Groupes, algorithmique et combinatoire: cours 2015

Laurent Hayez

Date de création: 30 septembre 2015
Dernière modification: 4 novembre 2015

Table des matières

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 un 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. $\mathbb{Z} = \langle a = 1 | - \rangle$.
2. $S_3 = \langle t_1, t_2 | t_1^2 = e = t_2^2, (t_1 t_2)^3 = e \rangle$.
3. $D_4 = \langle x, y | x^2 = y^4 = (xy)^2 = e \rangle$.
4. $\mathbb{Z}/7\mathbb{Z} = \langle x | x^7 = e \rangle$.

★

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

0.2. Problèmes de Dehn

0.2.1. Problème de l'égalite (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 $G = \langle x, y, z|x^2yx^{-1}z = x^3y^3\rangle$. Est-ce que $xyx^{-1}z =_G zx^2y^{-1}z$? Ou par exemple dans S_3, est-ce que $t_1t_2t_1^3t_2 =_{S_3} t_2t_1$? En fait, oui car

$$\begin{aligned} t_1t_2t_1^3t_2 &= t_1t_2t_1t_1^2t_2 & t_1^2 &= e \\ &= t_1t_2t_1t_2 & (t_1t_2)^3 &= e \\ &= t_2^{-1}t_1{-1} & t_1 = t_1^{-1},\ t_2 &= t_2^{-1} \\ &= t_2t_1. \end{aligned}$$

0.2.2. Problème des mots (PM)

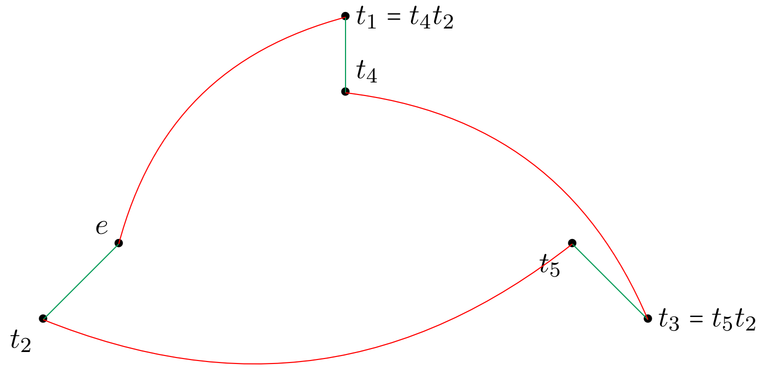
Existe-t-il un algorithme permettant de décider pour tout mot w sur X si $w =_G e$?

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 $\{(g, gx) : g \in G,\ x \in X\}$.

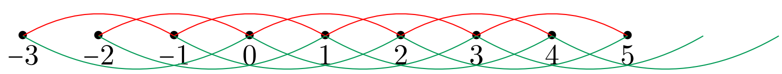
Exemples 0.4. 1. Considérons par exemple

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

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,....).

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 $A = \{a_1, \ldots, a_n\}$, 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 $aa a \cdots a^{-1}$, 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 $x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n}$ est la classe d'équivalence de $x_n^{-\varepsilon_n} \cdots x_1^{-\varepsilon_1}$ avec $\varepsilon_i \in \mathbb{Z}$ pour tout i. L'opération est la concaténation (la réduction est implicite).

On fait souvent l'abus de language 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 $a_1^{\varepsilon_1} \cdots a_n^{\varepsilon_n}$ est $a_n^{-\varepsilon_n} \cdots a_1^{-\varepsilon_1}$.
   - 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 $\langle a_1, a_2, \ldots, a_n | - \rangle$.

1.1. Propriété universelle du groupe libre (PU)

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

$$\begin{tikzcd}
A \arrow[rr, hook, "i"] \arrow[dr, "f"'] & & \mathbb{F}(A) \arrow[dl, "!\varphi"] \\
& G &
\end{tikzcd}$$

Ceci signifie que toute application $f : A \to G$ s'étend en un unique homomorphisme $\varphi : \mathbb{F}(A) \to G$ où pour $w = a_{i_1}^{\varepsilon_1} \cdots a_{i_n}^{\varepsilon_n}$ on pose $\varphi(w) = f(a_{i_1})^{\varepsilon_1} \cdots f(a_{i_n})^{\varepsilon_n}$ 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 $\varphi : \mathbb{F}(A) \to G$ implique que $\mathbb{F}(A)/\ker\varphi \cong \mathrm{Im}\varphi = G$. □

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 $G = \langle x, y | x^2y^3 = x^3y^4 = 1\rangle$. On a que $x^3y^4 = 1 = x(x^2y^3)y = xy$, donc $x = y^{-1}$ et $y = x^{-1}$. Ainsi $x^2y^3 = x^2(x^{-1})^3 = x^{-1} = 1$, 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 $w = ava^{-1}$ 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.** $w = a^{-1}bca^2b^{-1}a \xrightarrow{c.} bca^2b^{-1} \xrightarrow{c.} ca^2$. ★

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

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 $w_1 = cabc^{-1}$ et $w_2 = abbab^{-1}a^{-1}$. On effectue la réduction cyclique :
> $$w_1 \xrightarrow{c} ab, \quad w_2 \xrightarrow{c} bbab^{-1} \xrightarrow{c} ba.$$
> 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 pours les groupes libres

Pour deux présentations $\langle X_1 | R_1 \rangle$ et $\langle X_2 | R_2 \rangle$, il n'y 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 $f : X \to Y$).*

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

$$\begin{tikzcd} X \arrow[rr, "\tilde{f}"] \arrow[dr, "i_X"'] & & \mathbb{F}(Y) \\ & \mathbb{F}(X) \arrow[ur, "\varphi"'] & \end{tikzcd} \qquad \begin{tikzcd} X \arrow[rr, "\tilde{g}"] \arrow[dr, "i_Y"'] & & \mathbb{F}(X) \\ & \mathbb{F}(Y) \arrow[ur, "\psi"'] & \end{tikzcd} \qquad \begin{tikzcd} X \arrow[rr, hook, "i_X"] \arrow[dr, "i_X"'] & & \mathbb{F}(X) \\ & \mathbb{F}(X) \arrow[ur, "!\alpha = id_{\mathbb{F}(X)}"'] & \end{tikzcd}$$

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

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

"⇐" : 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 $V(X) = \mathbb{F}(X)/N(X) = \underbrace{\mathbb{Z}/2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/2\mathbb{Z}}_{|X|}$ 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 $g = a_{i_1}^{\varepsilon_1} \cdots a_{i_n}^{\varepsilon_n}$, 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

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

Ainsi, on a

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

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

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

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

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

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

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 $l = \left(\begin{smallmatrix} 1 & 0 \\ 2 & 1 \end{smallmatrix}\right)$ et $r = \left(\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right)$ 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 $X, Y \neq \varnothing$, tq $X \cap Y = \varnothing$ 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. $m = \alpha^{h_1}\beta^{k_1} \cdots \beta^{k_{n-1}}\alpha^{h_n}$ avec $h_i, k_i \in \mathbb{Z} \setminus \{0\}$. Alors supposons que $m =_G 1$. Ainsi

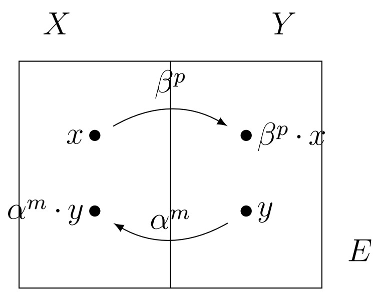


FIGURE 4.1. – Illustration du Lemme du Ping-Pong

$m \cdot Y = Y$.

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

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

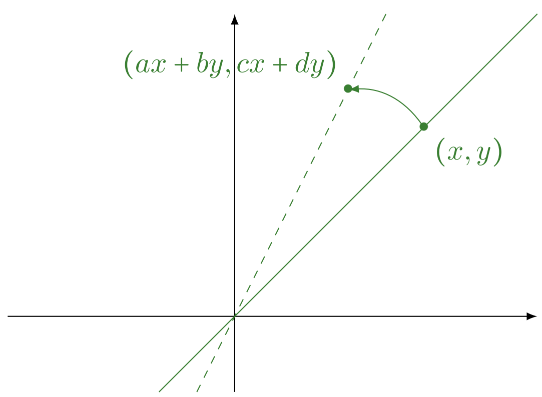
2. $m = \beta^{k_1} \cdots \beta^{k_n}$, donc $\alpha^{-h_1} m \alpha^{h_1}$ est comme au point 1 et ainsi $\alpha^{-h_1} m \alpha^{h_1} \neq_G 1$ ainsi $m \neq_G 1$.
3. Si $m = \alpha^{h_1} \cdots \beta^{k_n}$, pour $h_0 \neq h_1$ on regarde $\alpha^{-h_0}(\alpha^{h_1} \cdots \beta^{k_n})\alpha^{h_0}$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

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

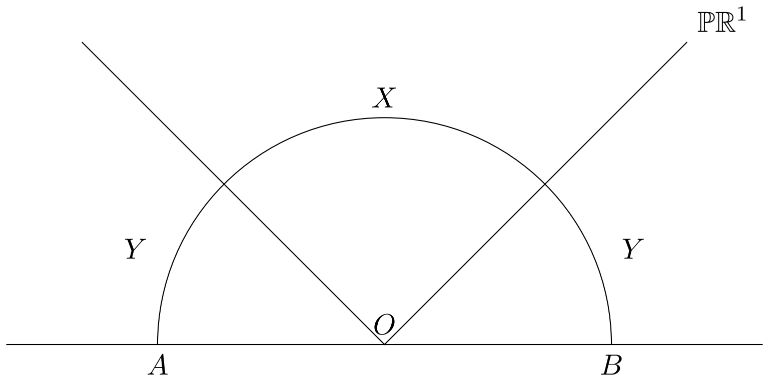
Preuve (DE 4.6)**.** Exercice.

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, $\mathbb{PR}^1$ (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 $\mathrm{Homeo}(\mathbb{R}) = \{\varphi : \mathbb{R} \to \mathbb{R} \mid \varphi \text{est continue et bijective}\}$. $\mathrm{Homeo}(\mathbb{R})$ contient beaucoup de groupes libres.

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

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 $f : X \to Y$ correspond un homomorphisme de groupes $f_* : F(X) \to F(Y)$.

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 $\gamma : [0,1] \to X$, $t \mapsto \gamma(t)$, 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.

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

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

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

telle que

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

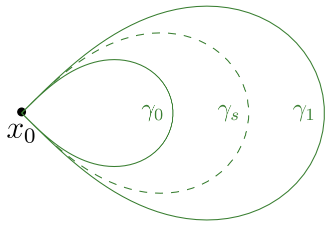


FIGURE 5.1. – Exemple d'homotopie

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 $\Pi_1(X,x_o)$ l'ensemble des classes d'homotopie des lacets de X basés en x_o. 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

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

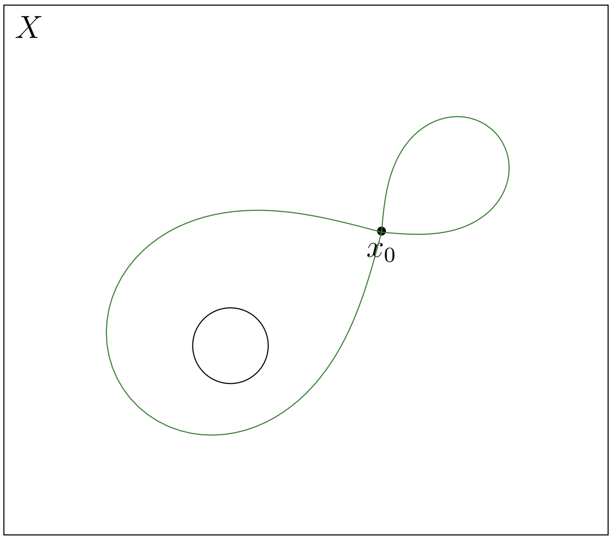


FIGURE 5.2. – Exemple d'homotopies ayant des classes d'équivalence différentes (le rond est un "trou")

(à vérifier).

Il faut encore montrer que :

- $\varepsilon_{x_o}\gamma \sim \gamma \sim \gamma\varepsilon_{x_0}$;
- $\gamma\check{\gamma} \sim \varepsilon_{x_0}$;
- associativité : si γ_0, γ_1, γ_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

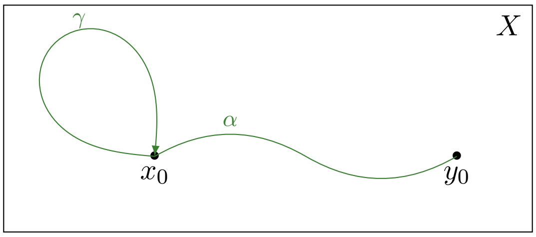
Rappel : Un espace est **connexe par arcs** si deux points peuvent être joints par un arc.

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

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

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 :

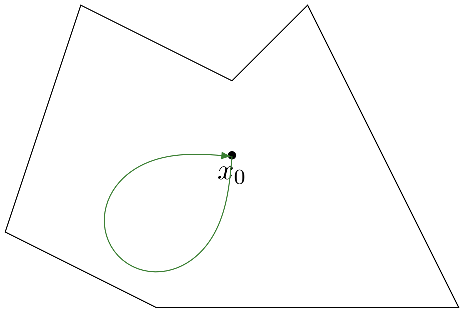


Ainsi pour passer de $\gamma \in \Pi_1(X, x_0)$ à un élément de $\Pi_1(X, y_0)$, on prend $\breve{\alpha}\gamma\alpha$. □

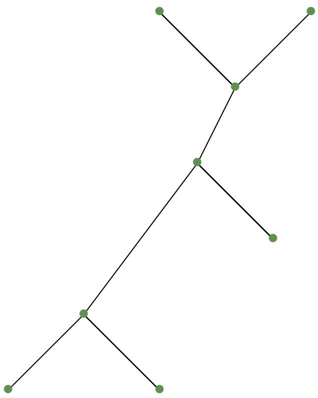
Définition 5.8. Un espace X (connexe par arcs) est **simplement connexe** si $\Pi_1(X) = 0$ (ou $\{1\}$). C'est-à-dire que tout lacet dans X est homotope à ε_{x_0}.

Exemples 5.9.

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



2. Les arbres sont simplements 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 $f : X \to Y$ une application continue, avec $y_0 = f(x_0)$. On pose $f_* : \Pi_1(X, x_0) \to \Pi_1(Y, y_0), [\gamma] \mapsto [f \circ \gamma]$. Alors f_* est un homomorphisme de groupes.*

De plus,

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

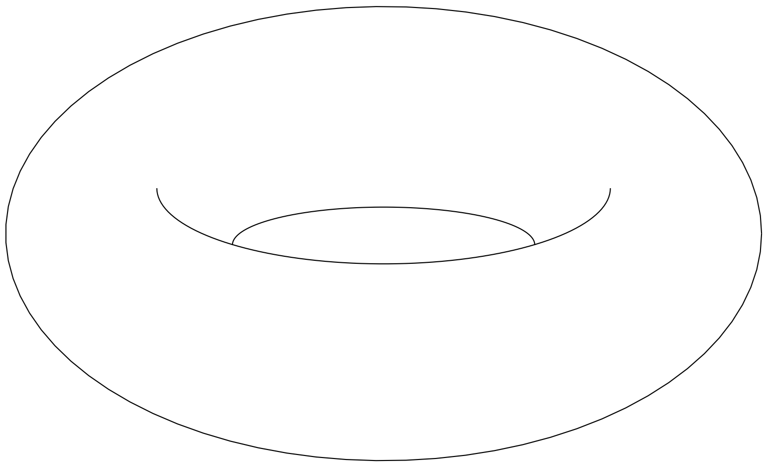
Preuve. Exercice. □

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

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

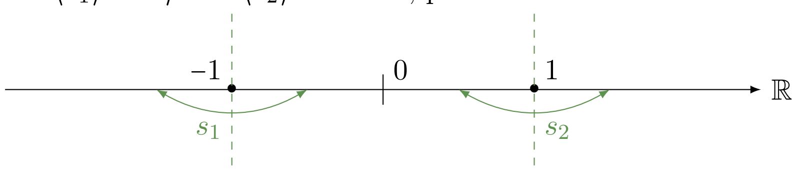
et $a_2, \ldots, a_k \neq \varepsilon_A$ et $b_1, \ldots, b_{k-1} \neq \varepsilon_B$.

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 dihédral 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 $Sym(X)$. On suppose que $|G_1| \geq 2$, $|G_2| \geq 3$. S'il existe deux parties $A_1, A_2 \subset X$ telles que $A_i \neq \varnothing$, $A_1 \not\subset A_2$ 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 $Sym(X)$ est isomorphe à $G_1 * G_2$.

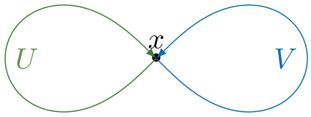
5.3. Théorème de Van Kampen (version simple)

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 $U \cap V = \{x\}$.



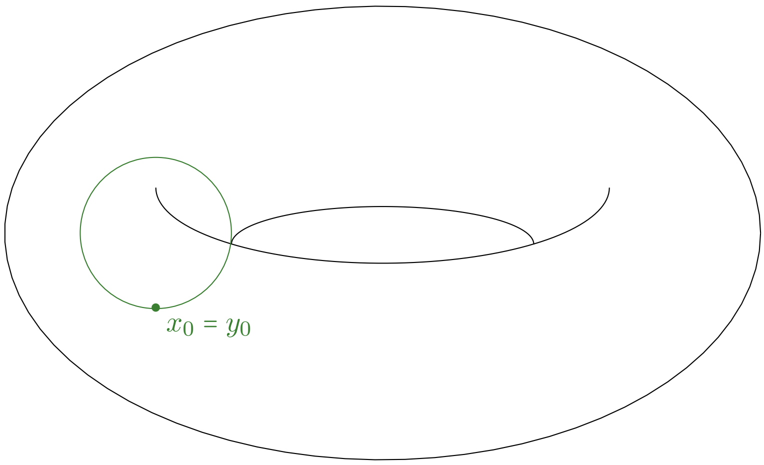
Le groupe fondamental est

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

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



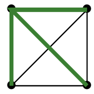
3. On appelle B_n le bouquet de n cercles. Alors

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

Plus généralement, si $X = (V, E)$ et 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

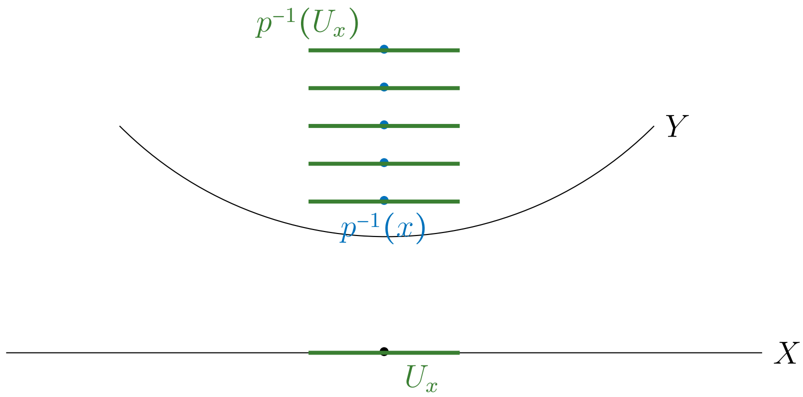
Tous les espaces sont supposés connexes par arcs et localement connexes par arcs.

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 $Y \to X$.
- 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 $h_x : p^{-1}(U_x) \to p^{-1} \times U_x$ tel que le diagramme suivant commute (où p_2 est la projection sur le 2ème facteur).

$$\begin{tikzcd}
p^{-1}(U_x) \arrow[rr, "h_x"] \arrow[dr, "p|_{p^{-1}(U_x)}"'] & & p^{-1}(x) \times U_x \arrow[dl, "p_2"] \\
& U_x &
\end{tikzcd}$$

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



On dira que $\underset{X}{\overset{Y}{\downarrow}}p$ 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.

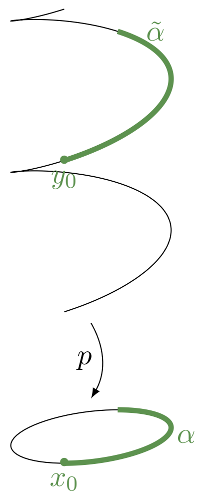
1. Soit $X = \{z \in \mathbb{C} \mid |z| = 1\}$. Alors l'espace Y peut être représenté par une hélice, mais $Y = \mathbb{R}$. Alors $p : \mathbb{R} \to \S^1$ est défini par $p(t) = e^{2\pi i t}$ et $\underset{X}{\overset{Y}{\downarrow}}p$ est un revêtement car p est surjective. Si $z = e^{2\pi i \varphi}$, alors $p^{-1}(z) = \varphi + \mathbb{Z}$ est discret dans $\mathbb{R}$. Enfin, si $z = e^{2\pi i \varphi} \in S^1$, $U_z = S^1 \smallsetminus \{-z\}$ (tout le cercle sauf le point opposé à z) est un voisinage de z, et $p^{-1}(U_z) = \mathbb{R} \smallsetminus \{\varphi + (2k+1)\pi, k \in \mathbb{Z}\} \cong \mathbb{Z} \times U_z$ 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 $p : S^1 \to S^1$, $z \mapsto z^n$ 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 $\underset{X}{\overset{Y}{\downarrow}}p$ un revêtement. Soit Z un espace connexe et soient $f_0, f_1 : Z \to Y$ deux applications continues avec $p \circ f_0 = p \circ f_1$. Alors $\{z \in Z | f_o(z) = f_1(z)\} = \varnothing$ ou Z.*

$$\begin{tikzcd} Z \arrow[d, bend right, "f_0"'] \arrow[d, bend left, "f_1"] \\ Y \arrow[d, "p"'] \\ X \end{tikzcd}$$

Preuve. Exercice.



$$\begin{tikzcd} Z = [0,1] \arrow[d, shift right, "\tilde{\alpha}_0"'] \arrow[d, shift left, "\tilde{\alpha}_1"] \\ Y \arrow[d, "p"'] \\ X \end{tikzcd}$$

□

Lemme 5.21 (relèvement des chemins). *Soient $x_0 \in X$, $y_0 \in p^{-1}(x)$. Pour tout chemin $\alpha : [0,1] \to X$ avec $\alpha(0) = x_0$, il existe un unique chemin $\tilde{\alpha} : [0,1] \to Y$ 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, $\tilde{\alpha}_0, \tilde{\alpha}_1 : Z = [0,1] \to Y$ 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 $\alpha_0, \alpha_1 : [0,1] \to X$ 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*

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

est injective (si $f : X \to Y$, on définit $f_* : \Pi_1(X, x_0) \to \Pi_1(Y, y_0)$ par $[\gamma] \to [f \circ \gamma]$). 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. □

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 $\begin{smallmatrix} X_H \\ \downarrow \\ X \end{smallmatrix} p$ 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 $\Pi_1(X)$. ♣

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 $\begin{smallmatrix} Y \\ \downarrow \\ X \end{smallmatrix} p$ est égal à*

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

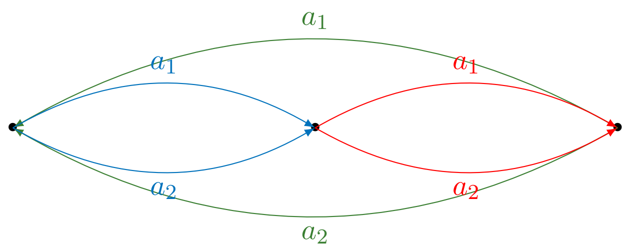
Preuve. Exercice 1, série 6. □

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

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

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 $\varphi : \mathbb{F}(X) \to G$ 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 $\varphi^1 : \mathbb{F}(x,y) \to G$ tel que $\varphi^1(x) = \varphi(x)$ et $\varphi^1(y^{-1}w(X)) = 1$ pour $x \in X$.

$$\begin{tikzcd}
X \cup \{y^{-1}\omega(X)\} \arrow[r] \arrow[d, "f"] & \mathbb{F}(X,y) = \mathbb{F}(X \cup \{y^{-1}\omega(X)\}) \arrow[d, "\chi"] \arrow[dl, "\varphi^1!"'] \\
G & \mathbb{F}(X) \arrow[l, "\varphi"]
\end{tikzcd}$$

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

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

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 $\langle X_2|s_1, \ldots, s_n\rangle$ est une présentation finie pour G.*

Chapitre 7.

Index