est-à-dire que H est libre sur $k(n-1) + 1$ générateurs.

Pour la deuxième partie de la preuve, on a besoin de la proposition suivante.

Proposition 5.27. *Le nombre de feuilles $\begin{smallmatrix} Y \\ \downarrow p \\ X \end{smallmatrix}$ est égal à*

$$[\Pi_1(X, x_0) : p_*(\Pi_1(Y, y_0))].$$

Preuve. Exercice 1, série 6. \square

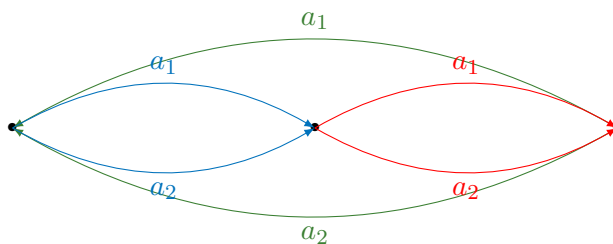
Preuve (DU THÉORÈME DE NIELSEN-SCHREIER). 1. F_n libre peut être vu comme le groupe fondamental d'un bouquet à n cercles. Pour chaque sous-groupe H de F_n , on a par le Théorème 5.24 un revêtement X_H tel que $p_*(\Pi_1(X_H)) = H$. On a vu que p_* est injective, donc on a vraiment l'isomorphisme $\Pi_1(X_H) \cong H$. Tout revêtement d'un graphe est un graphe, alors X_H est aussi un graphe. Mais le groupe fondamental d'un graphe est toujours libre, et ainsi H est libre.

2. Soit \mathbb{F}_n le groupe fondamental d'un bouquet à n boucles. Pour H un sous-

groupe de \mathbb{F}_n , il y a un revêtement X_H tel que $\Pi_1(X_H) \cong H$. Si $[\mathbb{F}_n : H] = k$, par la proposition 1 on a que X_H est un revêtement à k feuillets de X . Ainsi X_H est un graphe à k sommets et $k \cdot n$ arêtes. Ainsi $H = \Pi_1(X_H) \cong \mathbb{F}_{kn-k+1} = \mathbb{F}_{k(n-1)+1}$ où kn est le nombre d'arête et k est le nombre de sommets.

□

Exemple 5.28. Soit $n = 2$. Alors \mathbb{F}_2 est le groupe fondamental du bouquet à deux boucles, qu'on appelle a_1 et a_2 . Pour $k = 3$, on a le revêtement X_H suivant :



X_H a k sommets de degré $2n$ et a $\frac{k \cdot 2n}{2} = k \cdot n$ arêtes.

★

Chapitre 6.

Transformations de Tietze

Définition 6.1. Soit $\langle X_1, \dots, X_n | \underbrace{r_1, \dots, r_m}_R \rangle$ une présentation finie d'un groupe G .
Les transformations suivantes, appelées **transformation de Tietze**, changent la présentation sans changer le groupe.

Algorithm 6.1 Première transformation de Tietze

T_1 ou R^+ : Ajouter à la présentation de G un relateur r_{m+1} qui appartient à la clotûre normale de R (notée \overline{R} , $\triangleleft R \triangleright$ ou $gp_G(R)$).

Soit $r_{m+1} \in \overline{R} \setminus R$: $\langle X | R \rangle \xrightarrow{R^+, T_1} \langle X | R \cup \{r_{m+1}\} \rangle$.

|| **Exemple 6.2.** Considérons $\mathbb{Z}^2 = \langle a, b | aba^{-1}b^{-1} \rangle \xrightarrow{R^+} \langle a, b | [a, b], [a, b]^2 \rangle$.



Algorithm 6.2 Deuxième transformation de Tietze

R^- : Opération inverse de R^+ .

Soit $r \in R \setminus \overline{R} \setminus \{r\}$. Alors $\langle X | R \rangle \xrightarrow{R^-} \langle X | R \setminus \{r\} \rangle$.

Algorithm 6.3 Troisième transformation de Tietze

X^+ : Ajouter à la présentation de G un générateur x_{n+1} ainsi qu'une relation $x_{n+1} = w(x_1, \dots, x_n)$ (un mot sur x_1, \dots, x_n).

$\langle X | R \rangle \xrightarrow{X^+} \langle X, x_{n+1} | R \cup \{x_{n+1}w^{-1}(x_1, \dots, x_n)\} \rangle$

|| **Exemple 6.3.** Soit $G = \langle x, y | xyx = yxy \rangle$. C'est le groupe fondamental du noeud

Algorithm 6.4 Quatrième transformation de Tietze

X^- : Opération inverse de X^+ .

Soit $y \in X$, $w \in \langle X \setminus \{y\} \rangle$ et $y^{-1}w$ est le seul mot dans R qui contient y . Alors

$$\langle X|R \rangle \xrightarrow{X^-} \langle X \setminus \{y\} | R \setminus \{y^{-1}w\} \rangle.$$

de trèfle. On va utiliser les transformations de Tietze. On a

$$\begin{aligned} \langle x, y | xyx = yxy \rangle &\xrightarrow{X^+} \langle x, y, a, b | xyx = yxy, a = xy, b = yx \rangle \\ &\xrightarrow{R^+} \langle x, y, a, b | xyx = yxy, a = xy, b = yx, x = a^{-1}b, y = b^{-1}b^{-1}a^2, a^3 = b^2 \rangle \quad a^3 = xyxyxy \\ &\xrightarrow{R^-} \langle x, y, a, b | a^3 = b^2, x = a^{-1}b, y = b^{-1}a^2 \rangle \\ &\xrightarrow{X^-} \langle a, b | a^3 = b^2 \rangle. \end{aligned}$$

Cette dernière présentation correspond au produit libre amalgamé. ★

Proposition 6.4 (DE TIETZE). *Les transformations de Tietze ne changent pas le groupe.*

Preuve (POUR X^+). Supposons que $G = \langle X|R \rangle$, y est un symbole qui n'est pas dans X , et $w(X)$ un mot réduit de $\mathbb{F}(X)$. On veut montrer que $\langle X, y | R \cup \{y^{-1}w(X)\} \rangle \cong \langle X, R \rangle = G$.

Soit $\varphi : \mathbb{F}(X) \rightarrow G$ l'homomorphisme donné par la propriété universelle des groupes libres. Le groupe libre $\mathbb{F}(X, y)$ sur $X \cup \{y\}$ est engendré librement par $X \cup \{y^{-1}w(X)\}$. C'est-à-dire que $\mathbb{F}(X \cup \{y\}) = \mathbb{F}(X \cup \{y^{-1}w(X)\})$. C'est vrai car à partir de $y^{-1}w(X)$, on peut obtenir y (cette inclusion est sensée être facile), et à partir de y on peut obtenir $y^{-1}w(X)$. Ainsi on a

$$X \cup \{y^{-1}w(X)\} \hookrightarrow \mathbb{F}(X, y) = \mathbb{F}(X \cup \{y^{-1}w(X)\}).$$

Il y a un unique homomorphisme $\varphi^1 : \mathbb{F}(X, y) \rightarrow G$ tel que $\varphi^1(x) = \varphi(x)$ et $\varphi^1(y^{-1}w(X)) = 1$ pour $x \in X$.

$$\begin{array}{ccc} X \cup \{y^{-1}w(X)\} & \longrightarrow & \mathbb{F}(X, y) = \mathbb{F}(X \cup \{y^{-1}w(X)\}) \\ \downarrow f & \nearrow \varphi^1! & \downarrow \chi \\ G & \xleftarrow{\varphi} & \mathbb{F}(X) \end{array}$$

($f(x) = x$ si $x \in X$ et 1 si $x = y^{-1}w(X)$). L'homomorphisme $\varphi^1 : \mathbb{F}(X, y) \rightarrow G$ se factorise comme $\mathbb{F}(X, y) \xrightarrow{\chi} \mathbb{F}(X) \xrightarrow{\varphi} G$ où $\chi(x) = x$ pour tout $x \in X$ et $\chi(y) = w(x)$. Alors φ^1 est surjective et

$$\ker \varphi^1 = \chi^{-1}(\varphi^{-1}(1)) = \chi^{-1}(gp_{\mathbb{F}(X)}R) = gp_{\mathbb{F}(X, y)}(R \cup \{y^{-1}w(X)\}).$$

Ainsi par le premier théorème d'isomorphisme, on a que

$$G \cong \mathbb{F}(x, y) / \ker \varphi^1 = \langle X, y | R \cup \{y^{-1}w(X)\} \rangle.$$

□

Théorème 6.5 (DE TIETZE). *Soient $\mathcal{P}_1 = \langle X | R \rangle$ et $\mathcal{P}_2 = \langle Y | S \rangle$ des présentations finies pour un groupe G . Alors il existe une suite finie de transformations de Tietze qui transforment \mathcal{P}_1 en \mathcal{P}_2 .*

Preuve. cf. feuille annexe. G est donné par \mathcal{P}_1 et \mathcal{P}_2 . Alors chaque $x \in X$ peut être écrit comme un mot sur Y , et on note $x(Y)$. Alors $X(Y)$ représente tous les mots sur Y qui décrivent les éléments de X . De la même manière, on définit $y(X)$ et $Y(X)$.

On commence avec \mathcal{P}_1 et on utilise les transformations suivantes (voir feuille annexe).

Intuitivement, on ajoute tous les générateurs Y et on enlève tous les générateurs X . On utilise les transformations $R^+ |X| + |R| + |Y| + |S|$ fois et $R^- 2(|R| + |Y|)$ fois. Donc il y a un nombre fini de transformations de \mathcal{P}_1 à \mathcal{P}_2 . □

Corollaire 6.6. *On peut énumérer toutes les présentations finies d'un groupe G à partir d'une présentation quelconque pour G .*

Proposition 6.7. *Si le groupe G a une présentation finie $\langle X_1 | R \rangle$ et une présentation infinie $\langle X_2 | S \rangle$ où S est infini, alors il existe un entier n tel que $\langle X_2 | s_1, \dots, s_n \rangle$ est une présentation finie pour G .*

6.1. Algorithme de Todd-Coxeter (1936) (Coset enumeration)

Étant donné un groupe G , défini par une présentation finie $G = \langle X, R \rangle$, et un sous-groupe H de G d'indice fini dans G , on souhaite énumérer les éléments du quotient G/H et décrire l'action de G sur G/H .

6.1.1. Version basique

Si $H = \{1\}$, l'algorithme va énumérer les éléments de G , si G est fini.

Algorithm 6.5 Algorithme de Todd-Coxeter (basique)

$\forall r \in R$, créer un tableau de $|r| + 1$ colonnes.

Si $r = x_1 \cdots x_n$, le tableau est

	x_1	x_2	\cdots	x_1^{-1}	x_n	
1	-	2	\cdots	2	1	1
2						2

Définition	Bonus
$1x_1 = 2$	

On pose 1 dans la première et la dernière colonne (1 pour 1_G)


On pose 2 à la droite de 1, ça s'appelle la « définition » de 2 et on le pose dans un autre tableau, qui s'appelle le **tableau de définitions**. La notation $1x_1 = 2$ ou $2x_1^{-1} = 1$ ($1 = 1_G$, $2 = x_1$).

On pose 2 dans la première et la dernière colonne, deuxième ligne.

S'il y a un 2 à la gauche de x_1^{-1} , on pose 1 à droite de ce 2.

S'il y a un 2 à la droite de x_1 , on pose 1 à la gauche de x_1 .

On pose 3, 4, ... dans le tableau jusqu'à ce qu'il n'y ait plus d'espaces vides.

Remarque 6.8. Chaque nombre $1, 2, 3, \dots$ représente un élément de G . 

Remarque 6.9. Supposons qu'on ait une définition $ix_l = j$, et dans le tableau on ait aussi k à la droite de x_{l+1} , on a $kx_{l+1}^{-1} = j \iff jx_{l+1} = k$. On appelle cela un **bonus**.


x_p	x_{p+1}
i - j	= k

Dans le tableau, on note - quand on a une définition, et = lorsqu'on a un bonus. 

Exemple 6.10. Soit $G = \langle x \mid x^4 = 1 \rangle \cong \mathbb{Z}/4\mathbb{Z}$. L'unique relateur est x^4 .

x	x	x	x
1 - 2 - 3 - 4 = 1			
2	3	4	1
3	4	1	2
4	1	2	3

Définition	Bonus
$1x = 2$	
$2x = 3$	
$3x = 4$	$4x = 1$

Donc $|G| = 4$, avec $1 = 1_g$, $2 = x$, $3 = x^2$ et $4 = x^3$. 

Théorème 6.11. Si G est fini, l'algorithme de Todd-Coxeter s'arrête avec un tableau complet pour chaque relateur après un nombre fini d'étapes.

L'ensemble de sortie donné par l'algorithme contient tous les éléments de G , mais aussi l'action à droite de générateurs de G sur G .

6.1.2. Version générale

Soit $G = \langle X | R \rangle$, H un sous-groupe de G et $H \neq \{1\}$. Si $H = \langle Y \rangle$, alors H est donné par un ensemble Y de générateurs qui sont des mots sur X .

But : On obtient $|G : H|$ si $|G : H| < \infty$, l'action de G sur G/H , et un ensemble de représentants de classes à droite de H .

Algorithm 6.6 Algorithme de Todd-Coxeter

L'algorithme est le même que celui de la version basique, mais on ajoute un tableau pour chaque générateur de H .

L'algorithme se termine quand tous les espaces dans les tableaux des relateurs sont remplis.

$|G : H|$ = nombre de lignes en chaque tableau.

Exemple 6.12. Soit $G = \langle x | x^6 = 1 \rangle$, $H = \langle x^3 \rangle$. Ici, $1 = H$.

x	x	x	x	x	x
1	-	2	-	3	1
2		3		1	2
3		1		2	3

x	x	x
1	2	3 = 1

Définition	Bonus
$1x = 2$	
$2x = 3$	$3x = 1$

On a 3 lignes donc $|G : H| = 3$. Les classes à droites sont $1 = H$, $2 = Hx$ et $3 = Hx^2$.
Les représentants sont $\{1, x, x^2\}$. ★

Exemple 6.13. Soit $G = \langle x, y | x^3 = 1, y^3 = 1, (xy)^2 = 1 \rangle$ et $H = \langle x \rangle$.

Tableaux pour H et $x^3 = 1$:

x
1 = 1

x	x	x
1	1	1
2	3	4 = 2
3	4	2
4	2	3

Tableaux pour y^3 et $(xy)^2$

y	y	y	
1	-	2	- 3 = 1
2		3	1 2
3		1	2 3
4		4	4 4

x	y	x	y	
1	1	2	3	1
2	=	3	1	1 2
3		4	4	2 3
4		2	3	4 4

Tableau des définitions et bonus :

Définition	Bonus
	$1x = 1$
$1y = 2$	
$2y = 3$	$3y = 1, 2x = 3$
$3x = 4$	$4x = 2, 4y = 4$

On voit donc que $|G : H| = 4$ et les classes de H sont $1 = H$, $2 = Hy$, $3 = Hy^2$ et $4 = Hy^2x$. Il y a une action de G sur $G/H = \{1, 2, 3, 4\}$, c'est-à-dire qu'il y a un homomorphisme $\alpha : G \rightarrow \text{Sym}(4)$, $x \mapsto \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix} = \alpha(x)$ et $y \mapsto \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} = \alpha(y)$. Ainsi l'ordre de x $\text{ord}(x) \geq \text{ord}(\alpha(x)) = 3$, mais $x^3 = 1$ dans G donc $\text{ord}(x) = 3$. Comme $|H| = |\langle x \rangle| = 3 \Rightarrow |G| = |H||G : H| = 3 \cdot 4 = 12$. Mais $\langle (234), (123) \rangle \cong \text{Alt}(4)$ et α est injective, surjective et ainsi $G \cong \text{Alt}(4)$. ★

Exemple 6.14. Soit $G = F(2, 5) = \langle x, a, b, c, d | xa = b, ab = c, bc = d, cd = x, dx = a \rangle$ et soit $H = \langle x \rangle$. Le tableau pour H est simplement $1x = 1$, et donc c'est notre premier bonus.

Tableaux pour $xa = b$ et $ab = c$.

x	a	b^{-1}	
1	1	-	3 = 1
2		3	2
3			2 3

a	b	c^{-1}	
1	3	=	2 1
2		1	3 = 2
3			3 3

Tableaux pour $bc = d$ et $cd = x$.

b	c	d^{-1}	
1	3	≡	2 1
2			1 2
3	2	3	= 3

c	d	x^{-1}	
1	-	2	= 1 1
2		3	3 = 2
3			3 3

Tableau pour $dx = a$:

d	x	a^{-1}	
1	=	2	3 1
2		3	1 = 2
3		3	3 3

Tableau des définitions et bonus et tableau des relations

Définition	Bonus
$\underline{1c = 2}$	$1x = 1$
$1a = 3$	$2d = 1, 2a = 1$
	$1b = 3, 3b = 2, 2c = 3, 3d = 3$
	$2x = 3, 1d = 2, \underline{3c = 2}$

	x	a	b	c	d
1	1	3	3	2	2
2	3	1		3	1
3			2		3

À ce point, on déduit que $1 = 2c^{-1} = 3$, d'où $3 = 1b = 3b = 2$ et les tableaux se réduisent chacun à une ligne. Le second tableau de référence nous dit que chacun des cinq générateurs fixe 1 [voir feuille annexe pour détail, pas trop compris pourquoi], ainsi $F(2, 5) = \langle x \rangle$ et est donc abélien. Comme on sait déjà que le « derived factor group » de $F(2, 5)$ est Z_{11} , on en déduit que $F(2, 5) \cong Z_{11}$.

En fait on trouve que $G = H = \langle x \rangle$.

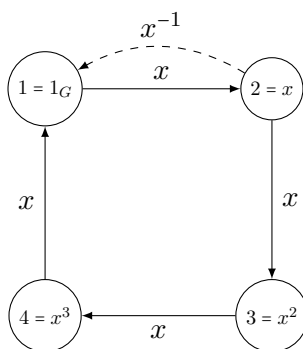


6.2. Algorithme de Todd-Coxeter pour les graphes

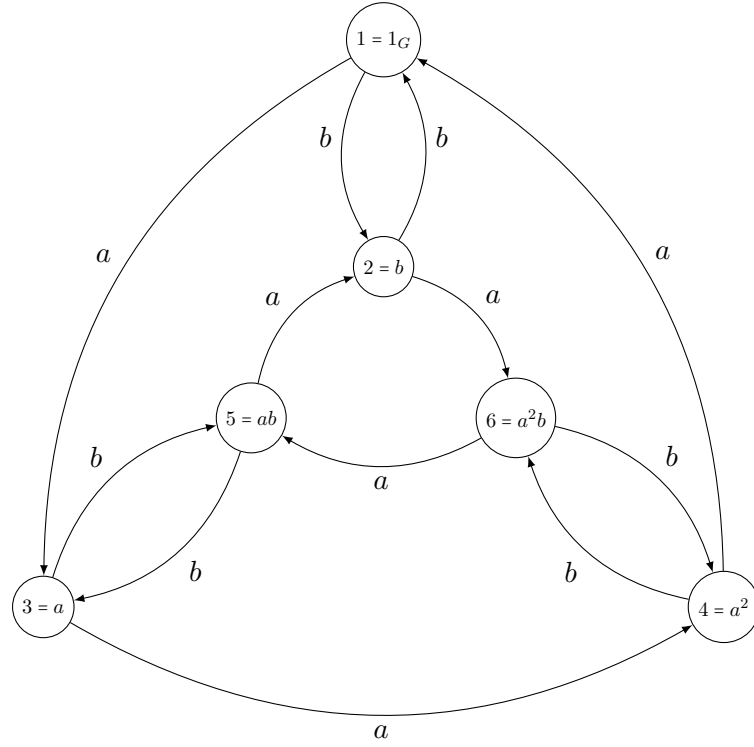
On utilise des graphes au lieu de tableaux.

6.2.1. $H = \{1\}$

Exemples 6.15. 1. Soit $G = \langle x | x^4 = 1 \rangle$.



2. Soit $G = \langle a, b | a^3 = 1, b^2 = 1, ab = ba^{-1} \iff abab^{-1} = 1 \iff abab = 1 \rangle$. C'est en fait $Sym(3)$.

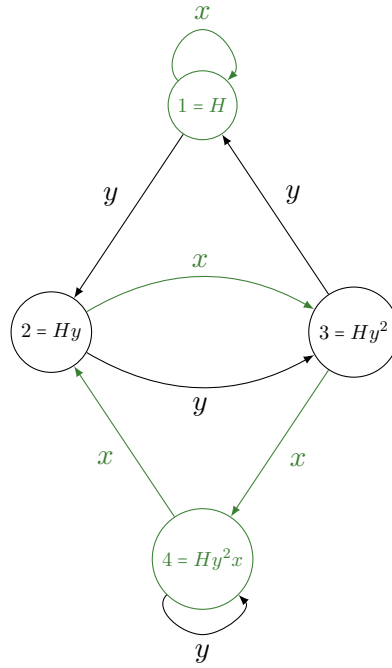


Pour $|G| < \infty$, l'algorithme de Todd-Coxeter (pour $H = \{1\}$) nous donne le **graphe de Cayley** (avec les générateurs dans la présentation).

6.2.2. $H \neq \{1\}$ et $|G : H| < \infty$

L'algorithme nous donne le **graphe de Schreier** de H dans G . Les sommets sont les classes de H et les arêtes correspondent à l'action de G sur le quotient G/H .

Exemple 6.16. Soit $G = \langle x, y | x^3 = y^3 = (xy)^2 = 1 \rangle$ et soit $H = \langle x \rangle$.



On a quatre classes, donc l'indice est 4. H n'est pas normal dans G , ainsi G/H n'est pas nécessairement un groupe, mais juste un ensemble de classes.

Raisonnement pour le graphe : On cherche ce que vaut $Hxyxy$. Comme $Hx = H$, on en déduit que $Hyxy = H$. On doit donc définir $2x = 3$.

On cherche Hy^2xy . Mais $xy = y^{-1}x^{-1}$, ainsi $Hy^2xy = Hyx^2 = 4$.



Chapitre 7.

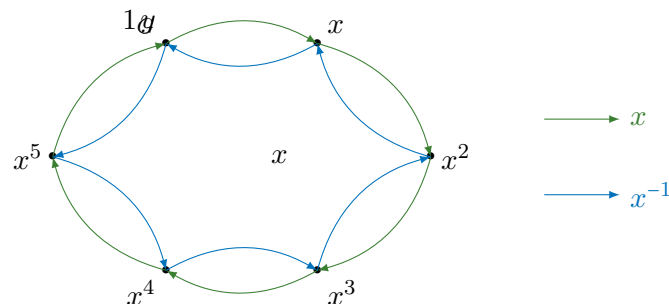
Graphes de Cayley (groupes comme espaces métriques)

Soit G un groupe, $S \subset G$ une partie symétrique ($s \in S \Rightarrow s^{-1} \in S$) et $1 \notin S$.

Définition 7.1. Le **graphe de Cayley**, noté $\Gamma(G, S)$ est le graphe dont l'ensemble des sommets est G et l'ensemble des arêtes est $E = \{(x, y) | xy^{-1} \in S \iff \exists s \in S : y = xs\}$.

Deux sommets sont **voisins**, et on les notes $x \sim y$, si y s'obtient à partir de x par multiplication par un élément de S .

Exemples 7.2. 1. Soit $G = \mathbb{Z}/6\mathbb{Z}$ et $S = \{x, x^{-1}\}$, pour $x = 1$ et $x^{-1} = 5$.



2. Soit $G = \mathbb{Z}/6\mathbb{Z}$ et $S = \{2, -2\}$.

3. Soit $G = \mathbb{Z}/6\mathbb{Z}$ et $S = \{3 = -3\}$.

4. Soit $G = \mathbb{Z}/6\mathbb{Z}$ et $S = \{2, -2, 3 = -3\}$.

5. Soit $G = \mathbb{Z}$ et $S = \{1, -1\}$.

6. Soit $G = \mathbb{Z}^2$ et $S = \{(\pm 1, 0), (0, \pm 1)\}$.

7. Soit $G = \mathbb{F}_2 = \mathbb{F}(a, b)$ le groupe libre avec 2 générateurs et soit $S = \{a^{\pm 1}, b^{\pm 1}\}$.



Propriétés 7.3. 1. $\Gamma(G, S)$ est k -régulier, où $k = |S|$ (c'est-à-dire tout sommet a

- k voisins).
2. $\Gamma(G, S)$ et connexe $\iff S$ engendre G .

Définition 7.4. Un **arbre** un graphe connexe sans chemins fermés.

Proposition 7.5. Soit G un groupe et $S \subseteq G$ un ensemble. Alors $G \cong \mathbb{F}(S)$ (le groupe libre sur S) si et seulement si $\Gamma(G, S)$ est un arbre.

Définition 7.6. Soient $\Gamma_1 = (V_1, E_1)$ et $\Gamma_2 = (V_2, E_2)$ deux graphes. Un **morphisme de graphe** est une application $\varphi : \Gamma_1 \rightarrow \Gamma_2$, $\varphi|_V : V_1 \rightarrow V_2$, $\varphi|_E : E_1 \rightarrow E_2$ telle que $(\varphi(v), \varphi(v')) \in E_2 \iff (v, v') \in E_1$.

Si φ est bijective et $\Gamma_1 = \Gamma_2$, φ s'appelle un **automorphisme de graphe**.

L'ensemble de tous les automorphisme de Γ , noté $Aut(\Gamma)$ forme un groupe.

Théorème 7.7. Soit G un groupe dénombrable. Alors il y a un graphe connexe X tel que $G \cong Aut(X)$.

Preuve. Soit $S = \{s_1, s_2, \dots\}$ un ensemble dénombrable de générateurs, c'est-à-dire que $G = \langle S \rangle$. Soit $X_0 = \Gamma(G, S)$ le graphe de Cayley de G par rapport à S . Il faut se convaincre que $G \not\cong Aut(X_0)$.

Pour chaque $i \geq 1$, soit T_i un arbre fini (qui correspond à s_i)

Figure de T_i ici.

Si $i \neq j$, on a que $T_i \not\cong T_j$, car on n'a pas le même nombre de sommets dans T_i et T_j . On doit montrer que $Aut(T_i) = \{id\}$ (exercice).

Dans le graphe de Cayley X_0 , on remplace chaque arête s_i par T_i , par exemple

Dessiner exemple ici

et on obtient un graphe X . On a ainsi une expansion de X_0 vers X ainsi qu'une contraction de X vers X_0 (en remplaçant T_i par s_i). On observe que chaque automorphisme $\varphi : X \rightarrow X$ induit un automorphisme $\varphi_0 : X_0 \rightarrow X_0$.

1. Si $\gamma \in Aut(X)$ fixe $x \in V(X)$ ($\gamma(x) = x$), alors $\gamma = id_X$. En effet, si $x \in V(X) \setminus V(X_0)$ et $\gamma(x) = x$, alors $x \in V(T_i) \setminus \{a_i, b_i\}$. Ainsi $\gamma(T_i) = T_i$. Supposons que $x \in V(X_0)$ et $\gamma(T_{x,j}) = T_{x,j}$ pour chaque $x \in T_{x,j}$. L'idée est que si on fixe un tel x , on est obligé de fixer l'arbre $T_{x,j}$ (car deux arbres différents ne sont pas isomorphes), ainsi on fixe tous les arbres, donc toutes les arêtes et ainsi on fixe xs_i pour chaque i , et par le Lemme de Zorn (car c'est un arbre infini, donc on doit faire ce processus à l'infini), on fixe l'arbre. C'est-à-dire que $\gamma(X) = X$, donc $\gamma = id$.

2. $\text{Aut}(X) \cong G$. Soit $\varphi : G \rightarrow \text{Aut}(X)$, $g \mapsto \varphi_g$ où $\varphi_g : X \rightarrow X$ est une extension de $\varphi_g^0 : X_0 \rightarrow X_0$ et $\varphi_g^0(v) = gv$ si $v \in V(X_0) = G$. Commençons par montrer que φ est injective. On a

$$\begin{aligned}\varphi(g) = \varphi(g') &\iff \varphi_g(v) = \varphi_{g'}(v) \\ &\iff gv = g'v \\ &\iff g = g'\end{aligned}$$

Montrons à présent que φ est surjective. Soit $\psi \in \text{Aut}(X)$ avec $\psi(v) = v'$ pour $v, v' \in X_0$, alors il existe $g \in G$ tel que $\varphi_g(v) = v'$ (par exemple on prend $g = v'v^{-1}$). On a $\psi(v) = \varphi_g(v)$, et ainsi $(\psi^{-1}\varphi_g)(v) = v$ et par la première observation, $\psi^{-1}\varphi_g = \text{id}$ et donc $\psi = \varphi_g$. \square

Remarque 7.8. Si on change l'ensemble S , les graphes de Cayley pour G sont différents entre eux (c'est-à-dire qu'ils ne sont pas isomorphes, en général). Mais ils sont **quasi-isométriques** \clubsuit

À présent, on supposera toujours que S engendre G (sinon le graphe n'est pas connexe, et on n'a pas des bonnes propriétés).

Définition 7.9. Soit $g \in G$. La **longueur** des mots de g est la distance de g à ε dans $\Gamma(G, S)$.

$$|g|_S := \min\{n \in \mathbb{N} \mid g = s_1 \cdots s_n, s_i \in S\}.$$

Pour $g \in G$, la **distance** de x à y est celle dans $\Gamma(G, S)$, notée $d_S(x, y) = |x^{-1}y|_S$.

- Observations 7.10.**
1. $d_S : G \times G \rightarrow \mathbb{N}$ est une distance sur G , invariante par l'action à gauche de G , $d_S(gx, gy) = d_S(x, y)$.
 2. Cette distance dépend du choix d'un système de générateurs S . Mais on va voir qu'en regardant le groupe « de loin », plusieurs propriétés importantes ne dépendent pas de S (Gromov, ~ 1980).

Exemple 7.11. Considérons $G = \mathbb{Z}$ et $S = \{\pm 1\}$. Le graphe de Cayley est simplement une droite infinie à gauche et à droite. Si à présent on considère $S' = \{\pm 2, \pm 3\}$, le graphe de Cayley devient



7.1. Quasi-isométries

Soient (X, d) , (X', d') deux espaces métriques.

Définition 7.12. Une application $f : X \rightarrow X'$ est une **quasi-isométrie** s'il existe $g : X' \rightarrow X$ et des constantes $\lambda > 0$, $c \geq 0$ telles que

1. $d'(f(x), f(y)) \leq \lambda d(x, y) + c$ pour tous $x, y \in X$;
2. $d(g(x'), g(y')) \leq \lambda d'(x', y') + c$ pour tous $x', y' \in X'$;
3. $d(g(f(x)), x) \leq c$ pour tout $x \in X$;
4. $d'(f'(g'(x')), x') \leq c$ pour tout $x' \in X'$.

Les deux premières inégalités disent que f, g sont Lipschitziennes à grande échelle. Les deux dernières disent que f, g sont **quasi-inverses** l'une de l'autre. On dit que (X, d) et (X', d') sont **quasi-isométriques** s'il existe une quasi-isométrie $f : X \rightarrow X'$.

- Exemples 7.13.**
1. Soit $X = \mathbb{R}$ et $X' = \mathbb{Z}$. Considérons $f(x) = [x]$ (partie entière de x). Alors f est une quasi-isométrie (qi) avec $\lambda = c = 1$.
 2. Un espace borné est qi à un point (si on regarde l'espace de très très loin, il est réduit à un point).
 3. **Exercice :** Être qi est une relation d'équivalence parmi les espaces métriques. ★

Proposition 7.14. Soient S, T deux parties génératrices finies de G . Les espaces $\Gamma(G, S)$ et $\Gamma(G, T)$ sont qi.

Preuve. L'idée de la preuve est que chaque $s \in S$ est un mot dans T . □

Proposition 7.15. Soit G un groupe et $H \leq G$ un sous-groupe de G d'indice fini ($|G : H| < \infty$). Alors G et H sont qi.

Preuve. On démontrera ce résultat comme corollaire d'autres résultats plus généraux. □

7.2. Actions propres

Définition 7.16. Soit G un groupe agissant par homéomorphismes sur un espace topologique séparé X . L'action de G sur X est **propre** si pour tout $K, L \subset X$ parties compactes

$$|\{g \in G \mid gK \cap L \neq \emptyset\}| < \infty.$$

Intuitivement, on ne peut pas avoir une infinité d'éléments des copies de K par l'action de G qui intersecte L .

Proposition 7.17. *Supposons que $K = L = \{x\}$, on voit que dans une action propre, tout stabilisateur est fini.*

$$\text{Stab}_G(x) = \{g \in G \mid gx = x\}.$$

Preuve. En fait on a que

$$\begin{aligned} \{gx\} \cap \{x\} \neq \emptyset &\iff \{gx\} \cap \{x\} = \{x\} \\ &\iff gx = x \end{aligned}$$

et donc c'est assez clair. □

Exemples 7.18. 1. Toute action d'un groupe fini est propre.

2. Si G agit sur X avec X compact, l'action est propre si et seulement si G est fini. Il suffit de prendre $K = L = X$.

3. L'action de \mathbb{Z}^n sur \mathbb{R}^n par translations est propre.

Preuve : Soient $K, L \subset \mathbb{R}^n$ deux parties compactes. Soit v tel que $(v+K) \cap L \neq \emptyset$ (ici on travaille avec des vecteurs, donc la translation est représentée par le "+"). si et seulement s'il existe $k \in K$ et $l \in L$ tels que $v + k = l$ ss'il existe $k \in K$ et $l \in L$ tels que $v = l - k$ si et seulement si $v \in L - K$ ($L - K = C$ est compact). Alors $v \in C \cap \mathbb{Z}^n$ est fini, ce qui conclut. ★

4. Si X est discret, l'action de G sur X est propre si et seulement si tous les stabilisateurs sont finis.

Preuve : Montrons que si tous les stabilisateurs sont finis, alors l'action de G sur X est propre. Si $K, L \subset X$ sont compacts, alors ils sont finis. On peut donc écrire $K = \{x_1, \dots, x_m\}$ et $L = \{y_1, \dots, y_n\}$. On a

$$gK \cap L \neq \emptyset \iff \exists i, j \text{ tq } gx_i = y_j.$$

$\{g \in G \mid gx_i = y_j\}$ est fini ; c'est une classe latérale de $\text{Stab}_G(x_i)$. ★

5. **Exercice :** Soit G un groupe agissant par multiplication à gauche sur (X, d) , on pose $\delta(Gx, Gy) = \inf\{d(gx, hy) \mid g, h \in G\}$. Montrer que δ est une distance sur l'espace des orbites $G \backslash X$ qui définit la topologie quotient. ★

Définition 7.19. Un espace métrique (X, d) est **géodésique** si pour tous $x, y \in X$ avec $\Delta = d(x, y)$, il existe $\gamma : [0, \Delta] \rightarrow X$ continue avec $\gamma(0) = x$, $\gamma(\Delta) = y$, et $d(\gamma(s), \gamma(t)) = |s - t|$ pour tous $s, t \in [0, \Delta]$. C'est équivalent à dire que deux points

quelconques peuvent être joints par un chemin géodésique, c'est-à-dire une isométrie d'un intervalle de \mathbb{R} dans X .

Exemples 7.20. 1. \mathbb{R}^n muni de la distance euclidienne est un espace géodésique.

2. Tous les espaces normés sont géodésiques.

Preuve : Soit X un espace normé et soit $\Delta = \|x - y\|$. On prend $\gamma(t) = x + \frac{t}{\Delta}(y - x)$, et donc $\|\gamma(s) - \gamma(t)\| = \frac{|s-t|}{\Delta} \|y - x\| = |s - t|$. ★

3. \mathbb{R}^2 muni de la norme $\|(x_1, x_2)\| = |x_1| + |x_2|$ n'est pas uniquement géodésique, c'est-à-dire qu'il existe en général plusieurs chemins géodésiques entre deux points.

4. $\mathbb{R}^2 \setminus \{(0, 0)\}$ muni de la métrique euclidienne n'est pas géodésique.

5. Un graphe étant un espace métrique discret se plonge de manière canonique dans un espace géodésique, sa **réalisation géométrique** obtenue en remplaçant chaque arête par une copie isométrique de l'intervalle $[0, 1]$.

5'. Les graphes de Cayley $\Gamma(G, S)$, $\langle S \rangle = G$ sont des espaces géodésiques. ★

7.3. Théorème fondamental de la théorie géométrique des groupes

Théorème 7.21 (EFREMOVICH (1953), ŠVARC (1959), MILNOR (1968)). *Soit X un espace métrique géodésique, dont les boules fermées sont compactes. Soit G un groupe agissant proprement par isométries sur X avec $G \setminus X$ compact. Alors G est finiment engendré et quasi-isométrique à X . Lemme de Milnor-Švarc*

Exemple 7.22. Soit $X = \mathbb{R}^n$ et $G = \mathbb{Z}^n$. On a une action propre de \mathbb{Z}^n sur \mathbb{R}^n par translations. En effet \mathbb{R}^n est un espace géodésique, les boules fermées sont compactes et les translations sont des isométries. Le quotient est compact et donc on a que \mathbb{Z}^n est finiment engendré et quasi-isométrique à \mathbb{R}^n . ★

Preuve (DE 7.21). Soit $\pi : X \rightarrow G \setminus X$, $x \mapsto Gx$ (orbite de x) la projection canonique. On met sur $G \setminus X$ la métrique $\delta(Gx, Gy) = \inf\{d(gx, hy) \mid g, h \in G\} = \inf\{d(kx, y) \mid k \in G\}$. Comme $G \setminus X$ est compact, le diamètre de $G \setminus X$ est fini. Posons

$$R := \sup\{\delta(Gx, Gy) \mid Gx, Gy \in G \setminus X\} < \infty.$$

Soit $x_0 \in X$ un point-base, et $B = B(x_0, R)$ la boule centrée en x_0 centrée en R . Soit $S = \{s \in G \mid s \neq 1, sB \cap B \neq \emptyset\}$, qui est un ensemble fini à cause de l'action propre de G , et de plus S est symétrique. Intuitivement, S représente les translations de B

qui intersectent B . Posons encore $r := \{\inf\{d(B, gB) \mid g \notin S \cup \{1\}\}\}$. Ce r est la plus petite distance entre un B est une translation de B qui n'intersecte pas B .

Assertion 1 : En fait, on a $r = \min\{d(B, gB) \mid g \notin S \cup \{1\}\} > 0$. En effet, soit $g' \in G$, $g' \notin S \cup \{1\}$; soit $r' = d(B, g'B) > 0$. Posons alors $T = \{g \in G \mid g \notin S \cup \{1\}, d(B, gB) \leq r'\}$. $T' \neq \emptyset$ car $g' \in T$. On va voir que T est fini. T est fini car $T \subset \{g \in G \mid gB(x_0, R+r') \cap B(x_0, R+r') \neq \emptyset\}$ qui est fini. En effet, il existe $x \in B$ et $g \in T$ tel que $d(x, gx) \leq r'$, donc si $x \in B$, $x \in B(x_0, R+r')$ et $d(x_0, gx) \leq d(x_0, x) + d(x, gx) \leq R + r'$. Ainsi $gx \in B(x_0, R+r')$. Ceci montre que $gx \in B(x_0, R+r') \cap gB(x_0, R+r')$. Comme r est l'infimum des nombres $d(B, gB) > 0$, pris sur T qui est fini, on a $r > 0$.

Exercice : $r \leq 2R$.

Soit $\lambda = \max_{s \in S} \{d(x_0, sx_0)\}$.

Assertion 2 : S engendre G et (*) $\frac{1}{\lambda}d(x_0, gx_0) \leq |g|_S \leq \frac{1}{r}d(x_0, gx_0) + 1$. Soit $g \in G$. Si $g \in S \cup \{1\}$, (*) est clair. Si $g \notin S \cup \{1\}$, soit k l'unique entier ≥ 0 tel que $R + (k-1)r \leq d(x_0, gx_0) \leq R + kr$ (**). Ce k existe car $d(x_0, gx_0) > R$. Comme X est géodésique, on peut trouver $x_1, \dots, x_k, x_{k+1} = gx_0$ dans X avec $d(x_0, x_1) \leq R$ et $d(x_i, x_{i+1}) < r$ pour $i = 1, \dots, k$. Ceci marche car on a $d(x_0, gx_0) \leq R + kr$, qui est ce qu'on veut. Comme $X = \bigcup_{g \in G} gB$, on peut choisir $g_0 = 1, g_1, \dots, g_k = g$ tels que $x_i \in g_{i-1}B$ pour $i = 1, \dots, k$. On pose $s_i = g_{i-1}^{-1}g_i$, ce qui veut dire que $s_i g_i^{-1} = g_{i-1}^{-1}$ et donc $g = s_1 s_2 \dots s_k$. On a $d(B, s_i B) \leq d(g_{i-1}^{-1}x_i, s_i g_i^{-1}x_{i+1}) = d(x_i, x_{i+1}) < r$. Par définition de r , $s_i \in S \cup \{1\}$ et donc S engendre G ! (On a $g_{i-1}^{-1}x \in B$ car $x \in g_{i-1}B$.) Pour la fin de la preuve, voir feuille annexe.

Observation : $d(x_0, g^{-1}hx_0) = d(gx_0, hx_0)$ (car la distance est invariante par actions à gauche). Ceci est la distance entre deux points dans l'orbite.

Ainsi (*) nous donne que

$$\frac{1}{\lambda}d(gx_0, gx_0) \leq d_S(g, h) \leq \frac{1}{r}d(gx_0, hx_0) + 1,$$

ce qui se traduit par le fait que G est qi à l'orbite Gx_0 , avec la métrique induite par d .

Assertion 3 : L'inclusion $f : Gx_0 \hookrightarrow X$ est une quasi-isométrie. On définit $f' : X \rightarrow Gx_0$ en envoyant un point $x \in X$ sur un point x' de Gx_0 à distance $\leq R$ de x , avec $f'(x) = x$ si $x \in Gx_0$. Alors

$$d(x, y) - 2R \leq d(f'(x), f'(y)) \leq d(x, y) + 2R.$$

Dessin distance orbite ici

On a que $f' \circ f = Id_{Gx_0}$, car si $x \in Gx_0$, alors $f'(f(x)) = x$. De plus $d(x, f(f'(x))) \leq R$, car pour tout $x \in X$, $f'(x) = x'$, $f(f'(x)) = f(x') = x'$. Ceci termine la preuve, car ainsi f et f' sont des qi. \square

Corollaire 7.23. *Soit G un groupe finiment engendré et soit H un sous-groupe d'indice fini. Alors H est finiment engendré, et q_i à G .*

Preuve. Exercice.



Chapitre 8.

Propriétés géométriques

Une propriété géométrique est une propriété invariante par quasi-isométries.

Définition 8.1. Deux groupes sont **commensurables** s'ils possèdent des sous-groupes d'indice fini isomorphes.

- Remarques 8.2.**
1. Pour les groupes finiment engendrés, deux groupes commensurables sont quasi-isométriques (à cause du corollaire précédent).
 2. En revanche, deux groupes quasi-isométriques n'impliquent pas qu'ils sont commensurables (en général).



- Exemples 8.3.**
1. Si F est un groupe fini, alors $\mathbb{Z} \times F$ et D_∞ sont commensurables, car ils possèdent tous les deux le sous-groupe \mathbb{Z} qui est d'indice fini.
 2. Pour $k, l \geq 2$, \mathbb{F}_k est commensurable à \mathbb{F}_l .



Définition 8.4. Soit (P) une propriété des groupes finiment engendrés. On dit que G est **virtuellement** (P) si G possède un sous-groupe H d'indice fini qui a la propriété (P) .

Exemple 8.5 (VIRTUELLEMENT LIBRE). Si G est virtuellement libre, alors G possède un sous-groupe H d'indice fini qui est libre.



- Exemples 8.6.**
1. « Être fini » est une propriété géométrique. Car G est fini ss'il est qi à $\{1\}$ et par transitivité, si H est qi à G , il est aussi qi à $\{1\}$ et donc fini.
 2. « Être cyclique infini », c'est-à-dire « être \mathbb{Z} », n'est pas une propriété géométrique. \mathbb{Z} et $\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ sont qi, mais le second n'est pas cyclique infini. De même pour \mathbb{Z} et D_∞ .



- Proposition 8.7.**
1. Être virtuellement \mathbb{Z} est une propriété géométrique.
 2. Être virtuellement libre est une propriété géométrique.
 3. Être virtuellement abélien est une propriété géométrique.
 4. Avoir une présentation finie est une propriété géométrique.
 5. Avoir un problème des mots résolubles est une propriété géométrique.
 6. Être virtuellement nilpotent est une propriété géométrique.

La proposition est difficile à prouver, mais pour quelques assertions, on peut le montrer en utilisant la croissance des groupes.

8.1. Croissance des groupes

Soit G un groupe finiment engendré et $S = S^{-1}$ une partie finie symétrique génératrice de G .

Définition 8.8. La fonction de croissance de G par rapport à S est

$$V_S : \mathbb{N} \rightarrow \mathbb{R}^+ (\mathbb{N}^+), \quad n \mapsto |B_S(n)|$$

où $B_S(n) = \{g \in G \mid |g|_S \leq n\}$.

Exemples 8.9. 1. Si G est fini, alors $V_S(n)$ est constant pour $n \gg 0$

2. Si $G = \mathbb{Z}$ et $S = \{\pm 1\}$,

Dessin ici

alors $V_S(n) = 2n + 1$.

3. Si $G = \mathbb{Z}^2$ avec $S = \{(\pm 1, 0), (0, \pm 1)\}$,

Dessin ici

alors $V_S(n) = 1 + 4 \sum_{j=1}^n (n + 1 - j) = 2n^2 + 2n + 1 \leq (2n + 1)^2$ (à vérifier).

4. Si $G = \mathbb{Z}^d$ avec $S = \{(\pm 1, 0, \dots, 0), \dots, (0, 0, \dots, \pm 1)\}$. Alors

$$|B_S(n)| \leq (2n+1)^d, \quad |B_S(n)| \geq \text{volume de la boule euclidienne de rayon } \frac{n}{\sqrt{d}} \cong C_d n^d.$$

5. Si $G = \mathbb{F}_k$, $S = \{a_1^{\pm 1}, \dots, a_k^{\pm 1}\}$. Soit $S(n) = \{g \in \mathbb{F}_k \mid |g|_S = n\}$. Alors $|S(n)| = 2k(2k - 1)^{n-1}$ (car on a $2k$ choix pour la première lettre du mot, et ensuite comme on ne considère que des mots réduits, on a $2k - 1$ choix pour le reste

des lettres du mot). Ainsi

$$V_S(n) = \sum_{i=0}^n |S(i)| = \dots = \frac{k(2k-1)^n - 1}{k-1}.$$

6. Le groupe de Heisenberg discret. Si A est un anneau commutatif à unité, le groupe de Heisenberg sur A est

$$Heis(A) = \left\{ \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} \mid x, y, z \in A \right\} \subseteq GL_3(A).$$


Considérons $Heis(\mathbb{Z}) = \langle a, b, c \rangle$.

$$a = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \quad c = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

On a que $[a, b] = c$, $[a, c] = [b, c] = 1$ (commutateurs). Ceci nous dit que c commute avec a et b .

Exercice : Pour tous $m, n \in \mathbb{Z}$, $a^m b^n = c^{mn} b^n a^m$ (*). Indication : démontrer que $a^m b = c^m b a^m$.



Remarque 8.10. (*) nous donne que tout $g \in G$ a une expression $g = a^m b^n c^p$ pour $m, n, p \in \mathbb{Z}$. 

Proposition 8.11 (CROISSANCE DU GROUPE DE HEISENBERG). *Pour le groupe de Heisenberg, il existe des polynômes P_1, P_2 de degré 4 tels que*

$$\forall n \in \mathbb{N}, P_1(n) \leq V_S(n) \leq P_2(n).$$

Preuve. 1. Montrons que si $g = a^m b^n c^p$, et $|g|_S \leq N$, alors $|m|, |n| \leq N$, $|p| \leq N^2$. En effet on a au plus $(2N+1)$ choix pour $|m|$ et $|n|$ et $2N^2+1$ choix pour $|p|$, donc

$$V_S(n) \leq (2N+1)^2(2N^2+1).$$

L'application $\alpha : Heis(\mathbb{Z}) \rightarrow \mathbb{Z}^2$, $a^m b^n c^p \mapsto (m, n)$ est un homomorphisme de groupes. On a $a^m b^n c^p a^{m'} b^{n'} c^{p'} = a^{m+m'} b^{n+n'} c^{p+p'}$. Ainsi $|\alpha(g)|_{\alpha(S)} \leq |g|_S \leq |g|_S$, c'est-à-dire $|m| + |n| \leq N$.

Montrons la seconde inégalité par récurrence sur N . Pour $N = 1$, c'est clairement bon. Soit $g' \in G$ avec $|g'|_S = N-1$, $g' = a^{m'} b^{n'} c^{p'}$. Alors on a un des trois cas :

- a) $g = g' \cdot a^{\pm 1}$;
- b) $g = g' \cdot b^{\pm 1}$;

c) $g = g' \cdot c^{\pm 1}$.

a) $g = g' a^{\pm 1} = a^{m'} b^{n'} c^{p'} a^{\pm 1} = a^{m'} b^{n'} a^{\pm 1} c^{p'} = a^{m'} c^{\pm n} a^{\pm 1} b^{n'} c^{p'} = \dots = a^{m' \pm 1} b^{n'} c^{p' \pm n'}$.
Comme $|p'| \leq (N-1)^2$, on a $|p' \pm n'| \leq (N-1)^2 + |n'| \leq (N-1)^2 + N \leq N^2$.

La deuxième inégalité est immédiate par récurrence.

b) $g' b^{\pm 1} = a^{m'} b^{n' \pm 1} c^{p'}$. Comme $|p'| \leq (N-1)^2$, on a $|p'| \leq N^2$.

c) $g' c^{\pm 1} = a^{m'} b^{n'} c^{p' \pm 1}$ et donc $|p' \pm 1| \leq |p'| + 1 \leq (N-1)^2 + 1 \leq N^2$.

2. Pour l'inégalité $P_1(n) \leq V_S(n)$, montrons que, si $m + n + 6\lfloor \sqrt{p} \rfloor \leq N$ avec $m, n, p \geq 0$, alors $|a^m b^n c^p|_S \leq N$. En effet, si $k^2 \leq p \leq (k+1)^2$, on a $a^m b^n c^p = a^m b^n c^{k^2} c^{p-k^2} = a^m b^n [a^k, b^k] c^{p-k^2}$, donc $|a^m b^n c^p| \leq m + n + 4k + p - k^2 < m + n + 4k + 2k + 1 \leq m + n + 6k \leq N$.

Exercice : $\iiint_{x+y+6\sqrt{z} \leq N, x, y, z \geq 0} 1 dx dy dz = kN^4$ avec k constante. □

Définition 8.12. Soient $f, g : \mathbb{R}^+ \rightarrow \mathbb{R}^+$. Alors $f < g$ s'il existe $a, b, c \in \mathbb{R}$, $c, a > 0$ avec $f(x) \leq cg(ax + b)$ pour $x \gg 0$. On dit que $f \approx g$ si $f < g$ et $g < f$.

Exercice 8.1. Si f, g sont des polynômes de même degré, alors $f \approx g$. ♣

Proposition 8.13 (ÉQUIVALENCE DE CROISSANCE). Soient (G_1, S) et (G_2, T) deux groupes quasi-isométriques (par exemples S, T deux parties génératrices finies du même groupe G). Alors $V_S \approx V_T$.

Preuve. Soit $f : G_1 \rightarrow G_2$ une quasi-isométrie, c'est-à-dire qu'il existe $\lambda > 0$, $c \geq 0$ telles que pour tous $x, y \in G_1$

$$\frac{1}{\lambda} |x^{-1}y|_S - c \leq |f(x)^{-1}f(y)|_T \leq \lambda |x^{-1}y|_S + c.$$

On peut supposer $f(1_{G_1}) = 1_{G_2}$ (remplacer f par $(f(1))^{-1}f$). Donc $\frac{1}{\lambda} |y|_S - c \leq |f(y)|_T \leq \lambda |y|_S + c$ pour tout $y \in G_1$. Soit $R \geq 0$ tel que pour tout $h \in G_2$, il existe $g \in G_1$ tel que $|f(g)^{-1}h|_T \leq R$ (quasi-surjectivité).

Pour chaque h dans G_2 , on choisit $g_h \in G_1$ tel que $|f(g_h)^{-1}h|_T \leq R$. Pour $h \in B_T(n)$, on a $|g_h|_S \leq \lambda(|f(g_h)|_T + c)$ ($\iff \frac{1}{\lambda}|g_h|_S - c \leq |f(g_h)|_T$) $\leq \lambda(R + n + c)$ par l'inégalité du triangle. Pour h fixé, le nombre de h' avec $g_h = g_{h'}$ est au plus $|B_T(h, 2R)| = V_T(2R)$.

Donc $V_T(n) \leq |\{g_h \mid h \in B_T(n)\}| V_T(2R) \leq V_S(\lambda R + \lambda n + \lambda c) V_T(2R)$, qui est exactement la définition de $V_T < V_S$.

Par symétrie on a $V_S < V_T$, d'où $V_S \approx V_T$. □

Définition 8.14. 1. La **suite dérivée** de G est définie par

$$G = G^{(0)} \supset G^{(1)} = [G, G] \supset \dots \supset G^{(k)} = [G^{(k-1)}, G^{(k-1)}] \supset \dots$$

2. La **suite descendante** de G est

$$G = G_0 \supset G_1 = [G_0, G_0] \supset [G, G_1] \supset \dots \supset G_k = [G, G_{k-1}] \supset \dots$$

On a donc que $G^{(k)} < G_k$.

Définition 8.15. 1. On dit que G est **résoluble** s'il existe $k \geq 1$ tel que $G^{(k)} = \{1\}$.

2. On dit que G est **nilpotent** s'il existe $k \geq 1$ tel que $G_k = \{1\}$.

On observe ainsi que si G est nilpotent, alors G est résoluble.

Exemples 8.16. 1. Tout groupe abélien est nilpotent (donc résoluble).

2. Pour tout anneau commutatif à unité A , le groupe de Heisenberg $Heis(A)$ est nilpotent, car

$$[Heis(A), Heis(A)] \subset \left\{ \begin{pmatrix} 1 & 0 & z \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \mid z \in A \right\} = Z(Heis(A))$$

le centre de $Heis(A)$ (pour rappel, $Z(G) = \{g \in G \mid [g, h] = 1 \ \forall h \in G\}$). De plus

$$Heis(A) \supset [Heis(A), Heis(A)] \supset [Heis(A), \underbrace{[Heis(A), Heis(A)]}_{\subset Z(Heis(A))}] = \{1\}$$

car le centre commute avec tous les éléments.



Proposition 8.17. Soit G un groupe nilpotent.

1. $G_{j+1} \triangleleft G_j$

2. G_j/G_{j+1} est abélien.

Preuve. Exercice.



En 1972, Hyman BASS démontre que tout groupe virtuellement nilpotent de présentation finie est à croissance polynomiale (avec un calcul explicite du degré de croissance).

Définition 8.18. Pour A abélien et finiment engendré, $A = \mathbb{Z} \oplus F$ où $|F| < \infty$ (voir la structure du groupe abélien), on définit le **rang** comme

$$\mathrm{rk}_{\mathbb{Z}} A = r.$$

Théorème 8.19 (DE BASS). Soit G un groupe nilpotent finiment engendré. Soit $n \in \mathbb{N}$ le minimum tel que $G_N = \{1\}$ (ce n s'appelle **degré de nilpotence**). La fonction de croissance de G est polynomiale de degré

$$\sum_{j=0}^{n-1} (j+1) \mathrm{rk}_{\mathbb{Z}} (G_j/G_{j+1}).$$

Corollaire 8.20. Soit G virtuellement nilpotent. Alors G a une croissance polynomiale.

Théorème 8.21 (DE GROMOV). Soit G un groupe finiment engendré à croissance polynomiale. Alors G est virtuellement nilpotent.

Le preuve de ce théorème a fondé la plupart des techniques actuelles de géométrie des groupes.

Corollaire 8.22. “Être virtuellement nilpotent” est une propriété géométrique. [pour rappel, une propriété géométrique est une propriété invariante par qi. Si A qi à B et si A a une propriété géométrique, alors B l’a aussi.]

Preuve. Soit G_1 quasi-isométrique à G_2 et soit G_1 virtuellement nilpotent. Par le corollaire ci-dessus, G_1 a une croissance polynomiale. Par la proposition d’équivalence des croissances, G_2 a une croissance polynomiale aussi. Ainsi par Gromov, G_2 est virtuellement nilpotent. \square

Corollaire 8.23. “Être virtuellement \mathbb{Z} (cyclique)” est une propriété géométrique.

Preuve. Soit G quasi-isométrique à \mathbb{Z} . Alors G a une croissance linéaire. En effet, dans \mathbb{Z} , les boules $V(n) = 2n + 1$, qui est linéaire. Comme une croissance linéaire est une croissance polynomiale, G est virtuellement nilpotent par Gromov.

Soit alors $H \leq G$ un sous-groupe d’indice fini tel que H est nilpotent. H a aussi une croissance linéaire car la croissance d’un sous-groupe ne peut pas être plus grande que celle du groupe. Par Bass, on a

$$1 = \sum_{j=0}^{n-1} (j+1) \mathrm{rk}_{\mathbb{Z}} (H_j/H_{j+1})$$

où n est le degré de nilpotence.

Comme $j+1$ et le rang sont tous deux positifs, la seule possibilité est que $\text{rk}_{\mathbb{Z}}(H_0/H_1) = 1$ et $\text{rk}_{\mathbb{Z}}(H_j/H_{j+1}) = 0$ pour tout $j \geq 1$, on a $H_0 = H$. Ainsi

$$H_0/H_1 = H/[H, H] \cong \mathbb{Z} \oplus F, \quad |F| < \infty.$$

$H_1/H_2 = [H, H]/[H, [H, H]]$ est fini, on regarde tous les quotients et on arrive à un moment à $H_n = \{1\}$, ainsi $H_{n-1}/H_n = H_{n-1}/\{1\}$ est fini, donc H_{n-1} est fini. Ceci montre que H_i est fini pour chaque i , donc c'est vrai en particulier pour H_1 . Donc $H_0/H_1 = H/\text{fini} \cong \mathbb{Z} \oplus F$ qui montre que H est virtuellement \mathbb{Z} , et donc G est aussi virtuellement \mathbb{Z} par Milnor-Švarc. \square

En 1983, R. GRIGORCHUCK a constuit le premier exemple d'un groupe (G, S) à **croissance intermédiaire**, et a montré que

$$e^{\sqrt{n}} < V_S(n) < e^{n^{0.991}}.$$

On a vu (Gromov et Bass) que la croissance polynomiale est équivalente pour un groupe à être virtuellement nilpotent. La croissance polynomiale est plus petite que la croissance intermédiaire (Grigorchuck), elle-même plus petite que la croissance exponentielle (presque tous les groupes ont une croissance exponentielle).

Définition 8.24. Soit G un groupe finiment avec une partie génératrice finie S . La **série de croissance** de G par rapport à S est

$$f_{(G,S)}(z) = \sum_{n \geq 0} a_n z^n$$

où $a_n = |\{g \in G \mid |g|_S = n\}|$ (mots de longueur n). On peut aussi parler de $b_n = V_S(n) = |\{g \in G \mid |g|_S \leq n\}|$ à la place de a_n .

Question : existe-t-il des groupes avec une croissance rationnelle, i.e. est-ce que $f(z)$ peut s'exprimer comme quotient de polynômes $P(z), Q(z) \in \mathbb{Z}[z]$?

Théorème 8.25. Soit G un groupe, $G = \langle S \rangle$ avec $|S| < \infty$. Si G a un langage de formes normales qui est régulier, alors la série $f_{(G,S)}(z)$ est rationnelle.

Définition 8.26. On appelle **formes normales** le fait de prendre un mot sur S pour chaque élément dans G .

- Exemples 8.27.**
1. Considérons \mathbb{Z}^2 avec le système de générateurs $\{a^{\pm 1}, b^{\pm 1}\}$. Un langage de formes normales est $\{a^n b^m, n, m \in \mathbb{Z}\}$.
 2. Considérons le groupe libre $(\mathbb{F}_2, \{a^{\pm 1}, b^{\pm 1}\})$. Un langage de formes normales est donné par tous les mots réduits (c'est le langage naturel sur le groupe



libre).



Chapitre 9.

Croissance et langages (formels)

Définition 9.1. Soit A un ensemble fini, et A^* l'ensemble de tous les mots formés à partir de A . A s'appelle un **alphabet**, et L est un **langage** sur A si L est un sous-ensemble de A^* .

Exemple 9.2. Soit $A = \{0, 1\}$. Alors $L_1 = \{0, 1, 01, 11\}$ et $L_2 = \{0^n 1^m \mid n, m \geq 1\}$ sont des langages sur A . ★

Définition 9.3. Un **automate fini déterministe (AFD)** est un quintuple (Q, A, δ, q_0, F) constitué des éléments suivants.

- A est un alphabet fini.
- Un ensemble fini d'états Q .
- Une fonction de transition $\delta : Q \times A \rightarrow Q$.
- Un état initial q_0 .
- Un ensemble d'états finaux (ou acceptants) $F \subset Q$.

Exemple 9.4. On peut représenter un AFD par un graphe fini.

// METTRE DESSIN ICI

Par convention, une flèche de rien vers un cercle représente l'état initial, un sommet avec deux cercles, un sommet avec un seul cercle représente un état, représentent un état final, $A = \{a, b\}$ et une flèche d'un sommet vers un autre avec une étiquette représente une transition et l'ensemble est $\delta : Q \times A \rightarrow Q$.

Un mot ω est reconnu par un automate s'il existe un chemin étiqueté par ω , partant de l'état initial et aboutissant dans un état final.

L'automate représenté à la figure ci-dessus accepte les mots commençant par a , avec au moins un b au milieu et terminant par a , et le mot a . Le langage reconnu par l'automate est l'ensemble des mots acceptés par l'automate. ★

Définition 9.5. Un langage est **régulier** s'il est accepté par un automate.

Proposition 9.6. La série de croissance f_L d'un langage L régulier est une fonction rationnelle :

$$f_L(z) = \sum_{n \geq 0} a_n z^n$$

où $a_n = |\{\omega \in L \mid |\omega| = n\}|$.

Preuve (INFORMELLE, PREUVE PAR EXEMPLE). Considérons l'automate \mathcal{A} sur $\{a, b\}$ suivant

// DESSIN DE L'AUTOMATE ICI

Les mots acceptés par \mathcal{A} sont des mots ne contenant pas deux a consécutifs. La **matrice de voisinage** de \mathcal{A} est

$$M = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 2 \end{pmatrix}$$

(on a une transition de 1 vers 2, donc $a_{12} = 1$, on a deux transitions de 3 vers 3, donc $a_{33} = 2$ etc.)

Pour tous $q, r \in \{1, 2, 3\}$ et tous $n \in \mathbb{N}$, $[M^n]_{q,r}$ est le nombre de chemins de longueur n joignant q à r .

$$M^3 = \begin{pmatrix} 3 & 2 & 3 \\ 2 & 1 & 5 \\ 0 & 0 & 8 \end{pmatrix}$$

par exemple veut dire qu'il y a deux chemins de longueur 3 joignant 2 à 1 (bbb ou bab).

Alors $a_n = \sum_{f \in \{1,2\}} [M^n]_{1,f}$ pour n fixé. Ainsi la série est

$$\begin{aligned} \sum_{n \geq 0} a_n z^n &= \sum_{n \geq 0} \sum_{f \in \{1,2\}} [M^n]_{1,f} z^n = \sum_{n \geq 0} [M^n]_{1,1} z^n + \sum_{n \geq 0} [M^n]_{1,2} z^n \\ &= [I + Mz + M^2 z^2 + \dots]_{1,1} + [I + Mz + M^2 z^2 + \dots]_{1,2} = [(I - Mz)^{-1}]_{1,1} + [(I - Mz)^{-1}]_{1,2} \\ &= \frac{1}{\det(I - Mz)} \left([(I - Mz)^{Adj}]_{1,1} + [(I - Mz)^{Adj}]_{1,2} \right), \end{aligned}$$

où le déterminant est un polynôme, et les coefficients sont des polynômes. Ainsi la fonction f_L est rationnelle. \square

Exemple 9.7. L'automate pour les formes normales de \mathbb{F}_2 sur $\{a, A = a^{-1}, b, B = b^{-1}\}$ est représenté ci-dessous.

// DESSIN ICI

Comme on représente le langage par un automate fini déterministe, le langage

est régulier. Ainsi la série de croissance de \mathbb{F}_2 par rapport à $\{a, A, b, B\}$ est rationnelle.

On a calculé que $a_n = 4 \cdot 3^{n-1}$, et

$$f_{(G,S)}(z) = 1 + \sum_{n \geq 1} 4 \cdot 3^{n-1} z^n = 1 + \frac{4}{3} \sum_{n \geq 1} (3z)^n = 1 + \frac{4}{3} \frac{1}{1-3z}.$$



Index

- Action
 - propre, 39
- Algorithme
 - de Todd-Coxeter
 - Pour les graphes, 35
- Alphabet, 49
- Arbre, 36
 - maximal, 24
- Automate
 - fini déterministe, 49
- Automorphisme
 - de graphe, 37
- Bonus, 32
- Bouquet
 - à n cercles, 23
 - à deux cercles, 23
- Connexe
 - par arcs, 19
 - simplement, 20
- distance entre deux mots, 38
- Espace
 - géodésique, 40
- Espaces
 - quasi-isométriques, 39
- Fonction
 - de croissance, 44
- Forme normale, 48
- Graphe
 - de Cayley, 35, 36
 - de Schreier, 35
 - quasi-isométrique, 38
- Groupe
 - de Heisenberg discret, 45
 - Fondamental, 18
 - nilpotent, 47
 - résoluble, 47
 - virtuellement (P), 43
- Groupes
 - commensurables, 43
- Langage, 49
 - régulier, 50
- Lemme
 - du Ping-Pong
 - 2^{de} version, 22
- Longueur d'un mot g , 38
- Morphisme
 - de graphe, 37
- Produit libre, 22
- Proposition
 - de TIETZE, 30
- Quasi-inverses, 39
- Quasi-isométrie, 38
- Réalisation géométrique, 41
- Relèvement
 - d'homotopies, 26
 - de chemins, 26
- Revêtement, 24
 - à n feuillets, 25
- Série
 - de croissance, 48
- Suite
 - dérivée, 46
 - descendante, 46

Tableau de définitions, 32
Théorème
 de TIETZE, 31
 de Milnor-Švarc, 41
 de Nielsen-Schreier, 27
 de Van Kampen, 23
Transformation de Tietze, 29

Voisinage
 trivialisant, 24