Sous-groupes distingués et groupes quotients

Travaux dirigés du 30 septembre et du 3 octobre 2025

Exercice 1. Manipulations de quotients

1. Soient H un sous-groupe distingué d'indice fini n de G, et $g \in G$. Montrer $g^n \in H$.
   Appliquons le théorème de Lagrange dans le groupe G/H (de cardinal n). Pour tout $g \in G$ on a $H = (gH)^n = g^n H$, et donc $g^n \in H$.
2. Montrer que si G est un groupe tel que $G/Z(G)$ est monogène, alors G est abélien.
   On suppose $G/Z(G)$ monogène engendré par $xZ(G)$. On en déduit que pour tout $g \in G$, alors $gZ(G)$ est de la forme $x^n Z(G)$ pour $n \in \mathbb{Z}$. En particulier, G est engendré par x et $Z(G)$. Comme x commute avec $Z(G)$ et lui-même, cela entraîne $x \in Z(G)$, puis $G = Z(G)$ est abélien.
3. Soient $(G_i)_{i\in I}$ une famille de groupes et, pour tout $i \in I$, H_i un sous-groupe distingué de G_i. On pose $G = \prod_{i\in I} G_i$, $H = \prod_{i\in I} H_i$. Montrer que H est distingué dans G, et qu'on a un isomorphisme naturel $G/H \simeq \prod_{i\in I} G_i/H_i$.
   Regardons l'application $f : \prod_{i\in I} G_i \to \prod_{i\in I} G_i/H_i$, $(g_i) \mapsto (g_i H_i)$. Elle est clairement surjective, et un morphisme de groupes. Son noyau est l'ensemble des $(g_i) \in \prod_{i\in I} G_i$ vérifiant $g_i H_i = H_i$ pour tout i, c'est-à-dire $g_i \in H_i$ pour tout i. On a donc $\ker f = \prod_{i\in I} H_i$. Ainsi, ce dernier est distingué et on conclut par $G/\ker f \simeq \operatorname{Im} f$.

Exercice 2. Deuxième théorème d'isomorphisme

Soit G un groupe, soit H un sous-groupe de G et soit N soit un sous-groupe du normalisateur de H (on dit que N *normalise* H).

1. Montrer que NH est un sous-groupe de G.
   Pour tout $n \in N$ on a $nHn^{-1} = H$, i.e. $nH = Hn$, donc NH est un sous-groupe de G.
2. Montrer que H est distingué dans NH et $N \cap H$ est distingué dans N.
   Comme H et N sont des sous-groupes du normalisateur de N, NH est un sous-groupe du normalisateur de H. Or H est distingué dans son propre normalisateur, donc *a fortiori* il est distingué dans NH. D'autre part, pour $n \in N$, on a $n(N\cap H)n^{-1} \subseteq N \cap nHn^{-1} = N \cap H$, donc $N \cap H$ est distingué dans N.
3. Montrer que $N/N\cap H \to NH/H$, $n(N\cap H) \mapsto nH$ est un isomorphisme.
   Comme la projection $\pi : NH \to NH/H$ est un morphisme de groupes et N est un sous-groupe de NH, la restriction de π à N, que l'on note f, est un morphisme de groupes. Ce morphisme est surjectif car pour tout $n \in N$ et $h \in H$ on a $nhH = n(hH) = nH = f(n)$. Par ailleurs, on a $\ker f = \{n \in N \mid nH = H\} = \{n \in N \mid n \in H\} = N \cap H$. On conclut par le premier théorème d'isomorphisme.

Exercice 3. Premier théorème de Sylow

Soit G un groupe fini d'ordre $p^n m$ avec p premier ne divisant pas m et $n \geq 1$. Pour $x \in G$, on note $\mathrm{Conj}(x)$ la classe de conjugaison de x et $C_G(x)$ son commutant.

1. Montrer que s'il existe $x \in G - Z(G)$ tel que $|\mathrm{Conj}(x)|$ est premier à p, alors on peut trouver un sous-groupe de G de cardinal $p^n m'$ avec $m' < m$.
   Le sous-groupe $H = C_G(x)$ de G est d'indice premier à p par la formule orbite-stabilisateur, donc de cardinal de la forme $p^n m'$ avec $m' | m$ (Lagrange). De plus, on a $m' < m$ car $|\mathrm{Conj}(x)| \neq 1$ (x n'est pas central).
2. Montrer que si $p || \mathrm{Conj}(x)|$ pour tout $x \in G - Z(G)$, alors on peut trouver un sous-groupe de G de cardinal p et distingué dans G.
   Par l'équation aux classes on a $p||Z(G)|$. Choisissons $x \in Z(G)$ d'ordre p (par exemple par Cauchy abélien). Alors $H = \langle x \rangle$ est d'ordre p et distingué dans G.
3. *(Premier théorème de Sylow)* Montrer que G possède un sous-groupe d'ordre p^n. Un tel sous-groupe s'appelle un p-*Sylow* de G.
   On raisonne par récurrence forte sur $|G|$ (le résultat est vrai pour $|G| = p$). S'il existe $x \in G - Z(G)$ tel que $|\mathrm{Conj}(x)|$ est premier à p, on trouve (question 1) un sous-groupe H de G de cardinal $p^n m'$ avec $m' < m$. Par hypothèse de récurrence, H admet un sous-groupe d'ordre p^n donc G aussi. Si $p || \mathrm{Conj}(x)|$ pour tout $x \in G - Z(G)$, alors on trouve (question 2) un sous-groupe H de G de cardinal p et distingué dans G. Alors le groupe quotient G/H est de cardinal $p^{n-1}m$ donc a, par hypothèse de récurrence, un sous-groupe d'ordre p^{n-1}. Ce sous-groupe est de la forme P/H, avec P sous-groupe de G contenant H, et on a $|P| = |P/H||H| = p^n$, ce qui conclut.

Exercice 4. Simplification par un groupe

Soient G, H et K des groupes finis. On se propose de montrer que si on a $G \times H \simeq G \times K$, alors on a $H \simeq K$. Pour deux groupes X, Y, on notera $\mathrm{Inj}(X, Y) \subseteq \mathrm{Hom}(X, Y)$ le sous-ensemble des morphismes injectifs.

1. Montrer que pour tout groupe fini S, on a $|\mathrm{Hom}(S, H)| = |\mathrm{Hom}(S, K)|$.
   Toute application $f : S \to H \times K$ s'écrit de manière unique sous la forme $f(x) = (a(x), b(x))$ avec $a : S \to H$ et $b : S \to K$ (quelconques). Par définition du groupe produit, f est un morphisme de groupes si, et seulement si, a et b en sont. Pour S fini on a donc $|\mathrm{Hom}(S, G \times H)| = |\mathrm{Hom}(S, G)||\mathrm{Hom}(S, H)|$, et de même $|\mathrm{Hom}(S, G \times K)| = |\mathrm{Hom}(S, G)||\mathrm{Hom}(S, K)|$. Mais on a aussi $|\mathrm{Hom}(S, G \times H)| = |\mathrm{Hom}(S, G \times K)|$ car on a $G \times H \simeq G \times K$ par hypothèse. Comme $|\mathrm{Hom}(S, G)|$ est fini non nul (considérer le morphisme trivial !), cela montre le résultat.
2. En déduire que pour tout groupe fini S, on a $|\mathrm{Inj}(S, H)| = |\mathrm{Inj}(S, K)|$.
   Par récurrence sur $|S|$ (c'est vrai pour $|S| = 1$). Tout morphisme $f : S \to H$ admet un noyau, qui est un sous-groupe distingué Q de S, et le morphisme f est injectif si et seulement si on a $Q = 1$. Le nombre de morphismes $S \to H$ de noyau Q est, par propriété universelle du groupe quotient, $|\mathrm{Inj}(S/Q, H)|$. La même chose vaut pour les morphismes $S \to K$ de noyau Q. Mais on a $|\mathrm{Inj}(S/Q, H)| = |\mathrm{Inj}(S/Q, K)|$ par hypothèse de récurrence quand $Q \neq 1$, et $|\mathrm{Hom}(S, H)| = |\mathrm{Hom}(S, K)|$ d'après la question 1 donc
   $$|\mathrm{Inj}(S, H)| + \sum_{\substack{Q \lhd S \\ Q \neq 1}} |\mathrm{Inj}(S/Q, H)| = |\mathrm{Inj}(S, K)| + \sum_{\substack{Q \lhd S \\ Q \neq 1}} |\mathrm{Inj}(S/Q, K)| = |\mathrm{Inj}(S, K)| + \sum_{\substack{Q \lhd S \\ Q \neq 1}} |\mathrm{Inj}(S/Q, H)|$$
   d'où $|\mathrm{Inj}(S, H)| = |\mathrm{Inj}(S, K)|$.
3. Conclure.
   On a $|\mathrm{Inj}(H, H)| \geq 1$ (l'identité !). Par la question 2 pour $S = H$ on en déduit l'existence d'un morphisme injectif $H \to K$. C'est un isomorphisme, car on a $|H| = |K|$.
4. Donner un exemple de groupe infini G vérifiant $G \times \mathbb{Z}/2\mathbb{Z} \simeq G \simeq G \times G$.
   Le groupe $G = (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$ fonctionne car on a des bijections entre $\mathbb{N}$, $\mathbb{N} \sqcup \{*\}$ et $\mathbb{N} \sqcup \mathbb{N}$.

Exercice 5. Disgression arithmétique

Dans l'exercice 4 du TD précédent, on a vu que les sous-groupes du groupe des inversibles d'un corps étaient cycliques. Il en découle que pour p premier, $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique. Maintenant, on va regarder la structure de $(\mathbb{Z}/n\mathbb{Z})^\times$ pour n quelconque. D'après l'isomorphisme chinois, il suffit de traiter le cas où n est une puissance d'un nombre premier.

1. Soit $k \geq 0$ un entier. Montrer que si p est un nombre premier impair, alors $(1+p)^{p^k} \equiv 1 + p^{k+1}[p^{k+2}]$. Montrer également $(1+4)^{2^k} \equiv 1 + 2^{k+2}[2^{k+3}]$.
   Si p est un nombre premier, on rappelle la congruence $\binom{p}{i} \equiv 0[p]$ si $i \in \{1, \ldots, p-1\}$. On en déduit que $a \equiv b[p^k]$ entraîne $a^p \equiv b^p[p^{k+1}]$. On conclut par récurrence sur k.
2. Soit p premier impair et $m \geq 1$. Montrer que le groupe $(\mathbb{Z}/p^m\mathbb{Z})^\times$ est cyclique.
   Supposons p premier impair. La question précédente montre que la classe de $1+p$ est d'ordre p^{m-1} dans $(\mathbb{Z}/p^m\mathbb{Z})^\times$. On a $|(\mathbb{Z}/p^m\mathbb{Z})^\times| = \varphi(p^m) = (p-1)p^{m-1}$ avec $(p-1, p^{m-1}) = 1$. Il suffit donc de trouver un élément d'ordre $p-1$ dans $(\mathbb{Z}/p^m\mathbb{Z})^\times$, car en le multipliant avec la classe de $1+p$ on obtiendra un générateur. Mais comme $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique, il existe $a \in \mathbb{Z}$ premier à p (et donc à p^m) dont la classe modulo p engendre $(\mathbb{Z}/p\mathbb{Z})^\times$. Soit d l'ordre de la classe de a dans $(\mathbb{Z}/p^m\mathbb{Z})^\times$. En réduisant modulo p la relation $a^d \equiv 1[p^m]$, il vient que $p-1$ divise d. Mais alors $a^{\frac{d}{p-1}}$ est d'ordre $p-1$.
3. Soit $m \geq 2$. Montrer qu'on a $(\mathbb{Z}/2^m\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{m-2}\mathbb{Z}$.
   La question 1 assure que 5 est d'ordre 2^{m-2} dans $(\mathbb{Z}/2^m\mathbb{Z})^\times$. Vérifions que le morphisme de groupes
   $$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{m-2}\mathbb{Z} \to (\mathbb{Z}/2^m\mathbb{Z})^\times, \ (a, b) \mapsto (-1)^a 5^b \bmod 2^m$$
   est un isomorphisme. Pour des raisons de cardinal, il suffit de voir qu'il est injectif. Mais si $(-1)^a 5^b \equiv 1[2^m]$, alors par réduction modulo 4 il vient $(-1)^a = 1$, puis $5^b \equiv 1[2^m]$ et donc $q \equiv 0$ car 5 est d'ordre 2^{m-2} modulo 2^m, ce qui achève la preuve.

Exercice 6. En général, on ne peut vraiment rien dire sur l'ordre du produit de deux éléments

Dans l'exercice 5 du TD précédent, on a vu le résultat suivant :

Proposition. *Pour tous entiers $a, b, c \geq 3$ (avec éventuellement $c = \infty$), il existe un groupe fini possédant un élément d'ordre a et un autre d'ordre b, dont le produit est d'ordre c.*

On rappelle que l'on avait en fait montré l'existence d'un corps fini k avec $\mathrm{car}(k) \neq 2$ tel que le groupe $SL_2(k)$ convienne. En se plaçant dans le groupe quotient $SL_2/\{\pm 1\}$, généraliser la proposition à tout $a, b, c \geq 2$.

Observons que le seul élément d'ordre 2 de $SL_2(k)$, quand k est un corps de caractéristique différente de 2, est -1. En effet, si on a $g \in SL_2(k)$ d'ordre 2 alors $X^2 - 1 = (X-1)(X+1)$ annule g et est à racines simples, donc g est conjugué dans $GL_2(k)$ à $\mathrm{diag}(\pm 1, \pm 1)$. Mais $\det g = 1$ montre que ces deux signes sont les mêmes, et $g \neq 1$ conclut l'observation. Fixons $a, b, c \geq 2$ des entiers. Soit k un corps fini avec $\mathrm{car}(k) \neq 2$ tel que le groupe $SL_2(k)$ possède des éléments g et h avec g d'ordre $2a$, h d'ordre $2b$ et gh d'ordre $2c$. Notons $[g]$ et $[h]$ les images de g et h dans le groupe quotient $SL_2(k)/\{\pm 1\}$. On observe que l'on a $g^a = h^b = (gh)^c = -1$, car ces trois éléments sont d'ordre 2. On en déduit aisément que $[g]$, $[h]$ et $[g][h]$ sont d'ordre respectifs a, b et c dans $SL_2(k)/\{\pm 1\}$: ce que l'on cherchait à démontrer.

⁂ Exercice 7. Groupes libres et présentations de groupes

Soit X un ensemble fini. Pensons à X comme à un alphabet et définissons 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, 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 :

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

1. Vérifier que $\mathrm{Mots}(X)$ est un monoïde et qu'on a une inclusion $X \subseteq \mathrm{Mots}(X)$.
   La loi de composition est manifestement associative, de neutre le mot vide $\emptyset$, et fait donc de $\mathrm{Mots}(X)$ un monoïde. On a une inclusion $X \subseteq \mathrm{Mots}(X)$ (mots de longueur 1).
2. *(Propriété universelle de l'ensemble des mots)* Montrer que pour tout monoïde M, toute application $X \to M$ s'étend de manière unique en un morphisme de monoïdes $\mathrm{Mots}(X) \to M$.
   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 l'inclusion à gauche (resp. à droite) $X \subseteq X^{\pm}$. 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). Soit R la relation sur $\mathrm{Mots}\left(X^{\pm}\right)$ telle que deux mots sont équivalents si et seulement 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 $x \in X^{\pm}$.

3. Vérifier que R est une relation d'équivalence. On note l'ensemble quotient associé $\mathrm{F}_X = \mathrm{Mots}\left(X^{\pm}\right)/R$, et on notera $[m]$ la classe d'équivalence de m.
   La définition implique la réflexivité, la symétrie et la transitivité.
4. Montrer qu'il existe une unique loi de monoïde sur F_X telle que la projection canonique $\mathrm{Mots}\left(X^{\pm}\right) \to \mathrm{F}_X$ est un morphisme de monoïde.
   Soit $\pi : \mathrm{Mots}\left(X^{\pm}\right) \to \mathrm{F}_X$ la projection canonique. Toute loi de composition $\star$ sur F_X telle que π est un morphisme vérifie $[m] \star \left[m'\right] = \pi(m) \star \pi\left(m'\right) = \pi\left(mm'\right) = \left[mm'\right]$. Comme π est surjective, $\star$ est donc unique si elle existe, nécessairement associative car la loi de $\mathrm{Mots}\left(X^{\pm}\right)$ l'est, et admet $\pi(1) = [1]$ pour neutre.
   Pour l'existence, il s'agit de montrer que l'application $\mathrm{Mots}\left(X^{\pm}\right) \times \mathrm{Mots}\left(X^{\pm}\right) \to \mathrm{F}_X$, $(m, n) \mapsto [mn]$, passe au quotient en une application $\mathrm{F}_X \times \mathrm{F}_X \to \mathrm{F}_X$, c'est-à-dire que pour tous éléments m, m', n, n' dans $\mathrm{Mots}\left(X^{\pm}\right)$ vérifiant mRm' et nRn', on a $mnRm'n'$. Mais c'est clair par définition de R.
5. Montrer que cette loi fait de F_X un groupe engendré par les $[x]$ avec $x \in X$. On dit que F_X est le *groupe libre* sur X.
   Par définition de R on a $[x]\left[x^{-1}\right] = \left[xx^{-1}\right] = [1] = \left[x^{-1}x\right] = \left[x^{-1}\right][x]$ pour tout $x \in X^{\pm}$, de sorte que $\left[x^{-1}\right]$ est un inverse de $[x]$ dans F_X. De plus, comme $X^{\pm}$ engendre le monoïde $\mathrm{Mots}(X^{\pm})$, les $[x]$ avec $x \in X^{\pm}$ engendrent aussi F_X, qui est donc un groupe (l'inverse de $[x_1] \ldots [x_n]$ est $\left[x_n^{-1}\right] \ldots \left[x_1^{-1}\right]$). Enfin, comme on a l'inclusion à gauche (ou à droite) $X \subseteq X^{\pm}$ et $[x]^{-1} = \left[x^{-1}\right]$ dans F_X, il suffit d'une copie de X pour engendrer le groupe F_X.

6. *(Propriété universelle du groupe libre)* Montrer que pour tout groupe G et 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 $x \in X$.

   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 $f\left(x^{-1}\right) = f(x)^{-1}$ pour $x \in X$. Par la propriété universelle de l'ensemble des mots, il existe un (unique) morphisme de monoïdes $g : \mathrm{Mots}\left(X^{\pm}\right) \to G$ tel que $g(x) = f(x)$ et $g\left(x^{-1}\right) = f(x)^{-1}$ pour $x \in X$, et donc avec $g\left(x^{-1}\right) = g(x)^{-1}$ pour tout $x \in X^{\pm}$.
   Supposons que l'on ait $m, m' \in \mathrm{Mots}\left(X^{\pm}\right)$ avec $m' = n_1 x x^{-1} n_2$ et $m = n_1 n_2$, où $x \in X^{\pm}$ et n_1, n_2 des mots sur $X^{\pm}$. On a

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

   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 $m \in \mathrm{Mots}\left(X^{\pm}\right)$. Par définition de la loi quotient sur F_X, c'est automatiquement un morphisme de groupes : pour $m, m' \in \mathrm{Mots}\left(X^{\pm}\right)$ on a les égalités $f'\left([m]\left[m'\right]\right) = f'\left(\left[mm'\right]\right) = g\left(mm'\right) = g(m) g\left(m'\right) = f'([m]) f'\left(\left[m'\right]\right)$. □

7. 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 $1 \leq i < n$. Montrer que l'application canonique $\mathrm{Mots}\left(X^{\pm}\right) \to \mathrm{F}_X, m \mapsto [m]$, induit une bijection entre le sous-ensemble des mots réduits sur $X^{\pm}$ et F_X. En particulier, l'application naturelle $X^{\pm} \to \mathrm{F}_X, x \mapsto [x]$, est injective ; souvent, on notera simplement x la classe $[x]$ en voyant $X^{\pm}$ comme une partie de F_X.

   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 $\Omega \subset \mathrm{Mots}\left(X^{\pm}\right)$ désigne le sous-ensemble des mots réduits, on a défini une application

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

   Par la propriété universelle du groupe libre, il existe donc un (unique) 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 $f'([m]) = \mathrm{L}_{x_1} \circ \cdots \circ \mathrm{L}_{x_r}$. Mais alors 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 $1 \leq i < r$. Par ailleurs, pour $m, m' \in \Omega$ avec $[m] = \left[m'\right]$, on a $f'\left(\left[m'\right]\right) = f'([m])$, et donc $m = f'([m])(\emptyset) = f'\left(\left[m'\right]\right)(\emptyset) = m'$.

8. Décrire F_X pour $X = \emptyset$ et pour $X = \{x\}$ un singleton. Montrer que pour $|X| \geq 2$, le groupe F_X est non commutatif.

   On a $F_X = \{1\}$ 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

   $$\mathbb{Z} \xrightarrow{\sim} \mathrm{F}_X,\ n \mapsto x^n$$

   d'après la question précédente. Enfin, 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 la question précédente.

9. Montrer que toute application $X \to Y$ (resp. bijection) induit un morphisme (resp. isomorphisme) de groupes $\mathrm{F}_X \to \mathrm{F}_Y$. 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.

   C'est une conséquence de la propriété universelle du groupe libre : toute application $f : X \to Y$ est une application $X \to \mathrm{F}_Y$ donc induit un morphisme de groupes $f' : \mathrm{F}_X \to \mathrm{F}_Y$. Si $X \to Y$ est de surcroît une bijection, sa réciproque g donne également un morphisme $g' \mathrm{F}_Y \to \mathrm{F}_X$ tel que $g' \circ f'$ (qui prolonge $g \circ f$) soit l'identité sur X et $f' \circ g'$ (qui prolonge $f \circ g$) soit l'identité sur Y. Par la clause d'unicité dans la propriété universelle, on a donc $g \circ f = \mathrm{id}_X$ et $g \circ f = \mathrm{id}_Y$, d'où f isomorphisme.

On discute maintenant de 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 du groupe libre, iil existe un unique morphisme de groupes $f : \mathrm{F}_X \to G$, avec $f(x) = g_x$ pour tout $x \in X$. On dit alors qu'un mot $m \in \mathrm{Mots}\left(X^{\pm}\right)$ est une *relation* entre les g_x si on a $f([m]) = 1$. Comme tout mot m' équivalent à une relation m entre les g_x est encore une relation entre les g_x, 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 $\ker f \subseteq \mathrm{F}_X$. Comme les $x \in X$ engendrent F_X, le morphisme f est surjectif si et seulement si les g_x engendrent G, auquel cas on a $\mathrm{F}_X / \ker f \simeq G$.

10. Donner des exemples de relations vérifiées par un groupe commutatif, puis un groupe d'ordre n, puis $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$.
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 $b=(0,1)$.

11. Montrer 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 $\cup_{g\in G}gXg^{-1}$. C'est la *clôture normale* de X dans G, on la note $\langle X\rangle^{\triangleleft}$.
Tout sous-groupe distingué contenant X contient $Y:=\cup_{g\in G}gXg^{-1}$, et donc le sous-groupe $\langle Y\rangle$ engendré par Y. Par ailleurs, $\langle Y\rangle$ est distingué, car si $g\in G$ on peut écrire , ce qui conclut.

Soient $\mathscr{G}$ un ensemble et $\mathscr{R}\subseteq\mathrm{Mots}\left(\mathscr{G}^{\pm}\right)$ 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 $\langle\mathscr{G}\mid r=1,\forall r\in\mathscr{R}\rangle$. 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 $\mathscr{R}$). 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 $\langle g_1,\dots,g_n\mid r_1=r_2=\cdots=r_s=1\rangle$ et on parle de *présentation finie*.

12. *(Propriété universelle d'un groupe défini par générateurs et relations)* Soient $\mathscr{G}$ un ensemble, $\mathscr{R}\subset\mathrm{Mots}\left(\mathscr{G}^{\pm}\right)$ et G un groupe. Montrer qu'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 $r\in\mathscr{R}$.
Par la propriété universelle du groupe quotient, un morphisme de groupes $\mathrm{F}_{\mathscr{G}}/\langle\mathscr{R}\rangle^{\triangleleft}\to G$ est la même chose qu'un morphisme de groupes $\mathrm{F}_{\mathscr{G}}\to G$ trivial sur $\langle\mathscr{R}\rangle^{\triangleleft}$. On remarque que si $f:\mathrm{F}_{\mathscr{G}}\to G$ est un morphisme de groupes tel que $f(r)=1$ pour tout $r\in\mathscr{R}$, pour tout $g\in G$ on a $f(g\mathscr{R}g^{-1})=f(g)f(\mathscr{R})f(g)^{-1}=\{1\}$ donc f est trivial sur $\langle\mathscr{R}\rangle^{\triangleleft}$. Donc un morphisme de groupes $\mathrm{F}_{\mathscr{G}}/\langle\mathscr{R}\rangle^{\triangleleft}\to G$ est la même chose qu'un morphisme de groupes $\mathrm{F}_{\mathscr{G}}\to G$ tel que $f(r)=1$ pour tout $r\in\mathscr{R}$. Enfin, par la propriété universelle du groupe libre, c'est la même chose qu'une application $f:\mathscr{G}\to G$ telle que $f(r)=1$ pour tout $r\in\mathscr{R}$.

13. Montrer que μ_n admet la présentation $\langle a\mid a^n=1\rangle$ et $\mathbb{Z}\times\mathbb{Z}$ la présentation $\langle a,b\mid aba^{-1}b^{-1}=1\rangle$.
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 $0\le m<n$, puis $|G_1|\le n$, 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^mb^n avec $m,n\in\mathbb{Z}$. Mais alors on constate $f(x)=f(a)^mf(b)^n=(m,n)\in\mathbb{Z}^2$, de sorte que l'écriture $x=a^mb^n$ est unique, et f est bijective.

14. Montrer que tout groupe fini admet une présentation finie.
Soit G un groupe fini, soit $\mathscr{G}$ l'ensemble sous-jacent à G. Pour éviter les confusions, on le note $\{e_g\mid g\in G\}$. Soit

$$\mathscr{R}=\left\{e_ge_he_{gh}^{-1}\mid g,h\in G\right\}.$$

On pose $G'=\langle\mathscr{G}\mid r=1,\forall r\in\mathscr{R}\rangle$. Par la propriété universelle, il existe un unique morphisme de groupes $G'\to G$ envoyant e_g sur g. Ce morphisme est clairement surjectif, et tout élément de G' est de la forme $e_{g_1}^{\varepsilon_1}\dots e_{g_n}^{\varepsilon_n}=e_{g_1^{\varepsilon_1}\dots g_n^{\varepsilon_n}}$ ($n\ge1$, $\varepsilon_1,\dots,\varepsilon_n\in\{\pm1\}$), donc $\left|G'\right|\le|G|$, ce qui montre que le morphisme est bijectif et donc $\langle\mathscr{G}\mid r=1,\forall r\in\mathscr{R}\rangle$ est une présentation finie de G.