7. Complément I : Groupes additifs et multiplicatif usuels

On discute dans cette partie de quelques aspects de la structure des groupes additifs et multiplicatifs des anneaux $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$. Tous les groupes considérés ici seront donc abéliens. On a déjà vu que les sous-groupes de $\mathbb{Z}$ sont les $\mathbb{Z}n$ avec $n \in \mathbb{Z}$, on en déduit le :

COROLLAIRE 7.1. *Les sous-groupes de type fini de $\mathbb{Q}$ sont les $\mathbb{Z}\lambda$ avec $\lambda \in \mathbb{Q}$.*

DÉMONSTRATION — Soit $H = \sum_{i=1}^{n} \mathbb{Z}\lambda_i \subset \mathbb{Q}$. En considérant un dénominateur commun $m \geq 1$ des λ_i, on a $mH \subset \mathbb{Z}$, où $mH = \{mh \,|\, h \in H\}$. Mais alors mH est un sous-groupe de $\mathbb{Z}$, et donc de la forme $\mathbb{Z}n$. On en déduit $H = \mathbb{Z}\frac{n}{m}$. □

REMARQUE 7.2. *Il existe des sous-groupes de $\mathbb{Q}$ qui ne sont pas de type fini, comme le sous-groupe*[9] $\cup_{n\geq 1}\mathbb{Z}\frac{1}{10^n}$ *des nombres décimaux. Nous renvoyons à l'Exercice 2.32 pour une classification de tous les sous-groupes de $\mathbb{Q}$ (elle ne nous servira pas par la suite).*

Considérons maintenant le groupe additif de $\mathbb{R}$. C'est un groupe exotique ! En effet, l'inclusion $\mathbb{Q} \subset \mathbb{R}$ permet de voir $\mathbb{R}$ comme un $\mathbb{Q}$-espace vectoriel. D'après le Théorème 4.5, on peut en considérer une base $(b_i)_{i\in I}$ et donc un isomorphisme de $\mathbb{Q}$-espaces vectoriels $\mathbb{R} \simeq \mathbb{Q}^{(I)}$, le $\mathbb{Q}$-espace vectoriel des suites $(x_i)_{i\in I} \in \mathbb{Q}^I$ avec $x_i = 0$ pour tout $i \in I$ sauf un nombre fini (on renvoie à l'Exemple 1.14 pour les produits restreints). Comme $\mathbb{R}$ est indénombrable, alors que $\mathbb{Q}^n$ l'est pour tout entier $n \geq 1$, on constate que I est infini.[10] Il y a donc toute une zoologie de sous-groupes additifs de $\mathbb{R}$, que l'on n'a pas envie d'étudier en première approche. Une manière de contourner ce problème est de prendre en compte la topologie naturelle de $\mathbb{R}$. Si $H \subset \mathbb{R}$ est un sous-groupe, on constate immédiatement que son adhérence $\overline{H}$ est un sous-groupe (fermé) de $\mathbb{R}$. Ces derniers sont beaucoup plus sympathiques :

PROPOSITION 7.3. *Les sous-groupes fermés de $\mathbb{R}$ sont $\mathbb{R}$ et les $\mathbb{Z}\lambda$ avec $\lambda \in \mathbb{R}$.*

DÉMONSTRATION — Soit H un sous-groupe fermé de $\mathbb{R}$. On peut supposer $H \neq \{0\}$, auquel cas on a l'ensemble $A := H \cap \mathbb{R}_{>0}$ est non vide (considérer $h \mapsto -h$). Supposons d'abord $a = 0$. Comme $0 \notin A$, il existe une suite $h_n \in A$ tendant vers a. Soient $x \in \mathbb{R}$ et $N \geq 1$ un entier. Pour n assez grand on a $0 < h_n < 1/N$ et donc il existe $m \in \mathbb{Z}$ avec $|mh_n - x| \leq 1/N$. Ainsi, les éléments de H de la forme mh_n, avec $m \in \mathbb{Z}$ et $n \geq 1$ sont denses dans $\mathbb{R}$, puis $H = \mathbb{R}$. On peut donc supposer $a = 0$. Soit $h \in H$. Il existe $n \in \mathbb{Z}$ avec $0 \leq h - na < a$, et donc $h - na \in H$ est nul par définition de a. On a montré $H = \mathbb{Z}\,a$. □

Enfin, on a $\mathbb{C} \simeq \mathbb{R}^2$ comme $\mathbb{R}$-espace vectoriel, et donc comme groupe additif. Là encore, c'est une question un peu exotique d'étudier tous les sous-groupes de $\mathbb{C}$: en fait on a les isomorphismes de $\mathbb{Q}$-espaces vectoriels suivants (noter $I \sim I \coprod I$ pour I infini) :

$$\mathbb{R} \simeq \mathbb{Q}^{(I)} \simeq \mathbb{Q}^{(I \coprod I)} \simeq \mathbb{Q}^{(I)} \times \mathbb{Q}^{(I)} \simeq \mathbb{R}^2 \simeq \mathbb{C}$$

9. On vérifie aisément que si G est un groupe, et si $\{G_n\}_{n\geq 0}$ est une famille *croissante* de sous-groupes de G, *i.e.* vérifiant $G_n \subset G_{n+1}$, alors $\cup_{n\geq 0} G_n$ est un sous-groupe de G.

10. On peut en fait montrer que I est en bijection avec $\mathbb{R}$: voir l'Exercice 1.17 Chap. 1

Bien sûr, un tel isomorphisme n'est pas continu en tant qu'application $\mathbb{R} \to \mathbb{C}$! Dans la lignée de la Proposition 7.3, nous verrons au Complément 6 Chap. 3 que les sous-groupes *fermés* de $\mathbb{R}^n$, avec $n \geq 1$ quelconque, admettent une description intéressante.

Discutons maintenant des *groupes multiplicatifs*. Déjà, le groupe

$$\mathbb{Z}^\times = \{\pm 1\}$$

est à isomorphisme près l'unique groupe à 2 éléments. Pour décrire $\mathbb{Q}^\times$ on note P l'ensemble des nombres premiers et on considère le sous-groupe $\mathbb{Z}^{(\mathrm{P})} \subset \mathbb{Z}^{\mathrm{P}}$ des (x_p) avec $x_p = 0$ pour tout p sauf un nombre fini. On constate que l'application $(\epsilon, (n_p)_{p\in P}) \mapsto \epsilon \prod_{p\in \mathrm{P}} p^{n_p}$ définit un isomorphisme de groupes

$$\{\pm 1\} \times \mathbb{Z}^{(\mathrm{P})} \xrightarrow{\sim} \mathbb{Q}^\times,$$

le caractère bijectif de cette application venant de la factorisation unique d'un entier en produit de nombres premiers. On constate aussi que $\mathbb{R}_{>0}$ est un sous-groupe de $\mathbb{R}^\times$, et que l'application $(\epsilon, \lambda) \mapsto \epsilon\lambda$ induit un isomorphisme de groupes

$$\{\pm 1\} \times \mathbb{R}_{>0} \xrightarrow{\sim} \mathbb{R}^\times.$$

Enfin, l'application exponentielle $\exp : \mathbb{R} \to \mathbb{R}_{>0}$ induit un isomorphisme

$$\mathbb{R} \simeq \mathbb{R}_{>0},$$

et le groupe additif $\mathbb{R}$ a déjà étudié. Notons que l'exponentielle est continue d'inverse (le logarithme) continu : c'est un homéomorphisme, de sorte que les sous-groupes fermés de $\mathbb{R}_{>0}$ (pour la topologie usuelle) se déduisent aussi de ceux de $\mathbb{R}$: ce sont donc $\mathbb{R}_{>0}$ et les $a^{\mathbb{Z}}$ avec $a \in \mathbb{R}_{>0}$. On note enfin $\mathbb{U}$, $\mathrm{U}(1)$ ou S^1 le sous-groupe des éléments de $\mathbb{C}^\times$ de valeur absolue 1 (*cercle unité*). La multiplication dans $\mathbb{C}^\times$ induit un isomorphisme

$$\mathbb{R}_{>0} \times \mathbb{U} \xrightarrow{\sim} \mathbb{C}^\times.$$

Décrivons les sous-groupes de $\mathbb{U}$. On considère pour cela l'application

$$\psi : \mathbb{R} \to \mathbb{U},\ x \mapsto e^{2i\pi x}.$$

C'est un morphisme de groupes, surjectif de noyau $\mathbb{Z}$. Elle induit donc un isomorphisme de groupes

$$\mathbb{R}/\mathbb{Z} \simeq \mathbb{U},\ x + \mathbb{Z} \mapsto e^{2i\pi x}.$$

En particulier, tout sous-groupe H de $\mathbb{U}$ est de la forme $H = \psi(H')$ où H' est un sous-groupe de $\mathbb{R}$ contenant $\mathbb{Z}$ (Proposition 2.10), et on a alors $H' = \psi^{-1}(H)$. Nous nous sommes donc encore ramenés aux sous-groupes de $\mathbb{R}$. Là encore, les sous-groupes fermés de $\mathbb{U}$ (pour la topologie usuelle) sont les plus raisonnables. Rappelons que $\mu_n \subset \mathbb{C}^\times$ désigne le sous-groupe (cyclique d'ordre n) des racines n-èmes de l'unité.

PROPOSITION 7.4. *Les sous-groupes fermés de $\mathbb{U}$ sont $\mathbb{U}$ et les μ_n avec $n \geq 1$.*

DÉMONSTRATION — Si H est un sous-groupe fermé de $\mathbb{U}$ alors, par continuité de ψ, $H' = \psi^{-1}(H)$ est un sous-groupe fermé de $\mathbb{R}$. Si $H' = \mathbb{R}$ on a $H = \psi(H') = \mathbb{U}$. Sinon, il existe $\lambda \in \mathbb{R}$ tel que $H' = \mathbb{Z}\lambda$. Mais on a aussi $H' \supset \ker\psi = \mathbb{Z}$, donc il existe $n \in \mathbb{Z}$ tel que $n\lambda = 1$, *i.e.* $\lambda = 1/n$. Cela montre $H = \psi(\mathbb{Z}\frac{1}{n}) = \mu_n$. □

REMARQUE 7.5. (Groupes topologiques) Un *groupe topologique* est la donnée d'un groupe G, et d'une topologie sur l'ensemble G, tels que la loi de groupe $G\times G \to G, (x,y) \mapsto xy$ et l'inversion $G \to G, x \mapsto x^{-1}$, soient continues. Quand $k = \mathbb{R}$ ou $\mathbb{C}$, auquel cas on le note souvent $\mathbb{K}$, c'est le cas des groupes additifs $\mathbb{K}$ et $\mathbb{K}^n$ (topologie d'espace vectoriel normé) et aussi du groupe multiplicatif $\mathbb{K}^\times$, et plus généralement de $\mathrm{GL}_n(\mathbb{K})$ (ouvert de l'espace vectoriel normé $\mathrm{M}_n(\mathbb{K})$ défini par $\det \neq 0$). Dans tous ces cas, comme on l'a entrevu, les sous-groupes *fermés* sont alors les plus pertinents à considérer. Les outils idoines pour les étudier sont les notions de *groupes de Lie* et d'*algèbre de Lie*. Bien entendu, ces notions n'ont pas leur place dans un cours introductif comme celui-ci, et c'est pourquoi nous restreindrons le plus souvent dans ce cours à l'étude de leurs sous-groupes finis (voire *discrets*), sur lesquels les notions de Lie ne disent absolument rien par ailleurs (en fait, c'est même le cas le plus difficile !).

8. Complément II : Groupes libres

Soit X un ensemble. On se propose dans ce complément d'introduire le *groupe libre sur* X. Le cas où X est fini sera déjà très intéressant. Pensons à X comme à un alphabet et introduisons l'ensemble des *mots sur* X comme étant

$$\mathrm{Mots}(X) = \coprod_{n\geq 0} X^n.$$

Par convention, on a posé ici $X^0 = \{1\}$, et on note aussi $\emptyset$ son unique élément 1, appelé *mot vide*. Un élément de $X^n \subset \mathrm{Mots}(X)$ sera appelé *mot de longueur* n sur X, et on notera simplement $x_1 \cdots x_n$ le n-uplet $(x_1, \cdots, x_n)$. On définit une loi de composition sur $\mathrm{Mots}(X)$ par la concaténations des mots :

$$X^n \times X^m \to X^{n+m}, (x_1 \cdots x_n, y_1 \cdots y_m) \mapsto x_1 \cdots x_n y_1 \cdots y_n.$$

Cette loi est manifestement associative, de neutre le mot vide $\emptyset$, et fait donc de $\mathrm{Mots}(X)$ un monoïde. On a une inclusion évidente $X \subset \mathrm{Mots}(X)$ (mots de longueur 1). La *propriété universelle* de $\mathrm{Mots}(X)$ est la suivante :

PROPOSITION 8.1. *Soient X un ensemble et M un monoïde. Toute application $X \to M$ s'étend de manière unique en un morphisme de monoïdes* $\mathrm{Mots}(X) \to M$.

DÉMONSTRATION — Soit $f : X \to M$ une application. Supposons que $g : \mathrm{Mots}(X) \to M$ est un morphisme de monoïdes vérifiant $g(x) = f(x)$ pour $x \in X$. On a $g(\emptyset) = 1$ par définition et, pour $n \geq 1$ et $x_1, \ldots, x_n \in X$, on a

$$g(x_1 \cdots x_n) = g(x_1) \cdots g(x_n) = f(x_1) \cdots f(x_n),$$

de sorte que g est uniquement déterminé par f : c'est l'assertion d'unicité. Pour l'existence de g, on pose simplement $g(\emptyset) = 1$ et pour $n \geq 1$, $g(x_1, \ldots, x_n) = f(x_1) \cdots f(x_n)$: c'est clairement un morphisme de monoïdes étendant f. □

On pose maintenant $X^\pm = X \coprod X$. On a deux inclusions naturelles $X \to X^\pm$, à *gauche* et à *droite*. Pour fixer les idées on écrira $X \subset X^\pm$ l'inclusion dans le X de gauche. Tout élément $x \in X^\pm$ dans la copie de X à gauche (resp. droite) a un correspondant que l'on notera x^{-1} dans celle de droite (resp. de gauche). On a ainsi défini une involution $X^\pm \to X^\pm, x \mapsto x^{-1}$, échangeant les deux facteurs. Nous voudrons à terme penser à x^{-1} comme à un inverse de x, mais prenons garde que

cela n'en est pas un dans le monoïde $\mathrm{Mots}(X^{\pm})$. Par exemple si $X = \{a, b\}$ a deux éléments, on a $X^{\pm} = \{a, a^{-1}, b, b^{-1}\}$ et les $2^4 = 16$ mots de longueur 2 sur $X^{\pm}$ sont

$$aa,\ aa^{-1},\ ab,\ ab^{-1},\ a^{-1}a,\ a^{-1}a^{-1},\ a^{-1}b,\ a^{-1}b^{-1},\ ba,\ ba^{-1},\ bb,\ bb^{-1},\ b^{-1}a,\ b^{-1}a^{-1},\ b^{-1}b,\ b^{-1}b^{-1}.$$

Au final, on retiendra qu'en définissant $X^{\pm}$ on a simplement « dédoublé l'alphabet X en rajoutant formellement, pour chaque lettre $x \in X$, la lettre x^{-1} ». Nous renvoyons à l'Exercice 1.1 pour la notion précise de relation d'équivalence engendrée par une relation, utilisée ci-dessous.

Définition 8.2. *Si m et m' sont deux mots sur $X^{\pm}$, on dit que m est une* contraction élémentaire *de m', et on note $m\,C\,m'$, s'il existe $n_1, n_2 \in \mathrm{Mots}(X^{\pm})$ et $x \in X^{\pm}$ tels que $m = n_1 n_2$ et $m' = n_1 x x^{-1} n_2$. On note R la relation d'équivalence sur $\mathrm{Mots}(X^{\pm})$ engendrée par la relation C, et on note l'ensemble quotient associé*

$$\mathrm{F}_X = \mathrm{Mots}(X^{\pm})/R.$$

On dira simplement que deux mots sur $X^{\pm}$ sont *équivalents* s'ils le sont pour R, et on notera $[m]$ la classe d'équivalence de m. Par définition, deux mots sont équivalents si l'un s'obtient à partir de l'autre après une suite finie d'insertions ou suppressions de morceaux de la forme xx^{-1} avec $x \in X^{\pm}$. Il découle facilement des définitions que « la multiplication des mots passe aux classes d'équivalences » :

Lemme 8.3. *Soit M un monoïde, C une relation sur M et R la relation d'équivalence sur M engendrée par C. On suppose que pour tout $m, m', n \in M$ avec $m\,C\,m'$, on a : (i) $mn\,R\,m'n$ et (ii) $nm\,R\,nm'$. Alors il existe une unique loi de monoïde sur M/R telle que la projection canonique $M \to M/R$ est un morphisme de monoïde.*

Démonstration — Soit $\pi : M \to M/R$ la projection canonique. Toute loi de composition $\star$ sur M/R telle que π est un morphisme vérifie $[m]_R \star [m']_R = \pi(m) \star \pi(m') = \pi(mm') = [mm']_R$. Comme π est surjective, $\star$ est donc unique si elle existe, nécessairement associative car la loi de M l'est, et admet $\pi(1) = [1]_R$ pour neutre.

Pour l'existence, il s'agit de montrer que l'application $M \times M \to M/R$, $(m, n) \mapsto [mn]_R$, passe au quotient $M/R \times M/R \to M/R$, c'est-à-dire que pour tous éléments m, m', n, n' dans M vérifiant $m\,R\,m'$ et $n\,R\,n'$, on a $mn\,R\,m'n'$. Fixons donc de tels $m, m', n, n' \in M$. Comme R est engendrée par C, on a une suite d'éléments $m_1, \ldots, m_r$ de M vérifiant $m_1 = m$, $m_r = m'$, et soit $m_i\,C\,m_{i+1}$, soit $m_{i+1}\,C\,m_i$ pour $1 \leq i < r$. Par l'hypothèse (i) sur C, on a donc $m_i n\,R\,m_{i+1} n$ pour $1 \leq i < r$, puis $m_1 n\,R\,m_r n$ par transitivité de R, *i.e.* $mn\,R\,m'n$. Raisonnant de même en utilisant (ii) au lieu de (i), on montre aussi $m'n\,R\,m'n'$, et donc $mn\,R\,m'n'$. □

Ce lemme s'applique bien sûr à $M = \mathrm{Mots}(X^{\pm})$ et à sa relation de contraction C : pour tout $m, m', n \in M$ avec $m\,C\,m'$, on a même $mn\,C\,m'n$ et $nm\,C\,nm'$. Il existe donc une unique structure de monoïde sur F_X telle que la surjection naturelle

$$\mathrm{Mots}(X^{\pm}) \to \mathrm{F}_X,\ m \mapsto [m], \tag{9}$$

est un morphisme de monoïdes. Mais par définition de C on a aussi $[x][x^{-1}] = [xx^{-1}] = 1 = [x^{-1}x] = [x^{-1}][x]$ pour tout $x \in X^{\pm}$, de sorte que $[x^{-1}]$ est un inverse de $[x]$ dans F_X, ce qui était l'effet recherché ! Mais comme $X^{\pm}$ engendre le monoïde $\mathrm{Mots}(X)$, les $[x]$ avec $x \in X^{\pm}$ engendrent aussi F_X, qui est donc un groupe :

Définition 8.4. *Le groupe F_X ainsi défini est* le groupe libre sur X.

Le F dans F_X vient de l'anglais *free group*. Par construction, la projection canonique (9) induit par restriction aux inclusions naturelles $X \to X^{\pm} \to \mathrm{Mots}(X^{\pm})$ une application $X \to \mathrm{F}_X, x \mapsto [x]$. La *propriété universelle de* F_X est la suivante :

PROPOSITION 8.5. *Soient X un ensemble et G un groupe. Pour toute application $f : X \to G$, il existe un unique morphisme de groupes $f' : \mathrm{F}_X \to G$ tel que $f'([x]) = f(x)$ pour tout $x \in X$.*

DÉMONSTRATION — Le morphisme f' est unique s'il existe car les $[x]$ avec $x \in X$ engendrent le groupe F_X. Pour l'existence, on étend d'abord f en une application encore notée $f : X^{\pm} \to G$ en posant $f(x^{-1}) = f(x)^{-1}$ pour $x \in X$. Par la Proposition 8.1, il existe un morphisme de monoïdes $g : \mathrm{Mots}(X^{\pm}) \to G$ tel que $g(x) = f(x)$ et $g(x^{-1}) = f(x)^{-1}$ pour $x \in X$, et donc avec $g(x^{-1}) = g(x)^{-1}$ pour tout $x \in X^{\pm}$.

Supposons que l'on ait $m, m' \in \mathrm{Mots}(X^{\pm})$ avec m contraction élémentaire de m'. On a $m' = n_1 x x^{-1} n_2$ et $m = n_1 n_2$, avec $x \in X^{\pm}$ et n_1, n_2 des mots sur $X^{\pm}$, puis

$$g(m') = g(n_1)g(x)g(x)^{-1}g(n_2) = g(n_1)g(n_2) = g(m).$$

Cela montre que g est constante sur les classes d'équivalence de mots sur $X^{\pm}$, et donc induit par passage au quotient une application $f' : \mathrm{F}_X \to G$ vérifiant $f'([m]) = g(m)$ pour tout $m \in \mathrm{Mots}(X^{\pm})$. Par définition de la loi quotient sur F_X, c'est automatiquement un morphisme de groupes : pour $m, m' \in \mathrm{Mots}(X^{\pm})$ on a les égalités $f'([m][m']) = f'([mm']) = g(mm') = g(m)g(m') = f'([m])f'([m'])$. □

La notion suivante de *mot réduit* nous donnera au final un représentant naturel de chaque classe d'équivalence de mots sur $X^{\pm}$:

DÉFINITION 8.6. *Un mot sur $X^{\pm}$ est dit réduit s'il est vide ou de la forme $x_1 \dots x_n$ avec $x_i \in X^{\pm}$ pour $1 \leq i \leq n$ et $x_{i+1} \neq x_i^{-1}$ pour $1 \leq i < n$.*

Par exemple, pour $a, b \in X$ les mots abb^{-1} et $a^{-1}ab$ ne sont pas réduits, mais aba^{-1} l'est pour $a \neq b$. Un mot de longueur ≤ 1 est trivialement réduit. Il est clair que tout mot sur $X^{\pm}$ est équivalent à un mot réduit : considérer par exemple un mot de longueur minimale dans sa classe d'équivalence. Il est moins évident, mais vrai, que deux mots réduits distincts ne sont pas équivalents.

THÉORÈME 8.7. *L'application canonique $\mathrm{Mots}(X^{\pm}) \to \mathrm{F}_X, m \mapsto [m]$, induit une bijection entre le sous-ensemble des mots réduits sur $X^{\pm}$ et F_X.*

DÉMONSTRATION — La surjectivité a déjà été justifiée. Montrons l'injectivité. Pour tout $x \in X^{\pm}$, et tout mot m sur $X^{\pm}$, on définit $\mathrm{L}_x(m)$ comme suit : si m ne commence pas par x^{-1} on pose $\mathrm{L}_x(m) = xm$, sinon on a $m = x^{-1}n$ pour un unique mot n et on pose $\mathrm{L}_x(m) = n$. Observons que si m est réduit, il en va de même de $\mathrm{L}_x(m)$. De plus, on a $\mathrm{L}_{x^{-1}}(\mathrm{L}_x(m)) = m$ pour tout mot réduit m. En effet, si $m = x^{-1}n$ on a $\mathrm{L}_{x^{-1}}(\mathrm{L}_x(m)) = \mathrm{L}_{x^{-1}}(n) = x^{-1}n = m$ car n ne commence pas par x, et si m ne commence pas par x^{-1} on a $\mathrm{L}_{x^{-1}}(\mathrm{L}_x(m)) = \mathrm{L}_{x^{-1}}(xm) = m$. Ainsi, si $\Omega \subset \mathrm{Mots}(X^{\pm})$ désigne le sous-ensemble des mots réduits, on a défini une application

$$f : X \to \mathrm{S}_\Omega, \ x \mapsto \mathrm{L}_x.$$

Par la propriété universelle du groupe libre, il existe donc un morphisme de groupes $f' : \mathrm{F}_X \to \mathrm{S}_\Omega$ envoyant $[x]$ sur L_x pour tout $x \in X^{\pm}$. Soit $m = x_1 \cdots x_r \in \Omega$.

On a $[m] = [x_1] \cdots [x_r]$ dans F_X, et donc $f'([m]) = \mathrm{L}_{x_1} \circ \cdots \circ \mathrm{L}_{x_r}$. Mézalor on constate

$$f'([m])(\emptyset) = \mathrm{L}_{x_1} \circ \cdots \circ \mathrm{L}_{x_r}(\emptyset) = \mathrm{L}_{x_1} \circ \cdots \circ \mathrm{L}_{x_{r-1}}(x_r) = \cdots = x_1 \cdots x_r = m,$$

car on a $x_i \neq x_{i+1}^{-1}$ pour $1 \leq i < r$. Ainsi, pour $m, m' \in \Omega$ avec $[m] = [m']$, on a $f'([m']) = f'([m])$, et donc $m = f'([m])(\emptyset) = f'([m'])(\emptyset) = m'$. □

En particulier, l'application naturelle $X^{\pm} \to \mathrm{F}_X, x \mapsto [x]$, est injective : on fait très souvent l'abus de langage de noter simplement x la classe $[x]$, ou encore

$$X^{\pm} \subset \mathrm{F}_X.$$

On a clairement $F_X = \{1\}$ pour $X = \emptyset$. Si $X = \{x\}$ est un singleton, les (classes des) mots réduits sur X sont les x^n avec $n \in \mathbb{Z}$, et on a donc un isomorphisme

$$\mathbb{Z} \xrightarrow{\sim} \mathrm{F}_X, \ n \mapsto x^n, \quad \text{si } X = \{x\},$$

d'après le Théorème 8.7. En revanche, pour $|X| \geq 2$, le groupe F_X est non commutatif : pour $a \neq b$ dans X, les (classes des) deux mots réduits ab et ba sont distincts dans F_X toujours par le théorème. Par la propriété universelle du groupe libre, *toute application $X \to Y$ (resp. bijection) induit un morphisme (resp. isomorphisme) de groupes $\mathrm{F}_X \to \mathrm{F}_Y$*. Cela donne sens à la seconde définition suivante.

Définition 8.8. *Un groupe G est dit* libre *s'il est isomorphe à F_X pour un certain X. Pour $n \geq 1$, on note F_n un groupe libre sur un ensemble à n éléments.*

Il est aisé de vérifier à l'aide du Théorème 8.7, que pour $X \subset Y$ le morphisme naturel $\mathrm{F}_X \to \mathrm{F}_Y$ est injectif. En particulier, F_n est isomorphe à un sous-groupe de F_m pour $n \leq m$. De plus, la théorie des *groupes abéliens libres* vue au chapitre suivant permettra de montrer simplement que $\mathrm{F}_n \simeq \mathrm{F}_m$ implique $n = m$. De manière plus intéressante, on peut montrer que pour tout $n \geq 3$, le groupe F_n est isomorphe à un sous-groupe de F_2, que l'on peut même choisir distingué d'indice $n-1$ (Nielsen-Schreier). Par exemple, le sous-groupe $\langle a^2, ab, b^2 \rangle$ du groupe F_2 libre sur $\{a, b\}$ est d'indice 2 (il coïncide avec les classes de mots de longueur paire sur $\{a, b\}^{\pm}$), et il est isomorphe à F_3 (ce n'est pas évident !).

Remarque 8.9. *Nielsen et Schreier ont montré plus généralement que* tout sous-groupe d'un groupe libre est isomorphe à un groupe libre*, et aussi que tout sous-groupe d'indice d de F_n est isomorphe à F_m avec $m = d(n-1)+1$. Pour démontrer ce type de résultats, il est commode d'avoir une approche plus géométrique à la construction de F_X, qui sera abordée en cours de topologie algébrique. Par exemple, le groupe F_2 est isomorphe au groupe fondamental de la figure* ∞.

Terminons cette courte introduction au groupe libre en discutant la notion de groupe défini par générateurs et relations. Soient G un groupe ainsi que $\{g_x\}_{x \in X}$ une famille d'éléments de G indexée par un ensemble X. Par propriété universelle de F_X, il existe un unique morphisme de groupes

$$f : \mathrm{F}_X \to G, \ \text{avec } f(x) = g_x \ \forall x \in X. \tag{10}$$

Définition 8.10. *Dans le contexte de* (10) *ci-dessus, on dit qu'un mot $m \in \mathrm{Mots}(X^{\pm})$ est une* relation *entre les g_x si on a $f([m]) = 1$. Tout mot m' équivalent à une relation m entre les g_x est bien sûr encore une relation entre les g_x, de sorte que l'on dira aussi que $[m] \in \mathrm{F}_X$ est une relation entre les g_x.*

L'ensemble de toutes les relations entre les g_x est donc simplement $\ker f \subset \mathrm{F}_X$. Comme les $x \in X$ engendrent F_X, le morphisme est surjectif si, et seulement si, les g_x engendrent G, auquel cas on a alors bien sûr $\mathrm{F}_X/\ker f \simeq G$.

EXEMPLE 8.11. Dans tout groupe commutatif G, le mot $aba^{-1}b^{-1}$ est une relation entre a et $b \in G$. Dans tout groupe G d'ordre n, et $g \in G$, le mot g^n est une relation satisfaite par g (Lagrange), ainsi que les mot g^{-n}, g^{2n} etc... Dans le groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, les mots a^2, b^4 et $aba^{-1}b^{-1}$ sont des relations entre $a = (1,0)$ et $b = (0,1)$. Nous verrons plus d'exemples quand nous aurons vu plus de groupes !

En pratique, on s'intéresse à trouver des générateurs du sous-groupe $\ker f$ des relations entre les g_x. Une construction utile à ce sujet est la suivante. Observons d'abord que pour toute partie X d'un groupe G, il existe un plus petit sous-groupe *distingué* de G contenant X, à savoir le sous-groupe engendré par $\cup_{g\in G} gXg^{-1}$. Nous le noterons $\langle X\rangle^{\triangleleft}$.

DÉFINITION 8.12. *Soient $\mathscr{G}$ un ensemble et $\mathscr{R} \subset \mathrm{Mots}(\mathscr{G}^{\pm})$ un sous-ensemble. Le groupe quotient $\mathrm{F}_{\mathscr{G}}/\langle\mathscr{R}\rangle^{\triangleleft}$ est appelé* groupe défini par les générateurs $\mathscr{G}$ et par les relations $\mathscr{R}$ *; on le note aussi $\langle \mathscr{G} \mid r = 1,\ \forall r \in \mathscr{R}\rangle$.*

Lorsque $\mathscr{G}$ et $\mathscr{R}$ sont finis, disons $\mathscr{G} = \{g_1, \dots, g_n\}$ (tous distincts) et $\mathscr{R} = \{r_1, \dots, r_s\}$, on le note aussi $\langle g_1, \dots, g_n \mid r_1 = r_2 = \cdots = r_s = 1\rangle$. La propriété universelle d'un groupe défini par générateurs et relations est alors la suivante.

PROPOSITION 8.13. *Soient $\mathscr{G}$ un ensemble, $\mathscr{R} \subset \mathrm{Mots}(\mathscr{G}^{\pm})$ et G un groupe. Il est équivalent de se donner un morphisme de groupes $\langle \mathscr{G} \mid r = 1,\ \forall r \in \mathscr{R}\rangle \to G$ et une application $f : \mathscr{G} \to G$ telle que $f(r) = 1$ pour tout $r \in \mathscr{R}$.*

DÉMONSTRATION — On applique simplement la propriété universelle du groupe quotient (Proposition 6.16), puis celle du groupe libre (Proposition 8.5). □

EXEMPLE 8.14. *Pour tout entier $n \geq 1$ on a des isomorphismes*

$$\langle a \mid a^n = 1\rangle \simeq \mu_n \quad \text{et} \quad \langle a, b \mid aba^{-1}b^{-1} = 1\rangle \simeq \mathbb{Z} \times \mathbb{Z}.$$

DÉMONSTRATION — Soit $G_1 = \langle a \mid a^n = 1\rangle$. Par la propriété universelle, il existe un unique morphisme de groupes $f : G_1 \to \mu_n$ envoyant a sur $\zeta := e^{2i\pi/n}$, car on a $\zeta^n = 1$. Ce morphisme est surjectif car ζ engendre μ_n. Mais comme (la classe de) a engendre G_1, avec $a^n = 1$, tout élément de G_1 est de la forme a^m avec $0 \leq m < n$, puis $|G_1| \leq n$, et f est bijectif pour des raisons de cardinal.

Soit $G_2 = \langle a, b \mid aba^{-1}b^{-1} = 1\rangle$. Par la propriété universelle, il existe un unique morphisme de groupes $f : G_2 \to \mathbb{Z} \times \mathbb{Z}$ envoyant a sur $(1,0)$ et b sur $(0,1)$, car $(1,0)$ et $(0,1)$ commutent dans le groupe (abélien) $\mathbb{Z} \times \mathbb{Z}$. Mais comme (les classes de) a et b engendrent G_2, et que l'on a $ab = ba$ par construction, tout élément x de G_2 s'écrit $a^m b^n$ avec $m, n \in \mathbb{Z}$. Mézalor on constate $f(x) = f(a)^m f(b)^n = (m,n) \in \mathbb{Z}^2$, de sorte que l'écriture $x = a^m b^n$ est unique, et f est bijective. □

EXEMPLE 8.15. *On a $\langle i,\ j,\ \epsilon \mid i^2 = \epsilon,\ j^2 = \epsilon,\ \epsilon^2 = 1,\ ij = \epsilon ji\} \simeq \mathrm{H}_8$.*

Démonstration — Soit G le groupe de gauche défini par générateurs et relations. Comme on a $I^2 = J^2 = -1$ et $IJ = -JI$ dans H_8, la propriété universelle de G montre qu'il existe un unique morphisme de groupes $f : G \to \mathrm{H}_8$ vérifiant $f(i) = I$, $f(j) = J$ et $f(\epsilon) = -1$. Ce morphisme est surjectif car I et J engendrent H_8. Pour voir qu'il est injectif, il suffit donc de voir $|G| \leq 8$.

Par définition, G est engendré par i, j et ϵ, avec $i^2 = j^2 = \epsilon$, $\epsilon^2 = 1$ et $ji = \epsilon ij$. Ces relations montrent que tout élément de G est de la forme $i^a\, j^b\, \epsilon^c$ avec $0 \leq a, b, c \leq 1$. On a donc bien $|G| \leq 2^3 = 8$, et au final, un isomorphisme $f : G \simeq \mathrm{H}_8$. □

Remarque 8.16. *Étant donné un groupe G, un isomorphisme*

$$\langle \mathscr{G} \mid r = 1,\ \forall r \in \mathscr{R} \rangle \xrightarrow{\sim} G$$

s'appelle une présentation *de G (par les générateurs $\mathscr{G}$ et les relations $\mathscr{R}$).*