Groupes libres, générateurs et relations

1 Groupes libres

1.1 Partie libre d'un groupe

Soit G un groupe, et X une partie de G. Si on trouve $x_1, \ldots, x_n$ dans X, et $\varepsilon_1, \ldots, \varepsilon_n$ dans $\{-1, 1\}$ tels que le produit $x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n}$ soit l'élément neutre de G, on dit que l'expression

$$x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n} = 1 \tag{1}$$

est une *relation* entre les éléments de X. Si dans cette relation il existe un i tel que $x_i = x_{i+1}$, et $\varepsilon_i = -\varepsilon_{i+1}$, l'associativité de la loi de composition permet d'obtenir une relation réduite équivalente en supprimant $x_i^{\varepsilon_i} x_{i+1}^{\varepsilon_{i+1}}$. En continuant ainsi tant qu'une telle simplification est possible (ce qui ne peut arriver qu'un nombre fini de fois), on obtient à la fin une relation *irréductible*, toujours équivalente à (1). Il est possible que cette expression finale soit simplement "$1 = 1$", auquel cas la relation de départ (1) est dite *triviale* (cela signifie en fait que cette relation est toujours vérifiée, pour n'importe quels éléments d'un groupe quelconque). Voici deux exemples de relations triviales

$$a^{-1}baa^{-1}b^{-1}a = 1 \quad ; \quad xz^{-1}y^2tt^{-1}y^{-2}zx^{-1} = 1.$$

Si l'expression (1) est non triviale, on dira que les éléments de X sont *liés* par cette relation. Remarquons alors que pour tout morphisme φ de G dans un groupe quelconque G', les images des éléments de X sont eux aussi liés par une relation non triviale : celle obtenue formellement à partir de (1) en remplaçant x_i par $\varphi(x_i)$. Par un morphisme de groupe, les images d'éléments liés par une telle relation ne peuvent donc pas être n'importe quoi !

Si il n'existe aucune relation non triviale liant les éléments de X, on dit que X est une partie *libre* du groupe G.

Si x et y sont deux éléments distincts de X qui commutent, on peut écrire la relation non triviale

$$xyx^{-1}y^{-1} = 1. \tag{2}$$

Ainsi, deux éléments distincts d'une partie libre d'un groupe ne peuvent jamais commuter. En particulier, une partie libre ne peut contenir *à la fois* un élément x et son inverse x^{-1} : s'ils sont distincts, ils commutent, ce qui contredirait la remarque précédente, et s'ils sont égaux, on a dans X la relation non triviale $x^2 = 1$.

1.2 Groupe libre

Un groupe G est dit *libre sur* X si X est une partie à la fois libre et génératrice de G (on dit alors que X est une *base* de X).

Proposition 1.1 *Le groupe G est libre sur X si et seulement si chaque $g \in G$, $g \neq 1$, s'écrit de manière* unique *sous la forme*

$$g = x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n},$$

où $x_1, \ldots, x_n$ sont dans X, $\varepsilon_1, \ldots, \varepsilon_n$ sont dans $\{-1, 1\}$, et il n'existe pas d'indice $i \in \{1, \ldots, n-1\}$ tel que $x_i = x_{i+1}$ et $\varepsilon_i = -\varepsilon_{i+1}$.

Preuve — Laissée en exercice.

Formellement, la définition de groupe libre ressemble étrangement à celle de groupe *abélien* libre. Pourtant, ces notions ne coïncident pas (voir l'exercice qui suit). La différence tient dans la notion de relation *triviale* entre les éléments du groupe : dans le cadre d'un groupe abélien, la relation de commutation (2) est considérée comme triviale, ce qui n'est plus le cas dans le cadre général !

Exercice 1.1 *Soit G un groupe libre sur X. Vérifier que si X est non vide, G est sans torsion, et que si $|X| \geq 2$, alors G n'est pas abélien.*

1.3 Construction d'un groupe libre sur un ensemble X

Étant donné un ensemble quelconque X, il est toujours possible de construire de manière canonique un groupe F_X libre sur X. On considère un autre ensemble X' de même cardinal, et disjoint de X. Une bijection $i : X \longrightarrow X'$ étant fixée, on note pour tout $x \in X$ $x^{-1} \stackrel{\text{déf}}{=} i(x)$, et $x^1 \stackrel{\text{déf}}{=} x$. Un *mot* sur l'ensemble $Y \stackrel{\text{déf}}{=} X \cup X'$ est une suite finie d'éléments de Y, notée sous la forme $w = x_1^{\varepsilon_1} \ldots x_n^{\varepsilon_n}$, où $x_i \in X$, et $\varepsilon_i \in \{-1, 1\}$. L'entier n est la *longueur* de ce mot. On identifie les mots de longueur 1 avec les éléments de Y, et on convient qu'il existe un unique mot de longueur 0, que l'on note 1. L'ensemble de tous les mots sur Y est noté Y^*, et on définit sur cet ensemble l'opération de *concaténation* en posant, pour $w = x_1^{\varepsilon_1} \ldots x_n^{\varepsilon_n}$ et $\tilde{w} = \tilde{x}_1^{\tilde{\varepsilon}_1} \ldots \tilde{x}_m^{\tilde{\varepsilon}_m}$ dans Y^*

$$w\tilde{w} \stackrel{\text{déf}}{=} x_1^{\varepsilon_1} \ldots x_n^{\varepsilon_n} \tilde{x}_1^{\tilde{\varepsilon}_1} \ldots \tilde{x}_m^{\tilde{\varepsilon}_m},$$

le mot de longueur nulle étant neutre pour cette opération : $\forall w \in Y^*$, $1w = w1 \stackrel{\text{déf}}{=} w$.

Un mot $w = x_1^{\varepsilon_1} \ldots x_n^{\varepsilon_n}$ dans Y^* sera dit *réduit* si il n'existe pas d'indice $i \in \{1, \ldots, n-1\}$ tel que $x_1 = x_{i+1}$ et $\varepsilon_i = -\varepsilon_{i+1}$. Tous les mots de longueur 1 et celui de longueur nulle sont bien sûrs réduits. Notre groupe F_X sera justement l'ensemble des mots réduits muni d'une loi de composition précisée dans la suite. On peut voir F_X comme l'ensemble des combinaisons formelles d'éléments de X que l'on ne peut pas simplifier.

On va définir par récurrence sur $\min\{n, m\}$ le produit $w.\tilde{w}$ des deux mots réduits w et $\tilde{w}$, de longueur respectives n et m. Si ce minimum vaut 0, c'est que l'un des deux vaut 1, dans ce cas on pose évidemment $w.1 \stackrel{\text{déf}}{=} w$ et $1.\tilde{w} \stackrel{\text{déf}}{=} \tilde{w}$.

Soient maintenant $w = x_1^{\varepsilon_1} \ldots x_n^{\varepsilon_n}$ et $\tilde{w} = \tilde{x}_1^{\tilde{\varepsilon}_1} \ldots \tilde{x}_m^{\tilde{\varepsilon}_m}$ deux mots réduits, et supposons par récurrence que l'on sache déjà définir le produit de deux mots réduits lorsque l'un des deux est de longueur strictement inférieure à $\min\{n, m\}$. Si la concaténation $w\tilde{w}$ est encore un mot réduit, on pose $w.\tilde{w} \stackrel{\text{déf}}{=} w\tilde{w}$. Si ce n'est pas le cas, c'est que $\tilde{x}_1 = x_n$, et $\tilde{\varepsilon}_1 = -\varepsilon_n$ et on pose alors $w.\tilde{w} \stackrel{\text{déf}}{=} x_1^{\varepsilon_1} \ldots x_{n-1}^{\varepsilon_{n-1}} . \tilde{x}_2^{\tilde{\varepsilon}_2} \ldots \tilde{x}_m^{\tilde{\varepsilon}_m}$.

Exercice 1.2 *Vérifier que le groupe F_X des mots réduits sur Y^* muni du produit défini ci-dessus est bien un groupe, et que X en est une famille libre et génératrice.*

Exercice 1.3 *Étant donné un ensemble X quelconque, montrer que l'on peut aussi construire de manière canonique un groupe* abélien $F_{(X)}$ *qui est libre de base X.*

1.4 Propriété universelle d'un groupe libre sur X

Théorème 1.2 *Soit G un groupe, et X une partie génératrice de G. Le groupe G est libre sur X si et seulement si pour tout groupe F et toute application $f : X \longrightarrow F$, il existe un unique homomorphisme de groupes de G dans F qui prolonge f.*

Preuve — Si G est libre sur X, on sait que tout $g \in G \setminus \{1\}$ s'écrit de manière unique sous la forme
$$g = x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n},$$
où les x_i sont dans X, les ε_i valent 1 ou -1, et il n'existe pas d'indice $i \in \{1, \ldots, n-1\}$ tel que $x_i = x_{i+1}$ et $\varepsilon_i = -\varepsilon_{i+1}$. Étant donnée une application f de X dans un groupe F, la seule façon de prolonger f en un morphisme φ de groupes entre G et F est de poser, pour un g qui s'écrit comme ci-dessus,
$$\varphi(g) \stackrel{\text{déf}}{=} f(x_1)^{\varepsilon_1} \cdots f(x_n)^{\varepsilon_n}.$$
Or, comme une telle écriture pour g est unique, cette formule définit sans ambiguïté une application de G vers F, et on vérifie facilement que cette application est un morphisme de groupes [...].

Réciproquement, supposons que toute application f de X vers un groupe F se prolonge en un unique homomorphisme de G vers F. Considérons en particulier l'injection canonique de X dans F_X, groupe libre sur X défini au paragraphe précédent. Elle se prolonge en un unique homomorphisme φ de G vers F_X. Puis, F_X étant libre sur X, on sait que l'injection canonique de X dans G se prolonge en un unique morphisme ψ de F_X dans G. On a alors $\psi \circ \varphi = \mathrm{Id}_G$ [...], ce qui prouve que φ est injectif, puis $\varphi \circ \psi = \mathrm{Id}_{F_X}$ [...], ce qui prouve que φ est surjectif. Finalement, φ est un isomorphisme entre G et F_X, qui vaut l'identité sur X. On en déduit que G est lui aussi libre sur X. ❑

Exercice 1.4 *Énoncer et démontrer la propriété universelle analogue pour un groupe* abélien *libre de base X.*

2 Générateurs et relations

2.1 Présentation d'un groupe

Soit G un groupe, et X une partie génératrice de G. D'après le théorème 1.2, l'injection naturelle de X dans G se prolonge en un unique morphisme de groupe φ de F_X (groupe libre sur X construit en 1.3) vers G ; et comme $< X >= G$, φ est surjectif. Le premier théorème d'isomorphisme permet alors d'affirmer que $G = \mathrm{Im}\,\varphi$ est isomorphe à $F_X/\mathrm{Ker}\,\varphi$, d'où le théorème qui suit.

Théorème 2.1 *Tout groupe est isomorphe à un groupe quotient d'un groupe libre.*

Notons de plus que chaque élément r de $\mathrm{Ker}\,\varphi$ fournit une relation non triviale "$r = 1$" entre les éléments de X dans G. Inversement, toute relation non triviale dans G liant les éléments de X s'écrit sous la forme "$r = 1$" avec $r \in \mathrm{Ker}\,\varphi$.

Ce qui précède montre que le groupe G est entièrement déterminé (à isomorphisme près) une fois que l'on connaît une partie génératrice X et l'ensemble $\operatorname{Ker}\varphi$ des relations non triviales liant les éléments de X. Il est généralement impossible d'énumérer de manière exhaustive tous les éléments de $\operatorname{Ker}\varphi$; mais la donnée d'une partie R de F_X telle que le sous-groupe *normal* de F_X engendré par R soit $\operatorname{Ker}\varphi$ suffit.

On appelle *présentation* du groupe G un couple noté $(X|R)$ tel que X soit une partie génératrice de G, et R une partie de F_X telle que G soit isomorphe au groupe quotient $F_X/(R)$, où (R) est le sous-groupe normal de F_X engendré par R. Si R est fini, on dit que X est *de présentation finie.*

Par exemple, $(x|x^n)$ est une présentation du groupe cyclique d'ordre n de générateur x. En effet, si $X = \{x\}$ est un singleton, le groupe F_X libre sur X est égal à $\{x^p,\ p \in \mathbb{Z}\}$, isomorphe à $\mathbb{Z}$, et le sous-groupe normal engendré par $R = \{x^n\}$ est $\{x^{np},\ p \in \mathbb{Z}\}$. Le groupe quotient $F_X/(R)$ est donc dans ce cas isomorphe à $\mathbb{Z}/n\mathbb{Z}$, qui est bien cyclique d'ordre n.

Exercice 2.1 *Montrer que si m et n sont deux entiers premiers entre eux,*

$$(x, y|x^n, y^m, xyx^{-1}y^{-1})$$

est une autre présentation du groupe cyclique d'ordre mn.

Voyons maintenant d'autres exemples de présentations de groupes.

2.2 Le groupe diédral D_n

Soit $n \geq 2$ un entier. On appelle *groupe diédral de degré n* le groupe des isométries du plan euclidien préservant un polygone régulier à n sommets. Ce groupe se note habituellement D_n. Si O est le centre du polygone, et $A_1, \ldots, A_n$ ses sommets, D_n contient evidemment la rotation ρ de centre O et d'angle $2\pi/n$, et la symétrie orthogonale σ d'axe (OA_1). La rotation ρ est d'ordre n, aussi les $2n$ isométries $\mathrm{Id}, \rho, \ldots, \rho^{n-1}, \sigma, \sigma\circ\rho, \ldots, \sigma\circ\rho^{n-1}$ sont deux à deux distinctes [...], et toutes dans D_n.

Exercice 2.2 *Montrer que D_n ne contient que $2n$ isométries, i.e.*

$$D_n = \{Id, \rho, \ldots, \rho^{n-1}, \sigma, \sigma\circ\rho, \ldots, \sigma\circ\rho^{n-1}\}$$

et vérifier que chaque élément de D_n de la forme $\sigma\circ\rho^j$ est d'ordre 2.

Proposition 2.2 *Soit G un groupe engendré par 2 éléments a et b, avec a d'ordre n ($n \geq 2$), b et ab d'ordre 2. Alors G est isomorphe au groupe diédral D_n.*

Preuve — Sous ces hypothèses, b ne peut pas appartenir au sous-groupe cyclique engendré par a [...]. G contient donc au moins $2n$ éléments distincts : $1, a, \ldots, a^{n-1}, b, ba, \ldots, ba^{n-1}$. Puis, en utilisant l'égalité $ab = ba^{-1}$, il est facile de montrer que chaque élément de la forme ba^j est d'ordre 2, et que le produit de deux quelconques des $2n$ éléments listés ci-dessus appartient encore à cette liste. On en déduit que les hypothèses faites sur G déterminent complètement sa structure de groupe, et donc G est isomorphe à D_n, qui vérifie les mêmes hypothèses. ❑

Remarque. Le groupe diédral D_2 est isomorphe au groupe produit $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, aussi appelé *groupe de Klein.* C'est le seul groupe diédral commutatif. Le groupe diédral D_3 est lui isomorphe au groupe symétrique $\mathbf{S}_3$.

Proposition 2.3 *Pour $n \geq 2$, $\Big(a, b | a^n, b^2, abab\Big)$ est une présentation du groupe diédral D_n.*

Preuve — Soit $F \overset{\text{déf}}{=} F_{\{a,b\}}$ le groupe libre sur $\{a, b\}$, et H le sous-groupe normal de F engendré par $R \overset{\text{déf}}{=} \{a^n, b^2, abab\}$, c'est-à-dire l'intersection de tous les sous-groupes normaux de F contenant R. Pour $x \in F$, on note $\dot{x}$ la classe de x dans le groupe quotient F/H. Puisque F est engendré par a et b, F/H est engendré par $\dot{a}$ et $\dot{b}$. Pour montrer que F/H est isomorphe au groupe diédral D_n, il suffit d'après la proposition 2.2 de vérifier que, dans ce groupe quotient, $\dot{a}$ est d'ordre n, $\dot{b}$ et $\dot{a}\dot{b}$ sont d'ordre 2.

Puisque $a^n \in H$, on a évidemment $\dot{a}^n = 1$ dans F/H. Il s'agit maintenant de voir pourquoi $\dot{a}^k \neq 1$ lorsque $1 \leq k < n$. Considérons l'application f de $\{a, b\}$ dans le groupe diédral D_n définie par $f(a) \overset{\text{déf}}{=} \rho$ et $f(b) \overset{\text{déf}}{=} \sigma$. Grâce à la propriété universelle du groupe libre F énoncée dans le théorème 1.2, on sait que f peut être prolongée en un unique morphisme $\varphi \,:\, F \longrightarrow D_n$. Son noyau $\operatorname{Ker}\varphi$ est alors un sous-groupe normal de F, qui contient a^n, b^2 et $abab$. On en déduit que $H \subset \operatorname{Ker}\varphi$. Or, pour $1 \leq k < n$, $\varphi(a^k) = \rho^k \neq \mathrm{Id}$, et donc $a^k \notin \operatorname{Ker}\varphi$; on a donc $a^k \notin H$, ce qui prouve que $\dot{a}^k \neq 1$ dans F/H. Ainsi, $\dot{a}$ est bien d'ordre n.

On prouve de la même façon que $\dot{b}$ et $\dot{a}\dot{b}$ sont d'ordre 2, ce qui achève la preuve de la proposition. ❑

2.3 Présentation d'un groupe abélien libre

Soient a et b deux éléments d'un groupe G. *Le commutateur* de a et b est l'élément de G noté $[a, b]$ défini par

$$[a, b] \overset{\text{déf}}{=} aba^{-1}b^{-1}.$$

On appelle *groupe dérivé de* G le sous-groupe de G engendré par les commutateurs. On le note $D(G)$. Remarquons que le commutateur de a et b vaut 1 si et seulement si a et b commutent. Ainsi, G est abélien si et seulement si $D(G) = \{1\}$.

Le groupe dérivé de G est un sous-groupe *caractéristique* de G, ce qui signifie qu'il est stable par tout automorphisme de G. En effet, si γ est un automorphisme de G, on vérifie aisément que pour a et b quelconques dans G, on a toujours $\gamma([a, b]) = [\gamma(a), \gamma(b)]$.

En particulier, $D(G)$ est stable par les automorphismes intérieurs, donc c'est un sous-groupe normal de G.

Exercice 2.3 *Soit N un sous-groupe normal du groupe G. Vérifier que le groupe quotient G/N est abélien si et seulement si $D(G) \subset N$.*

En conséquence du résultat énoncé dans l'exercice précédent, le groupe quotient $G/D(G)$ est abélien.

Théorème 2.4 *Soit X un ensemble non vide, et $F_{(X)}$ le groupe abélien libre de base X. Alors $F_{(X)}$ est isomorphe au quotient $F_X/D(F_X)$. Une présentation de $F_{(X)}$ est donc*

$$\Big(X \;\Big|\; [x, y],\ (x, y) \in X \times X\Big).$$

Preuve — On peut considérer X à la fois comme une partie du groupe libre F_X et une partie du groupe abélien libre $F_{(X)}$. Grâce à la propriété universelle du groupe libre F_X (théorème 1.2), il existe un unique morphisme $\varphi\ :\ F_X \longrightarrow F_{(X)}$ tel que $\forall x \in X$, $\varphi(x) = x$. Le groupe $F_{(X)}$ étant abélien, il en va de même du groupe quotient $F_X/\operatorname{Ker}\varphi$, et donc d'après l'exercice 2.3, $D(F_X) \subset \operatorname{Ker}\varphi$. En conséquence, π désignant la projection canonique de F_X sur $F_X/D(F_X)$, il existe un unique morphisme $\psi\ :\ F_X/D(F_X) \longrightarrow F_{(X)}$ vérifiant $\psi \circ \pi = \varphi$. En particulier, pour tout $x \in X$ on a $\psi \circ \pi(x) = \varphi(x) = x$.

$$\begin{tikzcd}
X \arrow[r, hook] \arrow[dr, hook] & F_X \arrow[d, "\varphi"'] \arrow[dr, "\pi"] & \\
& F_{(X)} \arrow[r, shift right, "\psi'"'] & F_X/D(F_X) \arrow[l, shift right, "\psi"']
\end{tikzcd}$$

Utilisons maintenant la propriété universelle du groupe abélien libre $F_{(X)}$. Puisque le quotient $F_X/D(F_X)$ est abélien, il existe un unique morphisme $\psi'\ :\ F_{(X)} \longrightarrow F_X/D(F_X)$ tel que pour tout $x \in X$, $\psi'(x) = \pi(x)$. Pour tout $x \in X$, on a alors $\psi(\psi'(x)) = \psi(\pi(x)) = x$, et comme X engendre $F_{(X)}$, $\psi \circ \psi' = \mathrm{Id}_{F_{(X)}}$. De même, pour tout $x \in X$, $\psi'(\psi \circ \pi(x)) = \psi'(x) = \pi(x)$, et comme $\pi(X)$ engendre le groupe $F_X/D(F_X)$, $\psi' \circ \psi = \mathrm{Id}_{F_X/D(F_X)}$.

Ainsi, ψ est inversible d'inverse ψ', et donc ψ est un isomorphisme entre $F_X/D(F_X)$ et $F_{(X)}$. ❏

3 Rang d'un groupe libre

3.1 Définition du rang d'un groupe libre

Théorème 3.1 *Soit G un groupe libre, X et Y deux parties génératrices libres de ce groupe. Alors X et Y ont même cardinal.*

Preuve — Il suffit de montrer que, X et Y étant des ensembles non vides, les groupes libres F_X et F_Y sont isomorphes si et seulement si $|X| = |Y|$.

Si X et Y ont même cardinal, il est facile de construire un isomorphisme entre F_X et F_Y en étendant une bijection entre ces deux ensembles aux groupes libres qu'ils engendrent (utiliser le théorème 1.2).

Réciproquement, si F_X et F_Y sont isomorphes, alors les groupes quotients $F_X/D(F_X)$ et $F_Y/D(F_Y)$ le sont également. On en déduit d'après le théorème 2.4 que le groupe abélien libre $F_{(X)}$ de base X est isomorphe au groupe abélien libre $F_{(Y)}$, de base Y. Ces deux groupes abéliens libres sont donc de même rang, d'où $|X| = |Y|$. ❏

Comme pour les groupes abéliens libres, on appelle *rang* du groupe libre G le cardinal commun de ses parties libres génératrices.

3.2 Sous-groupe d'un groupe libre

Il est naturel de se demander si un sous-groupe d'un groupe libre est encore un groupe libre. La réponse est oui, mais la situation est beaucoup moins simple que pour les groupes abéliens libres ; aussi on ne démontre pas ici le théorème suivant.

Théorème 3.2 (Nielsen-Schreier) *Un sous-groupe d'un groupe libre est encore un groupe libre.*

Malheureusement, le rang d'un sous-groupe d'un groupe libre peut être plus grand que celui du groupe de départ. Un groupe libre de rang fini peut même contenir des sous-groupes de rang infini !

Pour la démonstrations des résultats cités dans ce paragraphe, le lecteur pourra consulter les ouvrages cités ci-dessous.

Références

[1] Josette CALAIS. *Éléments de Théorie des Groupes.* Puf, 1998.

[2] J.J. ROTMAN. *An Introduction to the Theory of Groups.* Graduate Texts in Mathematics. Springer-Verlag, 1995.

[3] M. SUZUKI. *Group Theory I.* Springer-Verlag, 1982.