Groupe De Lecture

Antoines Petitjean et Derimay

1 Produits libres, groupes libres

Définition 1.
Soit A un ensemble, on note $W(A)$ l'ensemble des mots sur A, défini par

$$\{a_1a_2\dots a_n, n \in \mathbb{N}, a_i \in A\}$$

Pour un mot $a_1a_2\dots a_n$, on appelle n la longueur du mot. Quand $n = 0$, il s'agit du mot vide ε.
Remarquons par ailleurs que A est naturellement inclus dans $W(A)$: c'est l'ensemble des mots de longueur 1.

On peut alors définir une loi de composition interne $\cdot$ sur $W(A)$ comme étant la juxtaposition de deux mots : si $w = a_1a_2\dots a_n$ et $w' = b_1b_2\dots b_m$, on a $w \cdot w' = a_1a_2\dots a_nb_1b_2\dots b_m$. Il est aisé de vérifier que cette loi admet pour neutre le mot vide et que cette loi est associative, autrement dit $W(A)$ est un monoïde pour $\cdot$, mais ce n'est bien sûr pas un groupe, puisque la longueur de la juxtaposition de deux mots est la somme des deux longueurs, et celle-ci sera en particulier toujours strictement positive pour peu que l'un des deux mots considérés n'est pas le mot vide.
Pour cela, il faudrait pouvoir "simplifier" des lettres du mot, il nous faut donc une structure supplémentaire sur A.

Définition 2.
Soit $(G_i)_{i\in I}$ une famille de groupes. On note $A = \bigsqcup_{i\in I} G_i$. On peut alors définir la relation d'équivalence $\sim$ sur $W(A)$ engendrée par :

1. $\forall (w, w') \in W(A)^2, we_iw' \sim ww'$ (avec e_i le neutre de G_i)
2. $\forall (w, w') \in W(A)^2, \forall (a, b, c) \in G_i$ avec $c = ab$, $wabw' \sim wcw'$

Définition 3.
Le quotient $W(A)/\sim$ est un groupe. On l'appelle *produit libre des groupes* $(G_i)_{i\in I}$ et on le note $*_{i\in I}G_i$.

Démonstration. Montrons tout d'abord que la loi $\cdot$ sur $W(A)$ passe au quotient :
Pour $w, w', x, x' \in W(A)$ et $a, b \in G_{i_0}, c, d \in G_{i_1}$, on a $wabw' \cdot xcdx' \sim ww' \cdot xx'$ et $we_{i_0}w' \cdot xe_{i_1}x' \sim ww'xx'$, et comme $\sim$ est engendrée par ces deux relations, on a toujours $ww' \sim xx'$ dès que $w \sim x, w' \sim x'$.
Ainsi, $W(A)/\sim$ est un monoïde avec $\overline{w} \cdot \overline{w'} = \overline{w \cdot w'}$. Par ailleurs, pour $w = a_1a_2\dots a_n$, on a $w \cdot a_n^{-1}\dots a_2^{-1}a_1^{-1} \sim a_1a_2\dots a_{n-1}e_{i_n}a_{n-1}^{-1}\dots a_2^{-1}a_1^{-1} \sim \dots \sim \varepsilon$, donc la classe de $a_n^{-1}\dots a_2^{-1}a_1^{-1}$ est l'inverse de la classe de w, et on a bien montré que tout élément de $W(A)/\sim$ était effectivement inversible : $W(A)/\sim$ est bien un groupe. □

Définition 4.
Si $A = \bigsqcup_{i\in I} G_i$, on dira qu'un mot $w = a_1a_2\dots a_n \in W(A)$ est *réduit* si a_j et a_{j+1} ne sont pas dans le même groupe pour tout j et qu'aucun des a_j n'est le neutre d'un des groupes.

C'est un peu ce qu'on faisait avec $\sim$: si deux éléments consécutifs sont dans le même groupe on les transforme en un seul, et on fait juste disparaître les éléments neutres. La propriété suivante est donc assez naturelle :

Proposition 5.
Il y a exactement un mot réduit dans chaque classe d'équivalence par $\sim$ définie ci-dessus. Cela permet de considérer un ensemble agréable de représentants pour chaque classe d'équivalence pour $\sim$. Par la suite, on identifiera même une classe d'équivalence avec son mot réduit.

Corollaire 6.
Soient $(G_i)_{i\in I}$ une famille de groupes et $G = *_{i\in I} G_i$. Alors pour tout $i_0 \in I$ le morphisme canonique $G_{i_0} \to G$ est injectif.

Démonstration. L'image dans G de $g \in G_{i_0} \setminus \{e_{i_0}\}$ est un mot d'une lettre, donc un mot réduit qui n'est pas équivalent au mot vide. Ainsi, le noyau du morphisme est e_{i_0}. □

Définition 7.
Soit X un ensemble. On définit le *groupe libre sur* X comme le produit libre $F(X) = *_{x\in X}\mathbb{Z}$.

$F(X)$ représente l'ensemble des mots réduits que l'on peut former avec des éléments de X associés à un entier : $x_1^{n_1} x_2^{n_2} x_3^{n_3} \cdots$
On peut identifier chaque élément de X à x^{+1} dans $F(X)$ et considérer X comme une sous-partie de $F(X)$.
Le cardinal de X est appelé *rang* de $F(X)$.

Exemple 8.

1. Si $X = \varnothing$, $F(X)$ est le groupe trivial (groupe libre de rang 0)
2. Si $\mathrm{Card}(X) = 1$, alors $F(X) = \mathbb{Z}$ (groupe libre de rang 1)
3. Si $\mathrm{Card}(X) = 2$, alors $F(X)$ est l'ensemble des mots réduits avec 4 lettres a, b, a^{-1}, b^{-1} (groupe libre de rang 2)

Proposition 9.
Le produit libre vérifie également une propriété universelle, qui en fait le coproduit dans la catégorie des groupes :
Si G est un groupe, et que $(G_i)_{i\in I}$ est une famille de groupes, si on se donne également une famille h_i de morphismes de groupes avec $h_i : G_i \to G$, alors si on note f_i l'injection canonique de G_i dans $*_{i\in I} G_i$, il existe un unique morphisme h de $*_{i\in I} G_i$ dans G tel que $h \circ f_i = h_i$ pour tout i.
Le produit libre est dans ce sens l'équivalent en théorie des groupes de la somme directe en algèbre linéaire.

En particulier, dans le cas où $I = X$ et $G_i = \mathbb{Z}\ \forall i$, la donnée d'un morphisme $h_i : \mathbb{Z} \to G$ est la simple donnée d'un élément de G, donc la donnée d'une famille de morphismes $(h_x : \mathbb{Z} \to G)_{x\in X}$ n'est en fait rien d'autre qu'une fonction de X dans G, qui s'étend donc de manière unique en un morphisme de $F(X)$ dans G.

Corollaire 10.
Tout groupe est le quotient d'un groupe libre.

Démonstration. Soit G un groupe. $F(G)$ est l'ensemble des mots que l'on peut former avec les éléments de G sans tenir compte de la structure de groupe de G.

On considère le morphisme $h : F(G) \to G$ qui à un mot réduit $g_1^{n_1} g_2^{n_2} g_3^{n_3} \cdots$ dans $F(G)$ associe $g_1^{n_1} \cdot g_2^{n_2} \cdot g_3^{n_3} \cdots$ le produit des caractères du mot dans G. Alors h est un morphisme surjectif car $\forall g \in G, h(g^{+1}) = g$.
Donc, d'après le premier théorème d'isomorphisme, $F(G)/ker(h) \simeq im(h) = G$. $\square$

Il existe des théorèmes très intéressants sur les groupes libres, par exemple :

Théorème 1. *(Nielsen-Schreier)*
Tout sous-groupe d'un groupe libre est un groupe libre.

La démonstration de ce théorème est très complexe, et elle n'a pas été présentée dans le livre. Cependant nous pouvons prendre l'exemple de $\mathbb{Z}$:

Exemple 11.
Les sous groupes de $\mathbb{Z}$ sont les $n\mathbb{Z}$, qui sont isomorphes à $\mathbb{Z}$ par $\varphi : x \mapsto nx$. Ils sont donc également libres.

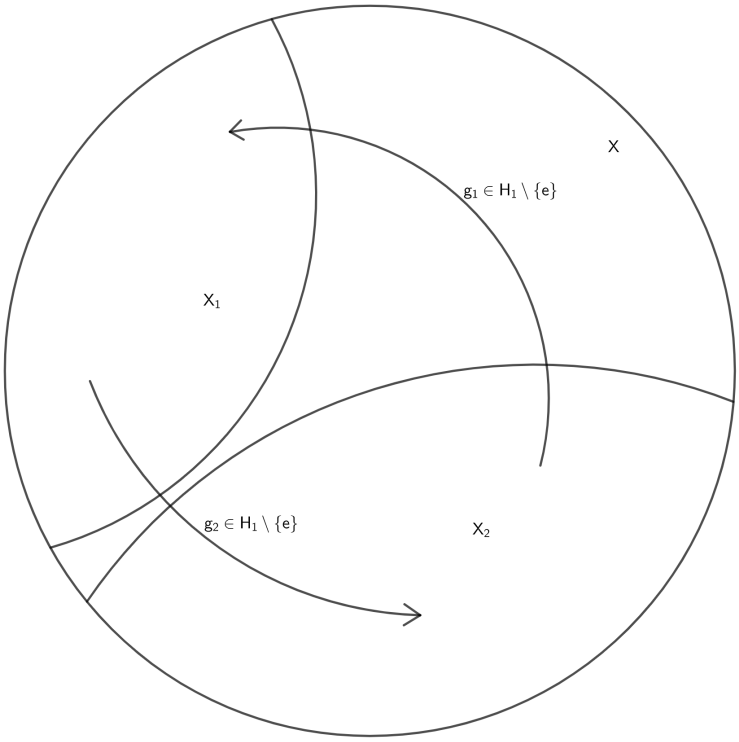
2 Lemme du ping-pong

Théorème 2. *(Lemme du ping-pong)*
Soit G un groupe agissant sur un ensemble X. Soient H_1 et H_2 deux sous-groupes de G. Soit H le sous-groupe de G engendré par H_1 et H_2. Supposons que $Card(H_1) \geqslant 3$ et $Card(H_2) \geqslant 2$. Supposons également qu'il existe deux sous-parties non vides X_1 et X_2 de X telles que :

1. X_2 n'est pas inclus dans X_1
2. $\forall g \in H_1 \setminus \{1\},\ g(X_2) \subset X_1$
3. $\forall g \in H_2 \setminus \{1\},\ g(X_1) \subset X_2$

Alors H est isomorphe au produit libre $H_1 * H_2$.

Démonstration. On considère le morphisme $h : H_1 * H_2 \to H$ qui à un mot réduit $h_1^{n_1} h_2^{n_2} h_3^{n_3} \cdots$ dans $H_1 * H_2$ associe $h_1^{n_1} \cdot h_2^{n_2} \cdot h_3^{n_3} \cdots$ le produit des caractères du mot, qui est dans H car H est engendré par H_1 et H_2. Montrons que h est bijectif.
Il est clair que h est surjectif car H est engendré par H_1 et H_2. Il reste à montrer que h est injectif, c'est-à-dire que l'image d'un mot réduit dans $H_1 * H_2 \setminus \{\varepsilon\}$ par h n'est pas e.
Soit $w \in H_1 * H_2 \setminus \{\varepsilon\}$. Il y a 4 formes possibles pour w.
Premier cas : $w = a_1 b_1 a_2 b_2 \cdots a_{k-1} b_{k-1} a_k$ avec $a_1, \cdots, a_k \in H_1 \setminus \{e\}$ et $b_1, \cdots, b_{k-1} \in H_2 \setminus \{e\}$
Alors $h(w)(H_2) = a_1 \cdot b_1 \cdots b_{k-1} \cdot a_k(H_2) \subset a_1 \cdot b_1 \cdots b_{k-1}(H_1) \subset \cdots \subset a_1 \cdot b_1(H_1) \subset a_1(H_2) \subset H_1$
Or $H_2 \not\subset H_1$ donc $h(w) \neq e$.
Deuxième cas : $w = b_1 a_1 b_2 a_2 \cdots b_{k-1} a_{k-1} b_k$ avec $a_1, \cdots, a_{k-1} \in H_1 \setminus \{e\}$ et $b_1, \cdots, b_k \in H_2 \setminus \{e\}$
Alors l'argument précédent s'applique à awa^{-1} avec $a \in H_1 \setminus \{e\}$ donc $h(awa^{-1}) \neq e$ donc $h(w) \neq e$.
Troisième cas : $w = a_1 b_1 a_2 b_2 \cdots a_k b_k$ avec $a_1, \cdots, a_k \in H_1 \setminus \{e\}$ et $b_1, \cdots, b_k \in H_2 \setminus \{e\}$
Alors l'argument précédent s'applique à awa^{-1} avec $a \in H_1 \setminus \{e, a_1^{-1}\}$ donc $h(w) \neq e$.
Quatrième cas : $w = b_1 a_1 b_2 a_2 \cdots b_k a_k$ avec $a_1, \cdots, a_k \in H_1 \setminus \{e\}$ et $b_1, \cdots, b_k \in H_2 \setminus \{e\}$
Alors l'argument précédent s'applique à awa^{-1} avec $a \in H_1 \setminus \{e, a_k\}$ donc $h(w) \neq e$. $\square$



Ce lemme est très puissant, et l'auteur donne de nombreux exemples d'utilisation de ce lemme. En voici un :

Exemple 12.
Dans $SL_2(\mathbb{Z})$, le sous-groupe engendré par les matrices $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$ est un sous-groupe libre d'ordre 2.

Démonstration. Considérons naturellement les sous-groupes de $SL_2(\mathbb{Z})$

$$H_1 = \left\langle \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \right\rangle = \left\{ \begin{pmatrix} 1 & 2n \\ 0 & 1 \end{pmatrix}, n \in \mathbb{Z} \right\} \text{ et } H_2 = \left\langle \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \right\rangle = \left\{ \begin{pmatrix} 1 & 0 \\ 2n & 1 \end{pmatrix}, n \in \mathbb{Z} \right\}.$$

Comme $GL_2(\mathbb{R})$ agit sur $\mathbb{R}^2$, $SL_2(\mathbb{Z})$ également. Considérons alors les ensembles $X_1 = \{(x, y) \in \mathbb{R}^2 : |x| > |y|\}$ et $X_2 = \{(x, y) \in \mathbb{R}^2 : |x| < |y|\}$.
Vérifions les hypothèse du lemme du ping-pong : les hypothèses de cardinalité sont toutes vérifiées, on a bien $X_2 \not\subset X_1$, soit $n \in \mathbb{Z} \setminus \{0\}$, et $(x, y) \in X_1$. Alors $\begin{pmatrix} 1 & 0 \\ 2n & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ 2nx + y \end{pmatrix}$.
Or on a $|x| > |y|$, donc $|2nx + y| \geqslant |2nx| - |y| = 2|n||x| - |y| \geqslant 2|x| - |y| > |x|$ car comme est un entier non nul, $|n| \geqslant 1$. L'autre inclusion à montrer est totalement similaire à celle-ci, et le lemme du ping-pong s'applique donc. $\square$

Théorème 3. *(Alternative de Tits)*
Soit G un sous-groupe de $GL(N, \mathbb{K})$ avec $N \geqslant 1$ et $\mathbb{K}$ un corps de caractéristique nulle. Alors soit G a un sous-groupe libre non commutatif, soit G a un sous-groupe résoluble d'indice fini.