GROUPES LIBRES ET PRÉSENTATIONS DE GROUPES

Nous verrons ici comment *présenter* un groupe en termes de *générateurs* et *relations*. Le but est de préciser le groupe de manière en même temps minimaliste et parlante.

Etant donné un groupe G, nous cherchons d'abord une liste d'éléments de G telle que l'ensemble de tous les produits possibles d'éléments de la liste est égal à G. On appelle une telle liste un *ensemble de générateurs* de G. Il est toujours possible de prendre comme ensemble de générateurs tout le groupe G, bien que ce ne soit en général de loin pas la meilleure solution.

Ensuite il faut trouver les égalités qui sont satisfaites par ces produits et éliminer celles qui sont superflues car conséquences de combinaisons d'autres égalités. Ces égalités forment un *ensemble de relations* de G, par rapport aux générateurs choisis.

Nous terminerons ce chapitre par une discussion d'une méthode de construction d'une nouvelle présentation de groupe à partir de deux morphismes de présentation.

A. Groupes libres

Les groupes libres forment une classe importante de groupes, car tout groupe est isomorphe à un quotient d'un groupe libre. En fait une présentation d'un groupe G n'est qu'une recette pour quotienter un certain groupe libre afin d'obtenir G.

Bien qu'ils soient d'ordre infini, les groupes libres sont les groupes les plus simples. On peut exprimer cette simplicité en termes d'homomorphismes. Etant donné deux groupes arbitraires, il n'est pas du tout évident de construire un homomorphisme entre eux, ou même de savoir s'il en existe un nontrivial. Par contre, les homomorphismes de source un groupe libre sont particulièrement faciles à définir. Plus précisément, on a la définition suivante.

Définition. Soit $\iota : X \hookrightarrow G$ une injection d'un ensemble quelconque dans un groupe. Le groupe G est dit *libre de base* X si pour toute application ensembliste $f : X \to H$, où H est un groupe, il existe un unique homomorphisme $\hat{f} : G \to H$ tel que $f = \hat{f}\iota$, i.e., tel que le diagramme suivant commute.

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[d, "\iota"'] & H \\ G \arrow[ur, "\hat{f}"'] & \end{tikzcd}$$

L'existence de l'homomorphisme $\hat{f}$, qui est *l'extension unique de* f, est dite la *propriété universelle du groupe libre.*

Remarque. Observer la ressemblance entre cette définition et celle de la base d'un espace vectoriel. Etant donné une application ensembliste d'une base d'un espace vectoriel V dans un autre espace vectoriel W, il existe une unique application linéaire de V dans W qui étend l'application ensembliste.

Comme toujours en mathématiques, il faut se méfier des belles défintions, car nous ne savons pas a priori s'il existe de groupes libres! Nous consacrerons le reste de ce paragraphe à la construction d'un groupe libre de base un ensemble quelconque. Mais d'abord, afin de nous encourager face à la construction un peu technique à venir, nous verrons que cette construction est en fait la seule possible. Tel est le contenu de la proposition suivante.

Propostion 1. *Soient G un groupe libre de base X et H un groupe libre de base Y. Si X et Y ont la même cardinalité, alors G et H sont isomorphes.*

Remarque. Cette démonstration se généralise pour démontrer l'unicité d'objets mathématiques qui satisfont à une propriété universelle de type quelconque. Nous en verrons un autre exemple à la fin de ce chapitre.

Preuve. Puisque X et Y ont la même cardinalité, il existe des bijections $\alpha : X \longrightarrow Y$ et $\beta : Y \longrightarrow X$ avec $\beta\alpha = Id_X$ et $\alpha\beta = Id_Y$. Soient $\iota : X \longrightarrow G$ et $j : Y \longrightarrow H$ les injections de la base dans le groupe libre. La propriété universelle de groupes libre nous garantit alors l'existence d'unique extensions $\widehat{j\alpha} : G \longrightarrow H$ de $j\alpha$ et $\widehat{\iota\beta} : H \longrightarrow G$ de $\iota\beta$. Ainsi, les deux carrés du diagramme suivant commutent,

$$\begin{tikzcd} X \arrow[r, "\iota"] \arrow[d, "\alpha"'] & G \arrow[d, "\widehat{j\alpha}"] \\ Y \arrow[r, "j"] \arrow[d, "\beta"'] & H \arrow[d, "\widehat{\iota\beta}"] \\ X \arrow[r, "\iota"] & G \end{tikzcd}$$

ce qui entraîne que le diagramme

$$\begin{tikzcd} X \arrow[r, "\iota"] \arrow[d, "\beta\alpha"'] & G \arrow[d, "\widehat{\iota\beta}\widehat{j\alpha}"] \\ X \arrow[r, "\iota"] & G \end{tikzcd}$$

commute aussi. Or $\beta\alpha = Id_X$, et le diagramme

$$\begin{tikzcd} X \arrow[r, "\iota"] \arrow[d, "Id_X"'] & G \arrow[d, "Id_G"] \\ X \arrow[r, "\iota"] & G \end{tikzcd}$$

commute. Puisque la propriété universelle de groupes libre nous garantit l'unicité de l'extension de Id_X, on obtient que $\widehat{\iota\beta}\widehat{j\alpha} = Id_G$.

De même on peut montrer que $\widehat{j\alpha}\widehat{\iota\beta} = Id_H$. Les homomorphismes $\widehat{j\alpha}$ et $\widehat{\iota\beta}$ sont donc des isomorphismes. $\square$

Puisqu'il n'existe qu'un groupe libre de base X pour tout ensemble X, il est raisonnable de fixer une notation pour cet unique groupe.

Terminologie. On écrit $\mathcal{F}(X)$ pour le groupe libre de base X.

La construction de $\mathcal{F}(X)$

Grosso modo, on construit $\mathcal{F}(X)$ en prenant tous les produits possibles d'éléments de X et en y ajoutant des inverses (car tout élément d'un groupe doit posséder un inverse). On veut que ce groupe soit aussi libre que possible de contraintes. On n'imposera comme relation entre les différents produits que des conditions sans lesquelles la structure du groupe n'aurait pas de sens.

Pour démarrer, on élargit X, en y ajoutant d'inverses formels aux éléments de X. Autrement dit, on considère l'ensemble

$$\overline{X} = X \cup \{x^{-1} : x \in X\}.$$

L'ensemble $\overline{X}$ s'appelle *l'alphabet* du groupe libre.

Etant donné l'alphabet $\overline{X}$ on fait ce que l'on fait toujours avec un alphabet: on forme des mots dont les lettres sont les éléments de l'alphabet. Dans notre cas, nous n'avons pas à nous inquieter pour savoir si nos mots signifient quelque chose, donc nous les prenons tous. Plus précisément, nous définissons *l'ensemble des mots en* X comme étant

$$\mathcal{M}(X) = \{s_1 s_2 \cdots s_n : s_i \in \overline{X}, n \in \mathbb{N}\} \cup \emptyset,$$

où s_i est une *syllabe* du mot $s_1 s_2 \cdots s_n$ et où $\emptyset$ dénote le mot vide.

Il est possible de définir un produit associatif $*$ sur $\mathcal{M}(X)$ par concatenation. Autrement dit,

$$(s_1 s_2 \cdots s_m) * (s'_1 s'_2 \cdots s'_n) = s_1 s_2 \cdots s_m s'_1 s'_2 \cdots s'_n.$$

Donc

$$(s_1 s_2 \cdots s_m) * \emptyset = s_1 s_2 \cdots s_m = \emptyset * (s_1 s_2 \cdots s_m),$$

i.e., $\emptyset$ est une identité à droite et à gauche par rapport au produit $*$ sur $\mathcal{M}(X)$.

Nous avons déjà fait un bon bout du chemin vers $\mathcal{F}(X)$. La seule chose qui manque est l'existence d'inverses. Dans $\mathcal{M}(X)$, nous n'avons même pas que $x * x^{-1} = \emptyset$; les inverses des éléments de X ne sont que formels.

Pour que chaque élément ait un inverse, il faut prendre des classes d'équivalence, selon une certaine relation d'équivalence. Puisque l'on veut évidemment que les inverses formels des éléments de X deviennent de vrais inverses, il va falloir que xx^{-1} et $x^{-1}x$ soient équivalents au mot vide et donc par extension que les mots $s_1 \cdots s_k x x^{-1} s_{k+1} \cdots s_n$ et $s_1 \cdots s_k x^{-1} x s_{k+1} \cdots s_n$ soient tous les deux équivalents à $s_1 \cdots s_n$. On appellera la suppression ou insertion de xx^{-1} ou de $x^{-1}x$ une *modification élémentaire*. On dira que deux mots w_1 et w_2 dans $\mathcal{M}(X)$ sont *équivalents*, dénoté $w_1 \sim w_2$, si et seulement s'il existe une chaîne finie de modifications élémentaires qui relie w_1 à w_2. Autrement dit, on prend la plus faible relation d'équivalence qui nous permet de dire que xx^{-1} et $x^{-1}x$ soient équivalents au mot vide.

Proposition 2. *Le produit $*$ défini ci-dessus induit une structure de groupe sur* $\mathcal{M}(X)/\sim\, = \{[s_1 \cdots s_n] : s_1 \cdots s_n \in \mathcal{M}(X)\}$.

Preuve. Il est clair que

$$w_1 \sim w_1' \quad \text{et} \quad w_2 \sim w_2' \Rightarrow w_1 * w_2 \sim w_1' * w_2'.$$

Le produit $*$ induit donc un produit $\bullet$ sur $\mathcal{M}(X)/\sim$ défini par

$$[w_1] \bullet [w_2] = [w_1 * w_2].$$

Le nouveau produit $\bullet$ est associatif, puisque $*$ l'était déjà. D'ailleurs, $[\emptyset]$ est une identité par rapport à $\bullet$, puisque $\emptyset$ l'était par rapport à $*$.

Choisir un élément quelconque $[s_1 \cdots s_n]$ de $\mathcal{M}(X)/\sim$. Ecrire

$$s_i^{-1} = \begin{cases} x^{-1} & \text{si} \quad s_i = x \\ x & \text{si} \quad s_i = x^{-1}. \end{cases}$$

Alors il est clair que

$$[s_1 \cdots s_n] \bullet [s_1^{-1} \cdots s_n^{-1}] = [s_1 \cdots s_n * s_1^{-1} \cdots s_n^{-1}] = [\emptyset],$$

i.e., tout élément possède un inverse par rapport au produit $\bullet$. $\square$

Ainsi nous avons bel et bien construit un groupe engendré par un ensemble, d'apparence de la manière la plus simple et libre de contraintes que possible. Reste à voir que ce groupe soit vraiment le groupe libre, i.e., qu'il satifasse à la propriété universelle du groupe libre. Tel est le contenu de la proposition suivante.

Proposition 3. *Soit $\iota : X \longrightarrow \mathcal{M}(X)/\sim$ l'inclusion naturelle, i.e., $\iota(x) = [x]$. Soit G un groupe quelconque et $f : X \longrightarrow G$ une application ensembliste. Alors il exist un unique homomorphisme $\hat{f} : \mathcal{M}(X)/\sim \longrightarrow G$ qui étend f, i.e., $\hat{f}\iota = f$.*

Preuve. On commence par définir une application $\tilde{f} : \mathcal{M}(X) \longrightarrow G$. On montre ensuite que deux éléments d'une même classe déquivalence sont envoyés par $\tilde{f}$ sur le même élément de G et que $\tilde{f}(w_1 * w_2) = \tilde{f}(w_1) \cdot \tilde{f}(w_2)$. D'ailleurs il sera évident que $\tilde{f}$ soit la seule application qui satisfait à ces deux propriétés. Ainsi $\tilde{f}$ induira un homomorphisme $\hat{f} : \mathcal{M}(X)/\sim \longrightarrow G$, qui sera, par l'unicité de $\tilde{f}$, l'unique extension de f possible.

Soit $x_1^{\epsilon_1} \cdots x_n^{\epsilon_n}$ dans $\mathcal{M}(X)$, où ϵ_i est 1 ou -1 pour tout i. Poser

$$\tilde{f}(x_1^{\epsilon_1} \cdots x_n^{\epsilon_n}) = f(x_1)^{\epsilon_1} \cdot \cdots \cdot f(x_n)^{\epsilon_n}.$$

Puisqu'il faut que $\tilde{f}(x) = f(x)$ pour tout x dans X et que $\tilde{f}$ soit multiplicatif (i.e., respecte les produits), on voit qu'il n'y a pas d'autre définition de $\tilde{f}$ possible.

D'ailleurs,

$$\begin{aligned}
\tilde{f}(x_1^{\epsilon_1} \cdots x_i^{\epsilon_i} x x^{-1} x_{i+1}^{\epsilon_{i+1}} \cdots x_n^{\epsilon_n}) &= f(x_1)^{\epsilon_1} \cdots f(x_i)^{\epsilon_i} f(x) f(x)^{-1} f(x_{i+1})^{\epsilon_{i+1}} \cdots f(x_n)^{\epsilon_n} \\
&= f(x_1)^{\epsilon_1} \cdots f(x_i)^{\epsilon_i} f(x_{i+1})^{\epsilon_{i+1}} \cdots f(x_n)^{\epsilon_n} \\
&= f(x_1)^{\epsilon_1} \cdots f(x_i)^{\epsilon_i} f(x)^{-1} f(x) f(x_{i+1})^{\epsilon_{i+1}} \cdots f(x_n)^{\epsilon_n} \\
&= \tilde{f}(x_1^{\epsilon_1} \cdots x_i^{\epsilon_i} x^{-1} x x_{i+1}^{\epsilon_{i+1}} \cdots x_n^{\epsilon_n}).
\end{aligned}$$

Autrement dit, deux mots qui ne diffèrent que par une modification élémentaire sont enovyés sur le même élément de G par $\tilde{f}$, ce qui entraîne que

$$w_1 \sim w_2 \Longrightarrow \tilde{f}(w_1) = \tilde{f}(w_2).$$

Ainsi si l'on pose $\hat{f}([w]) = \tilde{f}(w)$, alors $\hat{f}$ est bien défini. D'ailleurs, l'application $\hat{f}$ est un homomorphisme, car

$$\begin{aligned}\hat{f}([w_1] \bullet [w_2]) = \hat{f}([w_1 * w_2]) = \tilde{f}(w_1 * w_2) \\ = \tilde{f}(w_1) \cdot \tilde{f}(w_2) = \hat{f}([w_1]) \cdot \hat{f}([w_2]).\end{aligned}$$

Pour conclure, observer que l'unicité de $\tilde{f}$ entraîne celle de $\hat{f}$. □

Corollaire 4. $\mathcal{F}(X) = \mathcal{M}(X)/\sim$.

Exemples de groupes libres.

(1) $\mathcal{F}(x) = \mathbb{Z}$.
(2) $\mathcal{F}(x, y) = \{$chemins dans le treillis $\mathbb{Z} \times \mathbb{Z}\}$, où l'on interprète la multiplication de deux éléments comme étant la concatenation des chemins correspondants.

B. Présentations de groupe

Nous cherchons à trouver un moyen efficace de décrire la structure d'un groupe. Une façon de préciser la structure d'un goupe consiste à donner son tableau de multiplication, mais ceci est souvent loin d'être efficace.

Exemple. Pour préciser la structure de $\mathbb{Z}_4$, il faut soit écrire un tableau de multiplication à 16 éléments, soit dire qu'il s'agit d'un groupe à un seul générateur, dont la quatrième puissance est égale à l'identité.

Nous aimerions décrire un groupe en précisant le nombre de générateurs qu'il faut, puis en spécifiant des relations entre ces générateurs. Plus précisément, notre but est le suivant.

But. Etant donné un groupe G, écrire le comme un quotient d'un groupe libre $\mathcal{F}(X)$ par un sousgroupe normal Q. Les éléments de X sont les générateurs du groupe, tandis que Q est déterminé par les relations entre les générateurs.

La motivation de la défintion suivante doit donc être claire.

Définition. Une *présentation de groupe*, dénotée $(\mathbf{x} : \mathbf{r})$, consiste en un ensemble $\mathbf{x}$ et un sousensemble $\mathbf{r} \subseteq \mathcal{F}(\mathbf{x})$. Les éléments de $\mathbf{x}$ sont les *générateurs* de la présentation, et les éléments de $\mathbf{r}$ sont les *relateurs*.

La *conséquence* de $\mathbf{r}$, dénotée $Q(\mathbf{r})$, est le plus petit sousgroupe normal de $\mathcal{F}(\mathbf{x})$ qui contient $\mathbf{r}$. Autrement dit,

$$Q(\mathbf{r}) = \bigcap_{\mathbf{r} \subseteq N \triangleleft \mathcal{F}(\mathbf{x})} N.$$

Le *groupe défini par la présentation* $(\mathbf{x} : \mathbf{r})$, dénoté $|\mathbf{x} : \mathbf{r}|$, est le quotient du groupe libre $\mathcal{F}(\mathbf{x})$ par la conséquence $Q(\mathbf{r})$ de $\mathbf{r}$. Nous écrirons $\gamma_{(\mathbf{x}:\mathbf{r})}$ pour la projection $\mathcal{F}(\mathbf{x}) \to \mathcal{F}(\mathbf{x})/Q(\mathbf{r})$ et $[u]$ pour $\gamma_{(\mathbf{x}:\mathbf{r})}(u)$, pour u quelconque de $\mathcal{F}(\mathbf{x})$.

Il n'est pas facile à l'abord de comprendre pourquoi cette définition traduit de la meilleure manière possible notre but tant que nous l'avons expliqué de manière non-mathématique. Les deux propositions suivantes doivent nous permettre de mieux saisir la nature de $Q(\mathbf{r})$ et ainsi de voir pourquoi cette définition est la bonne.

Cette première proposition nous précise la propriété clé de la conséquence.

Proposition 5. *Soit $u \in \mathcal{F}(\mathbf{x})$. Alors $u \in Q(\mathbf{r})$ ssi pour tout homomorphisme $\varphi : \mathcal{F}(\mathbf{x}) \to H$,*

$$\mathbf{r} \subseteq \ker \varphi \Longrightarrow u \in \ker \varphi.$$

Preuve. $\underline{\Rightarrow}$: Supposons que $u \in Q(\mathbf{r})$ et que $\varphi : \mathcal{F}(\mathbf{x}) \to H$ est un homomorphisme tel que $\mathbf{r} \subseteq \ker \varphi$. Puisque $Q(\mathbf{r})$ est le plus petit sousgroupe normal qui contient $\mathbf{r}$ et $\varphi \lhd \mathcal{F}(\mathbf{x})$, on obtient que $Q(\mathbf{r}) \lhd \ker \varphi$. En particulier, $u \in \ker \varphi$.

$\underline{\Leftarrow}$: Tout sousgroupe normal $N \lhd \mathcal{F}(\mathbf{x})$ détermine un homomorphisme

$$\varphi_N : \mathcal{F}(\mathbf{x}) \to \mathcal{F}(\mathbf{x})/N$$

dont le noyau est N. En particulier on peut considérer $\varphi_{Q(\mathbf{r})}$, qui satisfait à $\mathbf{r} \subseteq \ker \varphi_{Q(\mathbf{r})}$. Par hypothèse on obtient donc que $u \in \ker \varphi_{Q(\mathbf{r})} = Q(\mathbf{r})$. □

La deuxième proposition nous offre une description explicite des éléments de la conséquence.

Proposition 6. *Le sousgroupe normal $Q(\mathbf{r})$ est égal à l'ensemble de tous les produits de conjugés de puissances d'éléments de $\mathbf{r}$. Autrement dit,*

$$Q(\mathbf{r}) = \{\Pi_{j=1}^m u_j r_j^{n_j} u_j^{-1} : r_j \in \mathbf{r}, u_j \in \mathcal{F}(\mathbf{x}), n_j, m \in \mathbb{N}\}.$$

Preuve. Soit N l'ensemble à droite de l'égalité ci-dessus. Nous démontrerons que $Q(\mathbf{r}) \subseteq N$ et que $N \subseteq Q(\mathbf{r})$, obtenant ainsi l'égalité des deux côtés.

Il est clair que N est un sousgroupe normal de $\mathcal{F}(\mathbf{x})$, et qu'il contient $\mathbf{r}$. Ainsi, par définition de la conséquence, $Q(\mathbf{r}) \subseteq N$.

Pour voir que $N \subseteq Q(\mathbf{r})$, choisir un élément quelconque $\Pi_{j=1}^m u_j r_j^{n_j} u_j^{-1}$ de N. Alors

$$\varphi_{Q(\mathbf{r})}(\Pi_{j=1}^m u_j r_j^{n_j} u_j^{-1}) = \Pi_{j=1}^m \varphi_{Q(\mathbf{r})}(u_j) \underbrace{\varphi_{Q(\mathbf{r})}(r_j)}_{=1}{}^{n(j)} \varphi_{Q(\mathbf{r})}(u_j)^{-1} = 1.$$

Ainsi, $N \subseteq \ker \varphi_{Q(\mathbf{r})} = Q(\mathbf{r})$. □

Nous avons vu comment trouver un groupe à partir d'une présentation; il nous reste à voir comment faire le chemin inverse.

Définition. Soit G un groupe quelconque. Une *présentation de G* consiste en une présentation $(\mathbf{x} : \mathbf{r})$ et un isomorphisme $|\mathbf{x} : \mathbf{r}| \xrightarrow{\cong} G$.

Exemples. En abusant un peu de la terminologie (i.e., en ne pas précisant l'isomorphisme, qui est presque évident), on peut dire que

(1) $(\mathbf{x} : \emptyset)$ est une présentation de $\mathcal{F}(\mathbf{x})$;
(2) $(x : x^7)$ est une présentation de $\mathbb{Z}_6$; et
(3) $(a, b : a^2, b^2, aba^{-1}b^{-1})$ est une présentation de $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Remarque. Tout groupe possède au moins une présentation. L'identité $G \xrightarrow{=} G$ (vue comme application ensembliste) s'étend de manière unique en un homomorphisme $p : \mathcal{F}(G) \to G$. Alors, $G \cong \mathcal{F}(G)/\ker p$, i.e., $(G : \ker p)$ est une présentation de G.

Cette présentation n'est pas très intéressant, car elle est toute sauf minimale!

Parlant de présentations minimales, il y a une classe de présentations qui nous intéressera particulièrement pendant ce cours. Il s'agit des présentations dites *finiment présentées*, qui sont définies comme suit.

Définition. Une présentation de groupe $(\mathbf{x} : \mathbf{r})$ (ou le groupe qu'elle définit) est *finiment engendrée* si $\mathbf{x}$ est fini, *finiment relatée* si $\mathbf{r}$ est fini, et *finiment présentée* si $\mathbf{x}$ et $\mathbf{r}$ sont finis.

Il y a une question évidente à se poser lorsque l'on travaille avec des présentations de groupe.

Question. Etant donné deux présentations, définissent-elles des groupes isomorphes?

En général on ne peut pas répondre à cette question. Il existe néanmoins des réponses dans des cas particuliers, ainsi que des théorèmes qui donnent des conditions nécessaires à l'existence d'un isomorphisme. Essayons de comprendre quelles sont ces conditions.

Pour que deux groupes G et H soient isomorphes, il faut d'abord qu'il existe au moins un homomorphisme de G à H. Nous aimerions donc pouvoir exprimer ces homomorphismes au niveau des présentations.

Définition. Un *morphisme de présentations* de source $(\mathbf{x} : \mathbf{r})$ et de but $(\mathbf{y} : \mathbf{s})$ consiste en une application ensembliste $\varphi : \mathbf{x} \to \mathcal{F}(\mathbf{y})$ telle que l'homomorphisme induit $\widehat{\varphi} : \mathcal{F}(\mathbf{x}) \to \mathcal{F}(\mathbf{y})$ satisfait à $\widehat{\varphi}(\mathbf{r}) \subseteq Q(\mathbf{s})$. On écrit $\varphi : (\mathbf{x} : \mathbf{r}) \to (\mathbf{y} : \mathbf{s})$, et on dit que φ est *l'application ensembliste sousjacente* au morphisme de présentation.

Un morphisme de présentations $\varphi : (\mathbf{x} : \mathbf{r}) \to (\mathbf{y} : \mathbf{s})$ induit un unique homomorphisme $\varphi_* : |\mathbf{x} : \mathbf{r}| \to |\mathbf{y} : \mathbf{s}|$, puisque $\mathbf{r} \subseteq \ker(\gamma_{(\mathbf{y}:\mathbf{s})}\widehat{\varphi})$ et donc $Q(\mathbf{r}) \subseteq \ker(\gamma_{(\mathbf{y}:\mathbf{s})}\widehat{\varphi})$. Plus précisément, on définit

$$\varphi_*([u]) = \varphi_*\big(\gamma_{(\mathbf{x}:\mathbf{r})}(u)\big) = \gamma_{(\mathbf{y}:\mathbf{s})}\big(\widehat{\varphi}(u)\big) = [\widehat{\varphi}(u)].$$

Remarque. Etant donné deux morphismes de présentation $\varphi : (\mathbf{x} : \mathbf{r}) \to (\mathbf{y} : \mathbf{s})$ et $\psi : (\mathbf{y} : \mathbf{s}) \to (\mathbf{z} : \mathbf{t})$, on peut définit leur composé $\psi\varphi$ comme étant le morphisme de présentations dont l'application ensembliste sousjacente est $\widehat{\psi}\varphi : \mathbf{x} \to \mathcal{F}(\mathbf{z})$. Il est clair que l'homomorphisme induit sur $\mathcal{F}(\mathbf{x})$ par cette application est $\widehat{\psi}\widehat{\varphi}$, ce qui garantit qu'il s'agit bien d'un morphisme de présentations, car

$$\widehat{\psi}\widehat{\varphi}(\mathbf{r}) \subseteq \widehat{\psi}(Q(\mathbf{s})) \subseteq Q(\mathbf{t}).$$

L'homomorphisme induit sur les groupes présentés est donc $\psi_*\varphi_*$.

Nous avons vu qu'un morphisme de présentations induit un homomorphisme sur les groupes présentés. Qu'en est-il du contraire?

PROPOSITION 7. *Pour tout homomorphisme* $f : |\mathbf{x} : \mathbf{r}| \to |\mathbf{y} : \mathbf{s}|$ *il existe un morphisme de présentations* $\varphi : (\mathbf{x} : \mathbf{r}) \to (\mathbf{y} : \mathbf{s})$ *tel que* $\varphi_* = f$.

PREUVE. Pour tout x dans $\mathbf{x}$, il existe v dans $\mathcal{F}(\mathbf{y})$ tel que $\gamma_{(\mathbf{y}:\mathbf{s})}(v) = f\gamma_{(\mathbf{x}:\mathbf{r})}(x)$, car $\gamma_{(\mathbf{y}:\mathbf{s})}$ est surjectif. Poser $\varphi(x) = v$.

Il faut vérifier que φ ainsi défini soit un morphisme de présentations et que $\varphi_* = f$. Or si $r \in \mathbf{r}$, alors

$$\gamma_{(\mathbf{y}:\mathbf{s})}\widehat{\varphi}(r) = f\gamma_{(\mathbf{x}:\mathbf{r})}(r) = 1.$$

Autrement dit, $\widehat{\varphi}(r) \in \ker \gamma_{(\mathbf{y}:\mathbf{s})} = Q(\mathbf{s})$. Ainsi, φ est bien un morphisme de présentations.

Pour terminer, souvenons-nous que φ_* est l'unique homomorphisme tel que $\varphi_*\gamma_{(\mathbf{x}:\mathbf{r})} = \gamma_{(\mathbf{y}:\mathbf{s})}\widehat{\varphi}$. Or $f\gamma_{(\mathbf{x}:\mathbf{r})} = \gamma_{(\mathbf{y}:\mathbf{s})}\widehat{\varphi}$ aussi. Ainsi, $\varphi_* = f$. $\square$

Ayant déterminé comment exprimer des homomorphismes de groupe au niveau des présentations, considérons le cas particulier des isomorphismes.

DÉFINITION. Deux présentations sont du *même type* ssi il existe deux morphismes de présentation $\varphi : (\mathbf{x} : \mathbf{r}) \to (\mathbf{y} : \mathbf{s})$ et $\psi : (\mathbf{y} : \mathbf{s}) \to (\mathbf{x} : \mathbf{r})$ tels que $\psi_*\varphi_* = I_{|\mathbf{x}:\mathbf{r}|}$ et $\varphi_*\psi_* = I_{|\mathbf{y}:\mathbf{s}|}$. On dit alors que φ est une *équivalence de présentation* et que ψ est son *équivalence inverse*.

REMARQUE. Il est facile de vérifier que la composition de deux équivalences de présentation est aussi une équivalence de présentation.

Voici la preuve qu'il faut bien étudier des équivalences de présentation pour comprendre des isomorphismes de groupe.

PROPOSITION 8. *Deux présentations sont du même type ssi les groupes qu'elles définissent sont isomorphes.*

PREUVE. $\underline{\Rightarrow}$: Soient $\varphi : (\mathbf{x} : \mathbf{r}) \to (\mathbf{y} : \mathbf{s})$ et $\psi : (\mathbf{y} : \mathbf{s}) \to (\mathbf{x} : \mathbf{r})$ des équivalences de présentation. Alors $\psi_*\varphi_* = I_{|\mathbf{x}:\mathbf{r}|}$ et $\varphi_*\psi_* = I_{|\mathbf{y}:\mathbf{s}|}$, i.e., φ_* et ψ_* sont des isomorphismes.

$\underline{\Leftarrow}$: Soit $f : |\mathbf{x} : \mathbf{r}| \to |\mathbf{y} : \mathbf{s}|$ un isomorphisme. Soient φ et ψ des morphismes de présentations tels que $\varphi_* = f$ et $\psi_* = f^{-1}$. Alors $\psi_*\varphi_* = I_{|\mathbf{x}:\mathbf{r}|}$ et $\varphi_*\psi_* = I_{|\mathbf{y}:\mathbf{s}|}$, et donc φ et ψ sont des équivalences. $\square$

On va maintenant spécialiser et ne considérer que certaines équivalences relativement simples et faciles à décrire. Il s'avéra en fait que *toute* équivalence de présentation peut s'écrire comme le composé de telles équivalences simples.

Soit $(\mathbf{x} : \mathbf{r})$ une présentation de groupe. Soit $s \in Q(\mathbf{r})$, et poser $\mathbf{s} = \mathbf{r} \cup \{s\}$. Il est facile de vérifier que $Q(\mathbf{r}) = Q(\mathbf{s})$, ce qui entraîne que $|\mathbf{x} : \mathbf{r}| = |\mathbf{x} : \mathbf{s}|$. Ainsi, l'inclusion $\iota : \mathbf{x} \hookrightarrow \mathcal{F}(\mathbf{x})$ est l'application ensembliste sousjacente à deux équivalences de présentation

$$\varphi_I : (\mathbf{x} : \mathbf{r}) \to (\mathbf{x} : \mathbf{s}),$$

appelée une *équivalence de type Ia*, et

$$\varphi'_I : (\mathbf{x} : \mathbf{s}) \to (\mathbf{x} : \mathbf{r}),$$

appelée une *équivalence de type Ib.* Une équivalence de type Ia ne fait que d'ajouter un relateur superflu, tandis qu'une équivalence de type Ib ne fait que d'enlever un relateur superflu.

Il y a un autre type d'équivalence simple qu'il nous faut considérer. Soit $(\mathbf{x}:\mathbf{r})$ une présentation de groupe. Choisir un élément $v \in \mathcal{F}(\mathbf{x})$. Définir une nouvelle présentation $(\mathbf{y}:\mathbf{s})$, où

$$\mathbf{y} = \mathbf{x} \cup \{y\},$$

i.e., on ajoute un nouveau générateur à $\mathbf{x}$, et

$$\mathbf{s} = \mathbf{r} \cup \{yv^{-1}\},$$

i.e., on impose que $[y] = [v]$ dans le groupe présenté.

Considérer l'inclusion $\varphi_{\mathrm{II}} : \mathbf{x} \longrightarrow \mathcal{F}(\mathbf{y})$ et l'application ensembliste $\varphi'_{\mathrm{II}} : \mathbf{y} \longrightarrow \mathcal{F}(\mathbf{x})$ définie par $\varphi'_{\mathrm{II}}(x) = x$ pour tout x dans $\mathbf{x}$ et $\varphi'_{\mathrm{II}}(y) = v$. Alors

$$\varphi_{\mathrm{II}}(\mathbf{r}) = \mathbf{r} \subset \mathbf{s} \subset Q(\mathbf{s})$$

et

$$\varphi'_{\mathrm{II}}(\mathbf{s}) = \mathbf{r} \cup \{\underbrace{\varphi'_{\mathrm{II}}(yv^{-1})}_{=vv^{-1}=1}\} = \mathbf{r} \subseteq Q(\mathbf{r}),$$

ce qui entraîne que φ_{II} et φ'_{II} sont les applications ensemblistes sousjacentes à deux morphismes de présentation, auxquels nous donnons les mêmes noms.

Lemme 9. *$\varphi_{\mathrm{II}} : (\mathbf{x}:\mathbf{r}) \to (\mathbf{y}:\mathbf{s})$ et $\varphi'_{\mathrm{II}} : (\mathbf{y}:\mathbf{s}) \to (\mathbf{x}:\mathbf{r})$ sont des équivalences de présentation.*

Preuve. Observer d'abord que $\widehat{\varphi}'_{\mathrm{II}}\varphi_{\mathrm{II}} : \mathbf{x} \longrightarrow \mathcal{F}(\mathbf{x})$ induit l'identité sur $\mathcal{F}(\mathbf{x})$. Alors on a forcément que $\varphi'_{\mathrm{II}*}\varphi_{\mathrm{II}*} = I_{|\mathbf{x}:\mathbf{r}|}$.

Deuxièmement, nous calculons

$$\widehat{\varphi}_{\mathrm{II}}\varphi'_{\mathrm{II}}(x) = x \quad \forall x \in \mathbf{x}$$

et

$$\widehat{\varphi}_{\mathrm{II}}\varphi'_{\mathrm{II}}(y) = v.$$

Ainsi,

$$\varphi_{\mathrm{II}*}\varphi'_{\mathrm{II}*}\big(\gamma_{(\mathbf{y}:\mathbf{s})}(x)\big) = \gamma_{(\mathbf{y}:\mathbf{s})}(x) \quad \forall x \in \mathbf{x}$$

et

$$\varphi_{\mathrm{II}*}\varphi'_{\mathrm{II}*}\big(\gamma_{(\mathbf{y}:\mathbf{s})}(y)\big) = \gamma_{(\mathbf{y}:\mathbf{s})}\widehat{\varphi}_{\mathrm{II}}\varphi'_{\mathrm{II}}(y) = \gamma_{(\mathbf{y}:\mathbf{s})}(v) = \gamma_{(\mathbf{y}:\mathbf{s})}(y),$$

où la dernière égalité est due au fait que $yv^{-1} \in \mathbf{s} \subseteq Q(\mathbf{s})$.

L'unicité de $\varphi_{\mathrm{II}*}\varphi'_{\mathrm{II}*}$ entraîne ensuite que $\varphi_{\mathrm{II}*}\varphi'_{\mathrm{II}*} = I_{|\mathbf{y}:\mathbf{s}|}$. □

Définition. Les équivalences φ_{II} et φ'_{II} s'appellent des *équivalences de type IIa et de type IIb*, respectivement

Nous allons démontrer par la suite que toute équivalence n'est qu'une composition d'équivalences de types Ia, Ib, IIa, et IIb. Mais avant de pouvoir le faire, il nous faut prouver le lemme suivant.

LEMME 10. *Soient* $\mathbf{x}$ *et* $\mathbf{y}$ *deux ensembles disjoints, et* $\mathbf{r} \subseteq \mathcal{F}(\mathbf{x})$. *Soit* $\theta : \mathcal{F}(\mathbf{x} \cup \mathbf{y}) \longrightarrow \mathcal{F}(\mathbf{x})$ *un homomorphisme tel que* $\theta(x) = x$ *pour tout* x *dans* $\mathbf{x}$. *Alors*

$$\ker \gamma_{(\mathbf{x}:\mathbf{r})}\theta = Q(\mathbf{r} \cup \{y\theta(y)^{-1} : y \in \mathbf{y}\}).$$

PREUVE. Afin de vérifier l'égalité, nous démontrerons les deux inclusions. Mais d'abord

(1) nous posons $\mathbf{s} = \mathbf{r} \cup \{y\theta(y)^{-1} : y \in \mathbf{y}\}$, pour simplifier la notation; et
(2) nous observons que $\theta^2(u) = \theta(u)$ pour tout u dans $\mathcal{F}(\mathbf{x}\cup\mathbf{y})$ car $\theta(u) \in \mathcal{F}(\mathbf{x})$ et la restriction de θ à $\mathcal{F}(\mathbf{x})$ est l'identité.

$\underline{\ker \gamma_{(\mathbf{x}:\mathbf{r})}\theta \subseteq Q(\mathbf{s})}$: Considérer l'homomorphisme quotient

$$\gamma_{|\mathbf{x}\cup\mathbf{y}:\mathbf{s}|} : \mathcal{F}(\mathbf{x} \cup \mathbf{y}) \longrightarrow \mathcal{F}(\mathbf{x} \cup \mathbf{y})/Q(\mathbf{s}).$$

Soit γ' la restriction de $\gamma_{|\mathbf{x}\cup\mathbf{y}:\mathbf{s}|}$ à $\mathcal{F}(\mathbf{x})$. Alors $\gamma'\theta = \gamma_{|\mathbf{x}\cup\mathbf{y}:\mathbf{s}|}$, car

$$\gamma'\theta(x) = \gamma'(x) = \gamma_{|\mathbf{x}\cup\mathbf{y}:\mathbf{s}|}(x) \quad \forall x \in \mathbf{x}$$

et

$$\begin{aligned}
\gamma'\theta(y) &= \gamma_{|\mathbf{x}\cup\mathbf{y}:\mathbf{s}|}\theta(y) && \text{car } \theta(y) \in \mathcal{F}(\mathbf{x}) \\
&= \gamma_{|\mathbf{x}\cup\mathbf{y}:\mathbf{s}|}(y\theta(y)^{-1})\gamma_{|\mathbf{x}\cup\mathbf{y}:\mathbf{s}|}\theta(y) && \text{car } y\theta(y)^{-1} \in Q(\mathbf{s}) = \ker \gamma_{|\mathbf{x}\cup\mathbf{y}:\mathbf{s}|} \\
&= \gamma_{|\mathbf{x}\cup\mathbf{y}:\mathbf{s}|}(y) && \text{pour tout } y \text{ dans } \mathbf{y}.
\end{aligned}$$

Choisir $u \in \ker \gamma_{|\mathbf{x}:\mathbf{r}|}\theta$. Alors

$$\gamma_{|\mathbf{x}\cup\mathbf{y}:\mathbf{s}|}(u\theta(u)^{-1}) = \gamma'\theta(u\theta(u)^{-1}) = \gamma'\theta(u)\gamma'\theta(u)^{-1} = 1.$$

Ainsi $u\theta(u)^{-1} \in Q(\mathbf{s})$ pour tout $u \in \ker \gamma_{|\mathbf{x}:\mathbf{r}|}\theta$. Or nous avons aussi que

$$u \in \ker \gamma_{|\mathbf{x}:\mathbf{r}|}\theta \Longleftrightarrow \theta(u) \in \ker \gamma_{|\mathbf{x}:\mathbf{r}|} = Q(\mathbf{r}) \subseteq Q(\mathbf{s}),$$

ce qui implique que

$$u = \big(u\theta(u)^{-1}\big)\theta(u) \in Q(\mathbf{s}).$$

Autrement dit, $\ker \gamma_{(\mathbf{x}:\mathbf{r})}\theta \subseteq Q(\mathbf{s})$.

$\underline{Q(\mathbf{s}) \subseteq \ker \gamma_{(\mathbf{x}:\mathbf{r})}\theta}$: Si $r \in \mathbf{r}$, alors $\gamma_{(\mathbf{x}:\mathbf{r})}\theta(r) = \gamma_{(\mathbf{x}:\mathbf{r})}(r) = 1$. Ainsi, $\mathbf{r} \subseteq \ker \gamma_{(\mathbf{x}:\mathbf{r})}\theta$.
D'ailleurs, pour tout $y \in \mathbf{y}$,

$$\gamma_{(\mathbf{x}:\mathbf{r})}\theta(y\theta(y)^{-1}) = \gamma_{(\mathbf{x}:\mathbf{r})}\theta(y)\gamma_{(\mathbf{x}:\mathbf{r})}\theta(y)^{-1} = 1,$$

i.e., $\{y\theta(y)^{-1} : y \in \mathbf{y}\} \subseteq \ker \gamma_{(\mathbf{x}:\mathbf{r})}\theta$. Donc on a que $\mathbf{s} \subseteq \ker \gamma_{(\mathbf{x}:\mathbf{r})}\theta$, ce qui entraîne que $Q(\mathbf{s}) \subseteq \ker \gamma_{(\mathbf{x}:\mathbf{r})}\theta$. $\square$

Nous sommes prêts maintenant à démontrer la décomposabilité des équivalences.

Théorème 11(Le théorème de Tietze). *Soient* $(\mathbf{x} : \mathbf{r})$ *et* $(\mathbf{y} : \mathbf{s})$ *deux présentations finiment présentées. Soient* $\varphi : (\mathbf{x} : \mathbf{r}) \to (\mathbf{y} : \mathbf{s})$ *et* $\psi : (\mathbf{y} : \mathbf{s}) \to (\mathbf{x} : \mathbf{r})$ *des équivalences inverses de présentation. Alors il existe une suite finie de couples d'équivalences inverses de type Ia et Ib, ou IIa et IIb,*

$$\mu_1, \mu_1'; ...; \mu_l, \mu_l'$$

telle que

$$\varphi = \mu_1 \cdots \mu_l \quad \textit{et} \quad \psi = \mu_l' \cdots \mu_1'.$$

Preuve. On résoud d'abord le cas spécial où $\mathbf{x} \cap \mathbf{y} = \emptyset$. L'idée de la preuve est de "grimper" de $(\mathbf{x} : \mathbf{r})$ jusqu'à $(\mathbf{x} \cup \mathbf{y} : \mathbf{r} \cup \{?\})$ et de $(\mathbf{y} : \mathbf{s})$ jusqu'à $(\mathbf{x} \cup \mathbf{y} : \mathbf{s} \cup \{??\})$ par des équivalences de type IIa et IIb, où $Q(\mathbf{r} \cup \{?\}) = Q(\mathbf{s} \cup \{??\})$. Le composé des premiers avec les inverses des derniers donnera (presque) l'équivalence voulue.

Définir d'abord $\rho : \mathcal{F}(\mathbf{x} \cup \mathbf{y}) \to \mathcal{F}(\mathbf{x})$ par $\rho(x) = x$ pour tout $x \in \mathbf{x}$ et $\rho(y) = \psi(y)$ pour tout $y \in \mathbf{y}$, et $\sigma : \mathcal{F}(\mathbf{x} \cup \mathbf{y}) \to \mathcal{F}(\mathbf{y})$ par $\sigma(x) = \varphi(x)$ pour tout $x \in \mathbf{x}$ et $\sigma(y) = y$ pour tout $y \in \mathbf{y}$.

Observer que

$$\gamma_{(\mathbf{x}:\mathbf{r})}\psi\sigma(x) = \gamma_{(\mathbf{x}:\mathbf{r})}\psi\varphi(x) = \psi_*\varphi_*([x]) = [x] = \gamma_{(\mathbf{x}:\mathbf{r})}\rho(x)$$

pour tout x dans $\mathbf{x}$. De plus il est immédiat que $\gamma_{(\mathbf{x}:\mathbf{r})}\psi\sigma(y) = \gamma_{(\mathbf{x}:\mathbf{r})}\rho(y)$ pour tout y dans $\mathbf{y}$.

Ecrire $\mathbf{x} = \{x_1, ..., x_m\}$ et $\mathbf{y} = \{y_1, ..., y_n\}$. Considérer les suites suivantes d'équivalences de type IIa et IIb.

$$(\mathbf{x} : \mathbf{r}) \underset{\tau_1'}{\overset{\tau_1}{\rightleftarrows}} (\mathbf{x} \cup \{y_1\} : \mathbf{r} \cup \{y_1\rho(y_1)^{-1}\}) \underset{\tau_2'}{\overset{\tau_2}{\rightleftarrows}} \cdots \underset{\tau_n'}{\overset{\tau_n}{\rightleftarrows}} (\mathbf{x} \cup \mathbf{y} : \mathbf{r} \cup \{y_i\rho(y_i)^{-1} : 1 \le i \le n\})$$

et

$$(\mathbf{y} : \mathbf{s}) \underset{\nu_1'}{\overset{\nu_1}{\rightleftarrows}} (\mathbf{y} \cup \{x_1\} : \mathbf{s} \cup \{x_1\sigma(x_1)^{-1}\}) \underset{\nu_2'}{\overset{\nu_2}{\rightleftarrows}} \cdots \underset{\nu_m'}{\overset{\nu_m}{\rightleftarrows}} (\mathbf{y} \cup \mathbf{x} : \mathbf{s} \cup \{x_i\sigma(x_i)^{-1} : 1 \le i \le m\}).$$

Poser $\mathbf{a} = \{y_i\rho(y_i)^{-1} : 1 \le i \le n\}$ et $\mathbf{b} = \{x_i\sigma(x_i)^{-1} : 1 \le i \le m\}$. Le Lemme 2.10 nous dit alors que

$$\ker \gamma_{(\mathbf{x}:\mathbf{r})}\rho = Q(\mathbf{r} \cup \mathbf{a}).$$

D'ailleurs, il est facile de voir que

$$\mathbf{s} \cup \mathbf{b} \subseteq \ker \gamma_{(\mathbf{y}:\mathbf{s})}\sigma \subseteq \ker \psi_*\gamma_{(\mathbf{y}:\mathbf{s})}\sigma = \ker \gamma_{(\mathbf{x}:\mathbf{r})}\psi\sigma = \ker \gamma_{(\mathbf{x}:\mathbf{r})}\rho.$$

Donc, on a que $\mathbf{s} \cup \mathbf{b} \subseteq Q(\mathbf{r} \cup \mathbf{a})$. De même, on peut montrer que $\mathbf{r} \cup \mathbf{a} \subseteq Q(\mathbf{s} \cup \mathbf{b})$.

Ainsi, il y a des équivalences de type Ia et Ib

$$(\mathbf{x} \cup \mathbf{y} : \mathbf{r} \cup \mathbf{a}) \underset{\xi_1'}{\overset{\xi_1}{\rightleftarrows}} (\mathbf{x} \cup \mathbf{y} : \mathbf{r} \cup \mathbf{a} \cup \{s_1\}) \underset{\xi_2'}{\overset{\xi_2}{\rightleftarrows}} \cdots$$

$$\cdots \underset{\xi_q'}{\overset{\xi_q}{\rightleftarrows}} (\mathbf{x} \cup \mathbf{y} : \mathbf{r} \cup \mathbf{a} \cup \mathbf{s}) \underset{\xi_{q+1}'}{\overset{\xi_{q+1}}{\rightleftarrows}} (\mathbf{x} \cup \mathbf{y} : \mathbf{r} \cup \mathbf{a} \cup \mathbf{s} \cup \{x_1\sigma(x_1)^{-1}\}) \underset{\xi_{q+2}'}{\overset{\xi_{q+2}}{\rightleftarrows}} \cdots$$

$$\cdots \underset{\xi_{q+m}'}{\overset{\xi_{q+m}}{\rightleftarrows}} (\mathbf{x} \cup \mathbf{y} : \mathbf{r} \cup \mathbf{a} \cup \mathbf{s} \cup \mathbf{b})$$

et

$$(\mathbf{x}\cup\mathbf{y}:\mathbf{s}\cup\mathbf{b}) \underset{\omega_1'}{\overset{\omega_1}{\rightleftarrows}} (\mathbf{x}\cup\mathbf{y}:\mathbf{s}\cup\mathbf{b}\cup\{r_1\}) \underset{\omega_2'}{\overset{\omega_2}{\rightleftarrows}} \cdots$$
$$\cdots \underset{\omega_p'}{\overset{\omega_p}{\rightleftarrows}} (\mathbf{x}\cup\mathbf{y}:\mathbf{s}\cup\mathbf{b}\cup\mathbf{r}) \underset{\omega_{p+1}'}{\overset{\omega_{p+1}}{\rightleftarrows}} (\mathbf{x}\cup\mathbf{y}:\mathbf{s}\cup\mathbf{b}\cup\mathbf{r}\cup\{y_1\rho(y_1)^{-1}\}) \underset{\omega_{p+2}'}{\overset{\omega_{p+2}}{\rightleftarrows}} \cdots$$
$$\cdots \underset{\omega_{p+n}'}{\overset{\omega_{p+n}}{\rightleftarrows}} (\mathbf{x}\cup\mathbf{y}:\mathbf{s}\cup\mathbf{b}\cup\mathbf{r}\cup\mathbf{a}),$$

où $\mathbf{r}=\{r_1,...,r_p\}$ et $\mathbf{s}=\{s_1,...,s_q\}$.

On peut résumer ce qui précède en disant qu'il existe des équivalences

$$(1)\qquad (\mathbf{x}:\mathbf{r}) \xrightarrow{\xi_{q+m}\cdots\xi_1\tau_n\cdots\tau_1} (\mathbf{x}\cup\mathbf{y}:\mathbf{r}\cup\mathbf{a}\cup\mathbf{s}\cup\mathbf{b}) \xrightarrow{\nu_1'\cdots\nu_m'\omega_1'\cdots\omega_{p+n}'} (\mathbf{y}:\mathbf{s})$$

et

$$(2)\qquad (\mathbf{x}:\mathbf{r}) \xleftarrow{\tau_1'\cdots\tau_n'\xi_1'\cdots\xi_{q+m}'} (\mathbf{x}\cup\mathbf{y}:\mathbf{r}\cup\mathbf{a}\cup\mathbf{s}\cup\mathbf{b}) \xleftarrow{\omega_{p+n}\cdots\omega_1\nu_m\cdots\nu_1} (\mathbf{y}:\mathbf{s}).$$

Il reste à voir que ces équivalences sont bel et bien ègales à φ et ψ, respectivement. Or

$$\tau_i(x_j)=x_j \quad \forall 1\le j\le m \quad \text{et} \quad \tau_i(y_j)=y_j \quad \forall 1\le j<i,$$
$$\xi_i(x_j)=\omega_i'(x_j)=x_j \quad \forall 1\le j\le m \quad \text{et} \quad \xi_i(y_j)=\omega_i'(y_j)=y_j \quad \forall 1\le j\le n,$$

et

$$\nu_i'(x_j)=\begin{cases} x_j & \forall 1\le j<i \\ \sigma(x_j)=f(x_j) & \text{si } j=i, \end{cases} \quad \text{et} \quad \nu_i'(y_j)=y_j \quad \forall 1\le j\le n.$$

Ainsi, l'équivalence (1) est égale à φ. De même, l'équivalence (2) est égale à ψ.

Considérer maintenant le cas où $\mathbf{x}\cap\mathbf{y}\neq\emptyset$. Soit $\mathbf{z}$ un ensemble de cardinalité m tel que $\mathbf{x}\cap\mathbf{z}=\emptyset=\mathbf{y}\cap\mathbf{z}$.

Ecrire $\mathbf{z}=\{z_1,...,z_m\}$, et définir $\lambda_1:\mathbf{x}\to\mathcal{F}(\mathbf{z})$ par $\lambda_1(x_i)=z_i$ et $\lambda_2:\mathbf{z}\to\mathcal{F}(\mathbf{x})$ par $\lambda_2(z_i)=x_i$. Les applications ensemblistes λ_1 et λ_2 induisent des isomorphismes $\widehat{\lambda}_1:\mathcal{F}(\mathbf{x})\to\mathcal{F}(\mathbf{z})$ et $\widehat{\lambda}_2:\mathcal{F}(\mathbf{z})\to\mathcal{F}(\mathbf{x})$. On a donc le diagramme suivant d'équivalences de présentation.

$$(\mathbf{x}:\mathbf{r}) \underset{\lambda_2}{\overset{\lambda_1}{\rightleftarrows}} (\mathbf{z}:\widehat{\lambda}_1(\mathbf{r})) \underset{\lambda_1\psi}{\overset{\varphi\lambda_2}{\rightleftarrows}} (\mathbf{y}:\mathbf{s})$$

On peut donc appliquer les résultats du premier cas aux couples d'équivalences (λ_1,λ_2) et $(\varphi\lambda_2,\lambda_1\psi)$. $\square$

C. Sommes amalgamées de groupes

Comme promis dans l'introduction de ce chapitre, nous verrons maintenant comment constuire une nouvelle présentation de groupe à partir de deux morphismes de présentation donnés. Cette construction ne s'applique qu'à deux morphismes qui ont la même présentation source. Ci-dessous nous énonçons la définition de l'objet recherché.

Définition. Soient $f_1 : G_0 \longrightarrow G_1$ et $f_2 : G_0 \longrightarrow G_2$ deux homomorphismes de groupe. La *somme amalgamée* de f_0 et de f_1 consiste en un groupe G et deux homomorphismes, $g_1 : G_1 \longrightarrow G$ et $g_2 : G_2 \longrightarrow G$ tels que

(1) $g_1 f_1 = g_2 f_2$;
(2) s'il existe des homomorphismes $h_1 : G_1 \longrightarrow H$ et $h_2 : G_2 \longrightarrow H$ tels que $h_1 f_1 = h_2 f_2$, alors il existe exactement un homomorphisme $h : G \longrightarrow H$ tel que $hg_1 = h_1$ et $hg_2 = h_2$.

La proposition suivante doit vous rappeler un résultat de la section A, sur les groupes libres. Il s'agit de nouveau d'une preuve d'unicité dans le cadre d'une propriété universelle.

Proposition 12. *Si la somme amalgamée de deux homomorphismes existe, elle est unique à isomorphisme près.*

Preuve. Supposons que G et G' sont tous les deux des sommes amalgamées de f_1 et f_2, i.e., il existe des homomorphismes $g_1 : G_1 \longrightarrow G$ et $g_2 : G_2 \longrightarrow G$ tels que $g_1 f_1 = g_2 f_2$ et $g_1' : G_1 \longrightarrow G'$ et $g_2' : G_2 \longrightarrow G'$ tels que $g_1' f_1 = g_2' f_2$. Alors par la propriété universelle des sommes amaglamées, il existe des homomorphismes $h : G \longrightarrow G'$ et $h' : G' \longrightarrow G$ tels que

$$hg_1 = g_1', \quad hg_2 = g_2', \quad h'g_1' = g_1, \quad \text{et} \quad h'g_2' = g_2.$$

Ainsi

$$h'hg_1 = g_1, \quad h'hg_2 = g_2, \quad hh'g_1 = g_1, \quad \text{et} \quad hh'g_2 = g_2.$$

Donc par unicité, $h'h = 1_G$ et $hh' = 1_{G'}$, autrement dit G et G' sont isomorphes □

Il nous faut maintenant vérfier que la définition n'est pas vide de sens. Il ne sert à rien de savoir qu'un objet est unique s'il n'existe pas!

Théorème 13. *La somme amalgamée de tout couple d'homomorphismes $f_1 : G_0 \longrightarrow G_1$ et $f_2 : G_0 \longrightarrow G_2$ existe.*

Preuve. Nous allons d'abord considérer le cas spécial où $G_0 = \{e\}$ et ensuite utiliser le résultat obtenu pour démontrer le cas général.

Cas spécial: La somme amalgamée de $\{1\} \hookrightarrow G_1$ et $\{1\} \hookrightarrow G_2$ s'appelle le *produit libre* de G_1 et G_2, que l'on dénote $G_1 * G_2$. Voyons comment prouver que le produit libre de tout couple de groupes existe.

Soit $(\mathbf{x} : \mathbf{r})$ et $(\mathbf{y} : \mathbf{s})$ des présentations de G_1 et G_2, respectivement, où l'on peut supposer sans perte de généralité que $\mathbf{x} \cap \mathbf{y} = \emptyset$. Par abus de notation, nous dirons que $G_1 = |\mathbf{x} : \mathbf{r}|$ et $G_2 = |\mathbf{y} : \mathbf{s}|$.

Considérer les morphismes de présentation $\varphi_1 : (\mathbf{x} : \mathbf{r}) \longrightarrow (\mathbf{x} \cup \mathbf{y} : \mathbf{r} \cup \mathbf{s})$, induit par l'inclusion $\mathbf{x} \hookrightarrow \mathcal{F}(\mathbf{x} \cup \mathbf{y})$, et $\varphi_2 : (\mathbf{y} : \mathbf{s}) \longrightarrow (\mathbf{x} \cup \mathbf{y} : \mathbf{r} \cup \mathbf{s})$, induit par l'inclusion $\mathbf{y} \hookrightarrow \mathcal{F}(\mathbf{x} \cup \mathbf{y})$. Soient $(\varphi_1)_* : G_1 \longrightarrow |\mathbf{x} \cup \mathbf{y} : \mathbf{r} \cup \mathbf{s}|$ et $(\varphi_2)_* : G_2 \longrightarrow |\mathbf{x} \cup \mathbf{y} : \mathbf{r} \cup \mathbf{s}|$ les homomorphismes induits par les morphismes de présentation φ_1 et φ_2.

Soient $h_1 : G_1 \longrightarrow H$ et $h_2 : G_2 \longrightarrow H$ deux autres homomorphismes quelconques. Définir $k : \mathcal{F}(\mathbf{x} \cup \mathbf{y}) \longrightarrow H$ par

$$k(x) = h_1 \gamma_{(\mathbf{x}:\mathbf{r})}(x) \quad \forall x \in \mathbf{x} \quad \text{et} \quad k(y) = h_2 \gamma_{(\mathbf{y}:\mathbf{s})}(y) \quad \forall y \in \mathbf{y}.$$

Il nous reste à montrer que $\mathbf{r} \cup \mathbf{s} \subseteq \ker k$, ce qui entraînera que $Q(\mathbf{r} \cup \mathbf{s}) \subseteq \ker k$. Ainsi, nous obtiendrons que k induit un homomorphisme $h : |\mathbf{x} \cup \mathbf{y} : \mathbf{r} \cup \mathbf{s}| \longrightarrow H$ défini par

$$h([x]) = k(x) = h_1([x]) \quad \forall x \in \mathbf{x} \quad \text{et} \quad h([y]) = k(y) = h_2([y]) \quad \forall y \in \mathbf{y}.$$

Puisque $h([x]) = h(\varphi_1)_*([x])$ pour tout $x \in \mathbf{x}$ et $h([y]) = h(\varphi_2)_*([y])$ pour tout $y \in \mathbf{y}$, nous aurons donc que $h(\varphi_1)_* = h_1$ et $h(\varphi_2)_* = h_2$.

D'ailleurs, si $h' : |\mathbf{x} \cup \mathbf{y} : \mathbf{r} \cup \mathbf{s}| \longrightarrow H$ satsifait à $h'(\varphi_1)_* = h_1$ et $h'(\varphi_2)_* = h_2$, alors forcément $h'([x]) = h_1([x])$ pour tout $x \in \mathbf{x}$ et $h([y]) = h_2([y])$ pour tout $y \in \mathbf{y}$. Autrement dit, $h = h'$, puisque ces homomorphismes sont déterminés par leurs valeurs sur les générateurs. Ainsi, on aura que

$$G_1 * G_2 = |\mathbf{x} \cup \mathbf{y} : \mathbf{r} \cup \mathbf{s}|.$$

Or, pour tout $r \in \mathbf{r}$, nous avons que

$$k(r) = g_1' \gamma_{(\mathbf{x}:\mathbf{r})}(r) = g_1'(1) = 1,$$

donc $\mathbf{r} \subseteq \ker k$. On peut montrer de manière presque identique que $\mathbf{s} \subseteq \ker k$. Ainsi, la démonstration du cas spécial est terminée.

Cas général: Poser $\mathbf{t} = \{(\varphi_1)_* f_1(a)(\varphi_2)_* f_2(a)^{-1} : a \in G_0\} \subset G_1 * G_2$. Soit N le plus petit sougroupe normal de $G_1 * G_2$ qui contient $\mathbf{t}$. Ecrire $G = (G_1 * G_2)/N$, et soit $q : G_1 * G_2 \longrightarrow G$ l'homomorphisme quotient. Poser

$$g_1 = q(\varphi_1)_* : G_1 \longrightarrow G, \quad g_2 = q(\varphi_2)_* : G_2 \longrightarrow G.$$

Nous affirmons que (G, g_1, g_2) est la somme amalgamée voulue. En effet, etant donné un diagramme commutatif d'homomorphismes de groupe

$$\begin{array}{ccc} G_0 & \xrightarrow{f_1} & G_1 \\ {\scriptstyle f_2}\big\downarrow & & {\scriptstyle h_1}\big\downarrow \\ G_2 & \xrightarrow{h_2} & H \end{array}$$

soit $h : G_1 * G_2 \longrightarrow H$ l'homomorphisme induit par h_1 et h_2. Alors pour tout $a \in G_0$,

$$h\big((\varphi_1)_* f_1(a)\big) = h_1 f_1(a) = h_2 f_2(a) = h\big((\varphi_2)_* f_2(a)\big).$$

Ainsi, $\mathbf{t} \subseteq \ker h$, ce qui implique que $N \subseteq \ker h$. Autrement dit, h induit un homomorphisme $\hbar : G \longrightarrow H$ tel que $\hbar q = h$. D'ailleurs,

$$\hbar g_1 = \hbar q(\varphi_1)_* = h(\varphi_1)_* = h_1.$$

De même, $\hbar g_2 = h_2$.

Pour conclure, observer que l'unicité de h entraîne celle de $\hbar$, qui est forcément induit par h. $\square$