On appelle *alphabet* tout ensemble fini non vide. Si A est un alphabet, on appelle ses éléments des *lettres*. Un mot u sur l'alphabet A est une suite finie de lettres de A. La longueur de cette suite est appelée la longueur du mot, notée $|u|$. Par exemple, si $A = \{a, b\}$, $u = aab$ est un mot de longueur 3 et $v = baababa$ est un mot de longueur 7.

Par convention, on considère aussi une suite de longueur 0, appelée le *mot vide* et notée 1. On note A^* l'ensemble de tous les mots sur l'alphabet A, y compris le mot vide.

On appelle *monoïde* tout ensemble M muni d'une loi de composition interne associative et contenant un élément neutre (noté 1_M). Si A est un alphabet, A^* muni de la concaténation est un monoïde. On rappelle que la concaténation de deux mots u et v, notée uv, est la suite de lettres qui commence par la suite u et continue avec la suite v. Pour les mots u et v cités en exemple ci-dessus, on a $uv = aabbaababa$. Si w est un mot et k est un entier strictement positif, on note w^k la concaténation de k copies de w. On peut ainsi écrire $u = a^2b$ et $v = ba(ab)^2a = ba^2(ba)^2$.

Si M (muni de l'opération $\odot$) et N (muni de l'opération $\otimes$) sont des monoïdes, un *morphisme* $\varphi\colon M \longrightarrow N$ est une application telle que $\varphi(1_M) = 1_N$ et telle que $\varphi(x \odot y) = \varphi(x) \otimes \varphi(y)$ pour tout $x, y \in M$. Un *isomorphisme* est un morphisme bijectif.

Soit G un monoïde, muni de l'opération $\odot$. Un élément $x \in G$ est dit *inversible* s'il existe $y \in G$ tel que $x \odot y = y \odot x = 1_G$. Dans ce cas, y est unique et est appelé l'*inverse* de x, noté x^{-1}. Rappelons qu'un groupe est un monoïde dans lequel chaque élément est inversible.

On notera $\mathsf{card}(X)$ le cardinal d'un ensemble fini X, c'est-à-dire le nombre d'éléments de X.

Dans ce sujet, on étudie les *groupes libres*. Ces groupes se caractérisent par le fait qu'ils sont entièrement déterminés par un ensemble de générateurs abstraits (ce qui justifie la terminologie, puisqu'ils sont libres de toute relation entre leurs générateurs). On examinera des propriétés élémentaires des groupes libres et quelques problèmes algorithmiques les concernant. Le problème s'achève par la démonstration du fait que tout sous-groupe finiment engendré d'un groupe libre est lui-même un groupe libre.

Note : les questions d'algorithmique sont sans doute à reformuler. Je ne suis pas sûr de ce qu'on peut admettre comme connu en matière d'algorithmique et de complexité...

1 – Préliminaires

Dans cette partie, on reprend quelques propriétés élémentaires des monoïdes et des groupes.

Question 1.1 *Soient M (muni de l'opération $\odot$) et N (muni de l'opération $\otimes$) des monoïdes. Soit $\varphi\colon M \longrightarrow N$ un morphisme.*

1.1.1 *Montrer que si φ est un isomorphisme, alors $\varphi^{-1}: N \longrightarrow M$ est un morphisme.*

> **Solution**. Par définition, φ est un morphisme bijectif. En particulier, on a $\varphi(1_M) = 1_N$ et donc $\varphi^{-1}(1_N) = 1_M$. Soient maintenant $x, y \in N$: on veut comparer $\varphi^{-1}(x \otimes y)$ et $\varphi^{-1}(x) \odot \varphi^{-1}(y)$. On a
>
> $$\varphi(\varphi^{-1}(x) \odot \varphi^{-1}(y)) = \varphi(\varphi^{-1}(x)) \otimes \varphi(\varphi^{-1}(y)) = x \otimes y,$$
>
> donc $\varphi^{-1}(x) \odot \varphi^{-1}(y) = \varphi^{-1}(x \otimes y)$, ce qui conclut la preuve.

1.1.2 *Montrer que si M et N sont des groupes et si $x \in M$, alors $\varphi(x^{-1}) = (\varphi(x))^{-1}$.*

> **Solution**. Par définition d'un morphisme, $\varphi(x) \otimes \varphi(x^{-1}) = \varphi(x \odot x^{-1}) = \varphi(1_M) = 1_N$. Symétriquement, $\varphi(x^{-1}) \otimes \varphi(x) = 1_N$ et donc $\varphi(x^{-1}) = (\varphi(x))^{-1}$.

Si M est un monoïde pour la loi de composition $\odot$ et si N est une partie de M, on dit que N est un *sous-monoïde* de M si $1_M \in N$ et si pour tout $x, y \in N$, on a $x \odot y \in N$. Si de plus M est un groupe et si N est un sous-monoïde tel que pour tout $x \in N$, on a $x^{-1} \in N$, on dit que N est un *sous-groupe* de M.

Question 1.2 *Soit R une partie d'un monoïde M.*

1.2.1 *Soit R^* l'ensemble consistant en l'élément neutre 1_M et les produits d'éléments de R, c'est-à-dire les éléments $r_1 \odot \cdots \odot r_n$ avec $n \geq 1$ et chaque $r_i \in R$. Montrer que R^* est un sous-monoïde de M, qui est minimal pour l'inclusion parmi tous les sous-monoïdes contenant R.*

> **Solution**. Il est évident par définition que R^* est un sous-monoïde. Si N est un sous-monoïde de M contenant R, alors M contient 1_M et tous les produits, de longueur arbitrairement grande, de ses éléments. En particulier, N contient les produits d'éléments de R, et donc $R^* \subseteq N$.

1.2.2 *Supposons que M est un groupe et soit $R^{-1} = \{r^{-1} \mid r \in R\}$. Montrer que $(R \cup R^{-1})^*$ est un sous-groupe de M, qui est minimal pour l'inclusion parmi tous les sous-groupes contenant R.*

> **Solution**. Par la question précédente, $(R \cup R^*)$ est un sous-monoïde de M. Il faut montrer que c'est un sous-groupe, la minimalité se vérifiera alors comme ci-dessus. Pour cela, considérons un élément quelconque de $(R \cup R^*)$, soit $x = r_1 \odot \cdots \odot r_n$ avec $n \geq 1$ et $r_i \in R \cup R^{-1}$ pour tout $1 \leq i \leq n$. Alors pour tout i, r_i^{-1} est aussi dans $R \cup R^{-1}$. Par conséquent $y = r_n^{-1} \odot \cdots \odot r_1^{-1} \in (R \cup R^*)$. Enfin on vérifie facilement que $x \odot y = y \odot x = 1_M$.

Dans ce dernier cas, on appelle $(R \cup R^{-1})^*$ le *sous-groupe engendré par R*.

2 – Mots réduits

Pour le reste du problème, on fixe un alphabet A. Pour chaque lettre $a \in A$, on introduit une nouvelle lettre $\bar{a}$ et on note $\tilde{A}$ l'alphabet $\{a \mid a \in A\} \cup \{\bar{a} \mid a \in A\}$. On étend l'application $a \mapsto \bar{a}$ à $\tilde{A}$ en posant $\bar{\bar{a}} = a$ for each $a \in A$.

Soient $u, v \in \tilde{A}^*$. On dit que u *se réduit en une étape en* v, noté $u \xrightarrow{1} v$, si u s'écrit $u = u_1 a\bar{a} u_2$ et $v = u_1 u_2$ avec $a \in \tilde{A}$ et $u_1, u_2 \in \tilde{A}^*$.

Si $k \geq 1$, on note $u \xrightarrow{k} v$ s'il existe des mots $u_0, \ldots, u_k \in \tilde{A}^*$ tels que $u = u_0$, $v = u_k$ et $u_i \xrightarrow{1} u_{i+1}$ pour $i = 0, 1, \ldots, k-1$. On note encore $u \xrightarrow{0} v$ si $u = v$, $u \xrightarrow{\leq k} v$ s'il existe $\ell \leq k$ tel que $u \xrightarrow{\ell} v$, et $u \xrightarrow{\infty} v$ s'il existe k tel que $u \xrightarrow{k} v$. Enfin, on dit qu'un mot $u \in \tilde{A}^*$ est *réduit* s'il n'existe aucun mot v tel que $u \xrightarrow{1} v$, c'est-à-dire si u ne contient pas deux lettres consécutives de la forme $a\bar{a}$ avec $a \in \tilde{A}$. En particulier, le mot vide est réduit.

Soit $F(A)$ l'ensemble des mots réduits de $\tilde{A}^*$. On va montrer que tout mot se réduit en un mot réduit unique.

Question 2.1 *On commence par montrer l'existence d'une réduction en un mot réduit.*

2.1.1 *Soit*

$$u = ab\bar{a}a\bar{b}\bar{b}aab\bar{b}\bar{a}\bar{a}aab\bar{b}\bar{a}ab.$$

Calculer un mot réduit v tel que $u \xrightarrow{\infty} v$.

Solution. $a\bar{b}aab$

2.1.2 *Montrer que pour tout mot $u \in \tilde{A}^*$, il existe un mot réduit v tel que $u \xrightarrow{\infty} v$.*

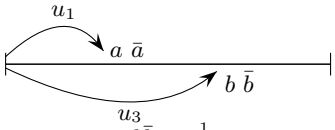
Solution. On procède par récurrence sur $|u|$. Si $|u| \leq 1$, alors u est réduit et $u \xrightarrow{\infty} u$. Supposons maintenant le résultat vrai pour les mots plus courts que u. Si u est réduit, alors $u \xrightarrow{\infty} u$. Si u n'est pas réduit, alors u peut s'écrire $u = u' a\bar{a} u''$ avec $a \in \tilde{A}$ et $u', u'' \in \tilde{A}^*$. On a alors $u \xrightarrow{1} u'u''$, et comme ce dernier mot est plus court que u, il existe un mot réduit v tel que $u'u'' \xrightarrow{\infty} v$. Mais alors $u \xrightarrow{\infty} v$, ce qu'il fallait démontrer.

Question 2.2 *Soient $u, x, y \in \tilde{A}^*$. Montrer que si $u \xrightarrow{1} x$ et $u \xrightarrow{1} y$, alors il existe z tel que $x \xrightarrow{\leq 1} z$ et $y \xrightarrow{\leq 1} z$.*

Solution. Par hypothèse, il existe des lettres $a, b \in \tilde{A}$ et des mots u_1, u_2, u_3, u_4 tels que

$$u = u_1 a\bar{a} u_2,\ x = u_1 u_2,\ u = u_3 b\bar{b} u_4,\ v = u_3 u_4.$$

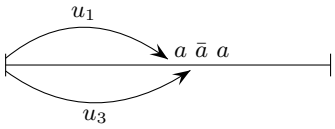
On distingue 5 cas, selon les longueurs respectives de u_1 et u_3.
(1) Si $|u_1| \leq |u_3| - 2$, alors il existe un mot v tel que $u_3 = u_1 a\bar{a} v$ et $u_2 = v b\bar{b} u_4$. Si on pose $z = u_1 v u_4$, on a



$$x \quad = \quad u_1 u_2 \quad = \quad u_1 v b\bar{b} u_4 \xrightarrow{1} u_1 v u_4 = z$$

$$y \quad = \quad u_3u_4 \quad = \quad u_1a\bar{a}vu_4 \xrightarrow{1} u_1vu_4 = z.$$

(2) Si $|u_1| = |u_3| - 1$, alors $b = \bar{a}$, $u_3 = u_1a$ et $u_2 = \bar{b}u_4 = au_4$.



Par conséquent, $x = u_1au_4 = y$ et on pose $z = x = y$.

(3) Si $|u_1| = |u_3|$, alors $u_1 = u_3$, $a = b$ et $u_2 = u_4$, si bien que $x = y$ et on pose $z = x = y$.

Les cas (4) et (5), où $|u_1| = |u_3| + 1$ et $|u_1| \geq |u_3| + 2$ sont duaux des cas (2) et (1) respectivement.

Question 2.3 *Montrer que pour tout mot $u \in \tilde{A}^*$, il existe un unique mot réduit v tel que $u \xrightarrow{\infty} v$.*

Solution. Supposons que $u \xrightarrow{k} v$ et $u \xrightarrow{\ell} v'$ avec v et v' réduits. On montre par récurrence sur $|u|$ que $v = v'$.

Si $|u| \leq 1$, alors $u = v = v'$ (et $k = \ell = 0$). Supposons maintenant que $|u| \geq 2$. Si $k = 0$ ou $\ell = 0$, alors u est réduit, $k = \ell = 0$ et $u = v = v'$.

Si $k, \ell \geq 1$, alors il existe des mots x, y tels que $u \xrightarrow{1} x \xrightarrow{k-1} v$ et $u \xrightarrow{1} y \xrightarrow{\ell-1} v'$, avec par conséquent $|x| < |u|$ et $|y| < |u|$. Appliquons la question 2.2 : il existe un mot z tel que $x \xrightarrow{\leq 1} z$ et $y \xrightarrow{\leq 1} z$. Puis la question 2.1.2 : il existe un mot réduit z' tel que $z \xrightarrow{\infty} z'$. Mais alors $x \xrightarrow{\infty} v$ et $x \xrightarrow{\infty} z'$, par hypothèse de récurrence il s'en suit que $v = z'$. Symétriquement, $v' = z'$ et donc $v = v'$.

On note $\rho(u)$ l'unique mot réduit tel que $u \xrightarrow{\infty} \rho(u)$ et on note $\rho\colon \tilde{A}^* \longrightarrow F(A)$ l'application $u \longmapsto \rho(u)$.

Question 2.4 *Donner un algorithme pour calculer le mot $\rho(u)$, étant donné $u \in \tilde{A}^*$. Estimer la complexité de cet algorithme en fonction de la longueur $n = |u|$.*

Solution. Deux solutions viennent à l'esprit. La première, moins efficace, consiste à lire le mot u de gauche à droite pour repérer puis éliminer des lettres $a\bar{a}$ consécutives, puis de répéter cette procédure jusqu'à ce qu'aucune simplification ne soit plus possible. Chaque lecture prend un temps $O(n)$, chacune diminue la longueur d'au moins deux unités, et donc l'algorithme termine après au plus $n/2$ lectures, soit une complexité en $O(n^2)$.

La seconde utilise un mécanisme de pile : on lit le mot u de gauche à droite, et on écrit à ses côtés un mot v sur le même alphabet. Au début v est le mot vide. Lorsqu'on lit un caractère $a \in \tilde{A}$ dans u, soit la dernière lettre de v est différente de $\bar{a}$ et on rajoute a à la fin de v ; soit la dernière lettre de v est $\bar{a}$ et on efface cette dernière lettre de v. A la fin, le mot v est égal à $\rho(u)$. La complexité de cet algorithme est $O(n)$.

3 – Groupes libres

On étend maintenant l'application $a \longmapsto \bar{a}$ à $\tilde{A}^*$ en posant

$$\begin{array}{rcl} \bar{1} & = & 1, \\ \overline{a_1 a_2 \cdots a_n} & = & \bar{a}_n \cdots \bar{a}_2 \bar{a}_1 \text{ si } a_1, \ldots, a_n \in \tilde{A}. \end{array}$$

On définit une loi de composition sur $F(A)$ en posant $u \odot v = \rho(uv)$.

Question 3.1 *Montrer que $F(A)$, muni de l'opération $\odot$, est un groupe.*

Indication. On pourra montrer dans un premier temps que si $u, v, w \in \tilde{A}^*$, alors $u \odot (v \odot w) = \rho(uvw)$.

> **Solution**. On se convainc que si $u, v, x, y \in \tilde{A}^*$ et $u \xrightarrow{\infty} v$, alors $xuy \xrightarrow{\infty} xvy$. Soient alors $u, v, w \in F(A)$: on a $uvw \xrightarrow{\infty} u\rho(vw)$. Par unicité de la réduction, on en déduit que $\rho(uvw) = \rho(u\,\rho(vw)) = u \odot (v \odot w)$. Par symétrie, $\rho(uvw) = (u \odot v) \odot w$, ce qui démontre l'associativité de l'opération $\odot$.
>
> Il est immédiat que le mot vide 1 est un élément neutre. Enfin, pour tout mot $u \in F(A)$, $\bar{u}$ est aussi un mot réduit (c'est-à-dire que $\bar{u} \in F(A)$) et $\rho(u\bar{u}) = 1$. On a donc $\bar{u} = u^{-1}$.

On appelle $F(A)$ le *groupe libre sur A*. On appelle *groupe libre* tout groupe isomorphe à un groupe de la forme $F(A)$.

Question 3.2 *Sous quelles hypothèses le groupe $F(A)$ est-il commutatif (c'est-à-dire tel que $u \odot v = v \odot u$ pour tout $u, v \in F(A)$) ?*

> **Solution**. Si A a au moins deux éléments a et b, alors ab et ba sont deux mots réduits distincts, donc $F(A)$ n'est pas commutatif. Si $A = \{a\}$, les mots réduits sont les mots de la forme 1, a^n et $\bar{a}^n$ $(n > 0)$. Il est facile de vérifier qu'alors $F(A)$ est commutatif (et isomorphe au groupe $(\mathbb{Z}, +)$).

Question 3.3 *Soit G un groupe et soit $\varphi' \colon A \longrightarrow G$ une application. Montrer que φ' admet un unique prolongement en un morphisme $\varphi \colon F(A) \longrightarrow G$.*

> **Solution**. On commence par étendre φ' à $\tilde{A}$ en posant $\varphi'(\bar{a}) = \varphi'(a)^{-1}$ pour tout $a \in A$. Puis on définit une application $\varphi \colon F(A) \to G$ de la façon suivante : $\varphi(1) = 1_G$ et si $u = a_1 \cdots a_n \in F(A)$ avec les $a_i \in \tilde{A}$, alors $\varphi(u) = \varphi'(a_1) \cdots \varphi'(a_n)$.
>
> Notons que si $u = a_1 \cdots a_n \in F(A)$ avec les $a_i \in \tilde{A}$, alors $\rho(u) = u$ et donc $u = a_1 \odot \cdots \odot a_n$. Il s'ensuit que que tout prolongement de φ' en un morphisme φ vérifie nécessairement l'égalité $\varphi(u) = \varphi'(a_1) \cdots \varphi'(a_n)$, c'est-à-dire qu'on a établi l'unicité de φ, si φ existe.
>
> Il faut maintenant de montrer que φ est un morphisme. Soient $u, v \in F(A)$ et soit q le plus long préfixe (segment initial) de v tel que $\bar{q}$ est un suffixe de u. On a alors $u = p\bar{q}$, $v = qr$ et $u \odot v = pr$. Par conséquent, au vu de la question 1.1.2
>
> $$\varphi(u \odot v) = \varphi(pr) = \varphi(p)\varphi(r) = \varphi(p)\varphi(q)^{-1}\varphi(q)\varphi(r) = \varphi(u)\varphi(v),$$
>
> ce qui conclut la preuve.

Autre preuve. On note que φ peut être défini de la même façon sur le monoïde $(A \cup \tilde{A})^*$ et que sur ce monoïde, φ est clairement un morphisme. On montre ensuite (directement depuis la définition) que $u \xrightarrow{1} v$ implique $\varphi(u) = \varphi(v)$. Mais alors $u \xrightarrow{\infty} v$ implique $\varphi(u) = \varphi(v)$ et en particulier $\varphi(u) = \varphi(\rho(u))$. Il s'ensuit que $\varphi(u \odot v) = \varphi(\rho(u)\rho(v)) = \varphi(\rho(u))\varphi(\rho(v)) = \varphi(u)\varphi(v)$.

Dans la situation de la question 3.3, on dit que le morphisme φ est *induit par* l'application φ'. Dans la suite, on utilisera librement le résultat de cette question : toute application de A dans un groupe G induit un unique morphisme de $F(A)$ dans G.

4 – Rang d'un groupe libre

Soit X une partie finie non vide de $F(A)$. On dit que X *est une base de* $F(A)$ si, étant donnés un alphabet B de même cardinal que X et une bijection $\varphi' : B \longrightarrow X$, le morphisme $\varphi : F(B) \longrightarrow F(A)$ induit par φ' est un isomorphisme. On admettra que cette condition ne dépend pas du choix de l'alphabet B et de la bijection φ'.

En particulier, l'ensemble A est une base de $F(A)$. Le but de cette partie est de montrer que toutes les bases de $F(A)$ ont le même cardinal.

Question 4.1 *Supposons que* $A = \{a, b\}$.

4.1.1 *Soient* $x = ab\bar{a}$ *et* $y = ab$. *Exprimer* a *et* b *comme produits d'éléments de la forme* x, x^{-1}, y *et* y^{-1} *(pour l'opération* $\odot$*), et en déduire que* $X = \{ab\bar{a}, ab\}$ *est une base de* $F(A)$.

Solution. On observe que $\bar{a} = y^{-1} \odot x$ et donc $a = x^{-1} \odot y$. Il suit que $b = a^{-1} \odot y = y^{-1} \odot x \odot y$.
Soit $B = \{c, d\}$ et soit la bijection $\varphi' : B \longrightarrow X$ donnée par $c \mapsto x$ et $d \mapsto y$. Soit $\psi' : A \longrightarrow B$ donné par $a \mapsto \bar{c}d$ et $b \mapsto \bar{d}cd$. Enfin, soient φ et ψ les morphismes induits par φ' et ψ' respectivement. Notons que $\varphi \circ \psi(a) = a$ et $\varphi \circ \psi(b) = b$. L'unicité du morphisme induit par une application (établie dans la question 3.3) implique que $\varphi \circ \psi = \mathsf{id}_{F(A)}$. De la même façon, on vérifie que $\psi \circ \varphi = \mathsf{id}_{F(B)}$. Par conséquent φ et ψ sont des isomorphismes et X est une base de $F(A)$.

4.1.2 *Montrer que* $\{ab\bar{a}\bar{b}, b\bar{a}\bar{b}a\}$ *n'est pas une base de* $F(A)$. *On montrera par example que si* $B = \{c, d\}$ *et* $\varphi' : B \longrightarrow F(A)$ *est tel que* $\varphi'(c) = ab\bar{a}\bar{b}$ *et* $\varphi'(d) = b\bar{a}\bar{b}a$, *alors le morphisme induit* $\varphi : F(B) \longrightarrow F(A)$ *n'est pas surjectif.*

Solution. On note que dans $\varphi'(c)$ et $\varphi'(d)$, la somme des puissances de a est nulle, de même que la somme des puissances de b. Il en va donc de même pour tous les éléments de $F(A)$ obtenus comme produits de ces éléments et de leurs inverses. Cela montre que le morphisme φ n'est pas surjectif et donc pas un isomorphisme.

Pour tout alphabet A, on considère un espace vectoriel $V(A)$ (sur $\mathbb{R}$), de dimension $\mathsf{card}(A)$ et une base E de $V(A)$. En particulier, E a le même cardinal que A et on considère une bijection $\kappa'_A : A \longrightarrow E$. Comme $V(A)$ muni de l'addition est un groupe, on peut considérer le morphisme $\kappa_A : F(A) \longrightarrow V(A)$ induit par l'application κ'_A.

Question 4.2 *Soient A et B deux alphabets et soit $\varphi : F(A) \longrightarrow F(B)$ un morphisme.*

4.2.1 *Montrer qu'il existe une application linéaire $\hat{\varphi} : V(A) \longrightarrow V(B)$ telle que $\kappa_B \circ \varphi = \hat{\varphi} \circ \kappa_A$, comme dans la figure 1.*

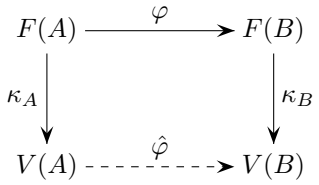


FIG. 1 – L'application linéaire $\hat{\varphi}$ définie par l'homomorphisms φ

Solution. Pour tout $a \in A$, posons $e_a = \kappa_A(a)$ et $f_a = \kappa_B(\varphi(a))$. Puisque $E = \{e_a \mid a \in A\}$ est une base de l'espace vectoriel $V(A)$, on sait qu'il existe une et une seule application linéaire $\hat{\varphi}$ de $V(A)$ dans $V(B)$ telle que $\hat{\varphi}(e_a) = f_a$. Si on considère $V(A)$ et $V(B)$ (munis de l'addition) comme des groupes, cette application linéaire est aussi un morphisme. Par conséquent, $\hat{\varphi} \circ \kappa_A$ est un morphisme, qui coïncide sur A avec $\kappa_B \circ \varphi$. L'énoncé d'unicité de la question 3.3 permet de conclure.

4.2.2 *Montrer que si le morphisme $\varphi : F(A) \longrightarrow F(B)$ est surjectif, alors $\mathsf{card}(B) \leq \mathsf{card}(A)$. Pour cela, on pourra montrer que l'application linéaire $\hat{\varphi}$ est surjective.*

Solution. Par construction, l'image de κ_B contient une base de $V(B)$. Si φ est surjectif, alors l'image de $\kappa_B \circ \varphi$ contient une base de $V(B)$. Or $\kappa_B \circ \varphi = \hat{\varphi} \circ \kappa_A$, par conséquent l'image de $\hat{\varphi}$ contient une base de $V(B)$. Les propriétés classiques des applications linéaires permettent de conclure que $\hat{\varphi}$ est surjective.
Il s'ensuit que $\dim(V(A)) \geq \dim(V(B))$ et par conséquent $\mathsf{card}(A) \geq \mathsf{card}(B)$.

4.2.3 *Montrer que toutes les bases de $F(A)$ ont le même cardinal.*

Solution. Si X est une base de $F(A)$ et si B est un ensemble de même cardinal que X, alors par définition $F(A)$ et $F(B)$ sont isomorphes. La question précédente montre qu'alors $\mathsf{card}(A) = \mathsf{card}(B)$ et donc $\mathsf{card}(A) = \mathsf{card}(X)$. Donc toutes les bases de $F(A)$ ont $\mathsf{card}(A)$ éléments.

Le cardinal commun de toutes les bases de $F(A)$, à savoir $\mathsf{card}(A)$, est appelée le *rang de* $F(A)$. Si G est un groupe isomorphe à $F(A)$, on dit que G est un *groupe libre de rang* $\mathsf{card}(A)$. Si $\varphi\colon G \longrightarrow F(A)$ est un isomorphisme et si B est une partie de G telle que $\varphi(B)$ est une base de $F(A)$, on dit que B est une *base de* G.

Question 4.3 *Soit $A = \{a, b\}$, soit $C = \{c_1, \ldots, c_n\}$ un alphabet à n éléments ($n \geq 1$) et soit $\varphi\colon F(C) \longrightarrow F(A)$ le morphisme induit par l'application $c_i \longmapsto a^i b \bar{a}^i$ ($i \in \{1, \ldots, n\}$.*

4.3.1 *Montrer que si $i \in \{1, \ldots, n\}$ et k est un entier relatif non nul, alors $\varphi(c_i^k) = a^i b^k \bar{a}^i$. (Si $k < 0$, b^k dénote le mot $\bar{b}^{|k|}$.)*

Solution. On peut procéder par récurrence : vrai pour $k = 1$ par définition. Si $k \geq 1$ et $\varphi(c_i^k) = a^i b^k \bar{a}^i$, alors $\varphi(c_i^{k+1}) = \varphi(c_i^k) \odot \varphi(c_i) = (a^i b^k \bar{a}^i) \odot (a^i b \bar{a}^i) = \rho(a^i b^k \bar{a}^i a^i b \bar{a}^i) = a^i b^k b \bar{a}^i = a^i b^{k+1} \bar{a}^i$.

[La récurrence n'est pas nécessaire : on peut aussi dire que $\varphi(c_i^k)$ est la $k$ième puissance (pour l'opération $\odot$) de $\varphi(c_i)$, qui est égale à $\rho((a^i b \bar{a}^i)^k)$. Comme $\rho(\bar{a}^i a^i) = 1$, il suit que $\varphi(c_i^k) = \rho(a^i b^k \bar{a}^i) = a^i b^k \bar{a}^i$.]

Donc la formule est vraie pour tout $k \geq 1$. De plus, $\varphi(c_i^{-k}) = \varphi(c_i)^{-k} = (\varphi(c_i)^{-1})^k$. Or $\varphi(c_i)^{-1} = \overline{a^i b \bar{a}^i} = a^i \bar{b} \bar{a}^i$. Par le même raisonnement que ci-dessus, on montre que $\varphi(c_i^{-k}) = \rho(a^i \bar{b}^k \bar{a}^i) = a^i \bar{b}^k \bar{a}^i = a^i b^{-k} \bar{a}^i$.

4.3.2 *Montrer que φ est injectif.*

Solution. Soit $x \neq 1$ dans $F(C)$. Alors le mot réduit x s'écrit de façon unique sous la forme suivante, $x = c_{i_1}^{k_1} c_{i_2}^{k_2} \cdots c_{i_r}^{k_r}$, où chaque k_h est un entier non nul (positif ou négatif) et où $i_h \neq i_{h+1}$ pour tout $1 \leq h < r$.

D'après la question précédente, $\varphi(c_{i_h}^{k_h}) = a^{i_h} b^{k_h} \bar{a}^{i_h}$ pour tout h. Alors $\varphi(x)$ est l'image par ρ de la concaténation des $a^{i_h} b^{k_h} \bar{a}^{i_h}$. Notons que

$$\rho(\bar{a}^{i_h} a^{i_{h+1}}) = \begin{cases} a^{i_{h+1} - i_h} & \text{si } i_{h+1} \geq i_h \\ \bar{a}^{i_h - i_{h+1}} & \text{si } i_{h+1} < i_h, \end{cases}$$

ce que l'on peut résumer dans tous les cas par la formule $\rho(\bar{a}^{i_h} a^{i_{h+1}}) = a^{i_{h+1} - i_h}$. Mais alors

$$\varphi(x) = \rho\Big(a^{i_1} b^{k_1} a^{i_2 - i_1} b_2^k \cdots a^{i_r - i_{r-1}} b^{k_r} a^{-i_r}\Big).$$

Vu les hypothèses faites sur les k_h et les i_h, ce mot est réduit et donc égal à $\varphi(x)$. On en déduit immédiatement que si $x \in \ker \varphi$, alors x est le mot vide, c'est-à-dire que $\ker \varphi = \{1\}$ et donc φ est injectif.

4.3.3 *En déduire qu'un groupe libre de rang 2 admet comme sous-groupes des groupes libres de tout rang fini.*

Solution. Soit $H = \varphi(F(C))$: H est un sous-groupe de $F(A)$ et comme φ est injectif, H est isomorphe à $F(C)$. Finalement $F(A)$ est de rang 2 (puisque A a 2 éléments) ; de même, $F(C)$ est de rang n (n choisi arbitrairement) et donc H est de rang n.

On peut s'en tenir là, c'est-à-dire se contenter de montrer que $F(A)$ admet comme sous-groupes des groupes libres de tout rang fini. Si on veut être plus conforme au texte de la question, on considère un groupe libre de rang 2, disons G. Par définition, il est isomorphe à $F(A)$, soit $\psi\colon F(A) \longrightarrow G$ un isomorphisme. Si H est un sous-groupe de $F(A)$ qui est libre de rang n, alors $\psi(H)$ (qui est isomorphe à H) est un sous-groupe de G qui est libre de rang n.

5 – Représentations des groupes libres

Les questions de cette partie donnent deux *représentations* d'un groupe libre $F(A)$, c'est-à-dire des morphismes injectifs de $F(A)$ dans un autre groupe, moins abstrait.

Question 5.1 *Dans cette question, on suppose que $A = \{a, b\}$. Soit GL_2 le groupe des matrices carrées d'ordre 2 inversibles, à coefficients réels et soient*

$$\alpha = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \qquad \beta = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$$

Montrer qu'il existe un morphisme injectif φ de $F(A)$ dans GL_2, tel que $\varphi(a) = \alpha$ et $\varphi(b) = \beta$.

Indication. On pourra considérer les quatre régions du plan Y_a, $Y_{\bar{a}}$, Y_b et $Y_{\bar{b}}$ décrites ci-dessous, et leurs images par les applications linéaires α, α^{-1}, β et β^{-1}.

$$\begin{aligned} Y_a &= \{(x, y) \in \mathbb{R}^2 \mid xy \geq 0, |y| \leq |x|\} \\ Y_{\bar{a}} &= \{(x, y) \in \mathbb{R}^2 \mid xy \leq 0, |y| \leq |x|\} \\ Y_b &= \{(x, y) \in \mathbb{R}^2 \mid xy \geq 0, |x| \leq |y|\} \\ Y_{\bar{b}} &= \{(x, y) \in \mathbb{R}^2 \mid xy \leq 0, |x| \leq |y|\}. \end{aligned}$$

On comparera ensuite $Im(\varphi(u))$ et $Im(\varphi(c))$ lorsque $u \in F(A)$ est un mot réduit et c est la première lettre de u.

Solution. L'existence et l'unicité de φ sont déjà acquises et il faut montrer l'injectivité, c'est-à-dire montrer que $\ker \varphi = \{1\}$.

On vérifie d'abord que l'application linéaire α envoie Y_a, Y_b et $Y_{\bar{b}}$ dans Y_a, et $Y_{\bar{a}}$ dans $Y_{\bar{a}} \cup Y_b \cup Y_{\bar{b}}$. Réciproquement, α^{-1} envoie $Y_{\bar{a}}$, Y_b et $Y_{\bar{b}}$ dans $Y_{\bar{a}}$, et Y_a dans $Y_a \cup Y_b \cup Y_{\bar{b}}$.

De même β envoie Y_b, Y_a et $Y_{\bar{a}}$ dans Y_b et $Y_{\bar{b}}$ dans $Y_{\bar{b}} \cup Y_a \cup Y_{\bar{a}}$; et réciproquement β^{-1} envoie $Y_{\bar{b}}$, Y_a et $Y_{\bar{a}}$ dans $Y_{\bar{b}}$, et Y_b dans $Y_b \cup Y_a \cup Y_{\bar{a}}$.

(Note : c'est toujours la même formule : si $c \in \tilde{A}$, alors $\varphi(c)$ envoie trois régions, dont Y_c, dans Y_c et envoie $Y_{\bar{c}}$ dans trois régions.)

Une façon de procéder à ces vérifications est de calculer les images des vecteurs

$$u_{a,b} = (1, 1), \;\; u_{b,\bar{b}} = (0, 1), \;\; u_{a,\bar{a}} = (1, 0), \;\; u_{\bar{a},\bar{b}} = (1, -1)$$

qui sont sur les frontières entre les domaines Y_c, voir la figure 2.

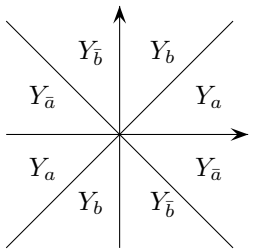


FIG. 2 – Les régions Y_a, $Y_{\bar{a}}$, Y_b et $Y_{\bar{b}}$

Soit alors u un mot réduit non vide et considérons sa dernière lettre c, $u = u'c$ avec $c \in \{a, b, \bar{a}, \bar{b}\}$, disons $c = a$. Comme $\varphi(a) = \alpha$, $\varphi(a)$ envoie $Y_a \cup Y_b \cup Y_{\bar{b}}$ dans Y_a. La dernière lettre de u', disons d, ne peut pas être un $\bar{a}$, donc $\varphi(d)$ envoie Y_a dans Y_d.

Une récurrence simple sur la longueur du mot u montre que $\varphi(u)$ envoie $Y_a \cup Y_b \cup Y_{\bar{b}}$ dans un unique Y_d (où d est la première lettre de u) et par conséquent $\varphi(u)$ n'est pas l'identité de $\mathbb{R}^2$. Ainsi $x \notin \ker\varphi$, $\ker\varphi = \{1\}$ et φ est injectif.

On appelle *série formelle sur A^* à coefficients entiers* une application R de A^* dans l'anneau $\mathbb{Z}$ des entiers relatifs. Il est commode de noter la série formelle R comme la somme formelle $R = \sum_{w \in A^*} R_w w$, où $R_w = R(w)$ est l'image de w par l'application R. On note $\mathbb{Z}[\![A]\!]$ l'ensemble des séries formelles sur A^* à coefficients entiers.

Si w est un mot, on notera simplement w la série formelle dont tous les coefficients sont nuls, sauf celui associé à w, qui vaut 1. On définit une addition et une multiplication dans $\mathbb{Z}[\![A]\!]$ de la façon suivante. Soient $R, S \in \mathbb{Z}[\![A]\!]$, avec $R = \sum_{w \in A^*} R_w w$ et $S = \sum_{w \in A^*} S_w w$. On pose

$$\begin{aligned} R + S &= \sum_{w \in A^*} (R_w + S_w) w \\ RS &= \sum_{w \in A^*} \Big(\sum_{uv = w} R_u S_v \Big) w. \end{aligned}$$

On notera que dans la définition du produit RS, le coefficient de w, c'est-à-dire la somme des $R_u S_v$ tels que $uv = w$ est une somme finie : en effet, pour chaque w, il n'existe qu'un nombre fini de mots u, v tels que $uv = w$.

On admettra que l'addition et la multiplication de $\mathbb{Z}[\![A]\!]$ sont associatives et que la multiplication est distributive par rapport à l'addition, si bien que $\mathbb{Z}[\![A]\!]$ est un anneau. Attention : l'addition est commutative mais la multiplication ne l'est pas. On note $U(A)$ l'ensemble des éléments inversibles de $\mathbb{Z}[\![A]\!]$, c'est-à-dire l'ensemble des éléments $u \in \mathbb{Z}[\![A]\!]$ tels qu'il existe $v \in \mathbb{Z}[\![A]\!]$ satisfaisant $uv = vu = 1$. On admettra que $U(A)$, muni de la multiplication, est un groupe.

Question 5.2 *Montrer que pour chaque $a \in A$, la série formelle $1+a$ appartient à $U(A)$.*

Solution. Soit $u_a = \sum_{n\geq 0}(-1)^n a^n$. On vérifie que les produits $u_a(1+a)$ et $(1+a)u_a$ sont tous deux égaux à 1.

Question 5.3 *Montrer qu'il existe un morphisme injectif φ de $F(A)$ dans $U(A)$, tel que $\varphi(a) = 1 + a$ pour chaque $a \in A$.*

Indication : Pour cela, on pourra considérer l'image $\varphi(w)$ d'un mot réduit $w \in F(A)$: on peut regrouper dans l'écriture de w les occurrences consécutives d'une même lettre, c'est-à-dire écrire $w = c_1^{n_1} c_2^{n_2} \cdots c_r^{n_r}$ où chaque n_h est un entier non nul (positif ou négatif), chaque $c_h \in A$ et où $c_h \neq c_{h+1}$ pour tout $1 \leq h < r$. Quel est alors le coefficient de $c_1 c_2 \cdots c_r$ dans $\varphi(w)$?

Solution. L'existence et l'unicité de le morphisme φ sont acquises et il faut montrer son injectivité, c'est-à-dire que $\ker\varphi = \{1\}$.

On observe d'abord que si $n > 0$ et $a \in A$, alors les coefficients de 1 et a dans $\varphi(a^n) = (1+a)^n$ sont respectivement 1 et n. On observe aussi que ces coefficients dans $\varphi(a^{-n}) = u_a^n$ sont respectivement 1 et $-n$ (comme dans la question précédente, $u_a = (1+a)^{-1} = \sum_{n\geq 0}(-1)^n a^n$).

Soit alors w un mot réduit non vide, que l'on peut écrire sous la forme $w = c_1^{n_1} c_2^{n_2} \cdots c_r^{n_r}$, où chaque n_h est un entier non nul (positif ou négatif), chaque $c_h \in A$ et où $c_h \neq c_{h+1}$ pour tout $1 \leq h < r$. Alors le coefficient de $c_1 c_2 \cdots c_r$ dans $\varphi(w)$ est égal à $n_1 \cdots n_r$ et par conséquent n'est pas nul. Il en découle que $w \notin \ker\varphi$ et donc que $\ker\varphi = \{1\}$.

6 – Mots cycliquement réduits et conjugaison

Soit $u \in \tilde{A}^*$. On dit que le mot u est *cycliquement réduit* si u est de longueur nulle, ou si $u = a_1 a_2 \cdots a_n$ ($n \geq 1$ et $a_i \in \tilde{A}$ pour tout i) et on a $a_{i+1} \neq \bar{a}_i$ pour $i = 1, \ldots, n-1$ et $a_1 \neq \bar{a}_n$. On observera que u est cycliquement réduit si et seulement si le mot u^2 est réduit.

Question 6.1 *Montrer que tout mot réduit $u \in F(A)$ admet une unique factorisation de la forme $u = \bar{w}vw$, où v est cycliquement réduit.*

Solution. Si $|u| \leq 1$, alors u est réduit et cycliquement réduit et la décomposition de u est donnée par $w = 1$ et $v = u$. On suppose maintenant que $u = a_1 \cdots a_n$ avec $n \geq 1$.

Si $u = \bar{w}vw$, alors pour tout $i \leq |w|$, on a $a_i = \bar{a}_{n-i+1}$. Si de plus v est cycliquement réduit et $|w| = j$, on a $a_{j+1} \neq \bar{a}_{n-j}$. On en déduit l'unicité de la factorisation, si elle existe, puisque la longueur du facteur w est entièrement déterminée par u.

Quant à l'existence, elle suit de même : soit j le plus grand entier tel que $0 \leq j \leq n/2$ et $a_i = \bar{a}_{n-i+1}$ pour tout $i \leq j$, soit $w = a_{n-j+1} \cdots a_n$ (le mot vide si $j = 0$) et $v = a_{j+1} \cdots a_{n-j}$ (le mot vide si $j = n/2$). Alors v est cycliquement réduit, $\bar{w} = a_1 \cdots a_j$ (le mot vide si $j = 0$) et $u = \bar{w}vw$.

On dit qu'un groupe G est *sans torsion* si, pour tout $x \in G$ différent de 1_G, on a $x^n \neq 1_G$ pour tout entier $n > 0$.

Question 6.2 *Déduire de la question 6.1 que $F(A)$ est un groupe sans torsion.*

Solution. Soit $u \neq 1$ un élément de $F(A)$ et soit $u = \bar{w}vw$ sa décomposition selon la question 6.1. On observe alors que pour tout $n \geq 1$, le mot $\bar{w}v^n w$ est réduit et on vérifie sans peine que $u^n = \bar{w}v^n w$. Il s'ensuit que $u^n \neq 1$. On a ainsi démontré que $F(A)$ est sans torsion.

Soient $u, v \in F(A)$. On dit que u et v sont *conjugués* et on note $u \equiv v$ s'il existe un mot $w \in F(A)$ tel que $v = \bar{w} \odot u \odot w$.

Question 6.3 *Montrer que la relation de conjugaison $\equiv$ est une relation réflexive, symétrique et transitive.*

Solution. Réflexivité : $u = \rho(1u1) = \bar{1} \odot u \odot 1$ (ou $u = \rho(\bar{u}uu) = \bar{u} \odot u \odot u$).

Symétrie : si $u = \bar{w} \odot v \odot w$, alors $w \odot u \odot \bar{w} = w \odot \bar{w} \odot v \odot w \odot \bar{w} = v$. Et comme $\bar{\bar{w}} = w$, la symétrie est démontrée.

Transitivité : si $v = \bar{w} \odot u \odot w$ et $y = \bar{x} \odot v \odot x$, alors $y = \bar{x} \odot (\bar{w} \odot u \odot w) \odot x = (\bar{x} \odot \bar{w}) \odot u \odot (w \odot x)$. Si $z = w \odot x$, on a $z = \rho(wx)$, donc $\bar{z} = \overline{\rho(wx)} = \rho(\overline{wx}) = \rho(\bar{x}\ \bar{w}) = \bar{x} \odot \bar{w}$. Par conséquent, $y = \bar{z} \odot u \odot z$, ce qu'il fallait démontrer.

Question 6.4 *Soient u et v deux mots cycliquement réduits non vides. Montrer que u et v sont conjugués si et seulement si v est une permutation cyclique de u, c'est-à-dire s'il existe des mots r, s tels que $u = rs$ et $v = sr$.*

Solution. Si $u = rs$ et $v = sr$, alors $\bar{s} \odot v \odot s = \rho(\bar{s}vs) = \rho(\bar{s}srs) = \rho(rs) = u$ (la dernière égalité puisqu'on suppose que u est réduit). Par conséquent $u \equiv v$.

Réciproquement, supposons que u, v sont cycliquement réduits et non vides, et que $u \equiv v$: il existe $w \in F(A)$ tel que $v = \bar{w} \odot u \odot w = \rho(\bar{w}uw)$ et on peut supposer w réduit et de longueur minimale.

Si $w = 1$, alors $v = u$ et on peut prendre $r = u$ et $s = 1$. Supposons maintenant que w n'est pas le mot vide. Comme u est cycliquement réduit, les mots $\bar{w}u$ et uw ne peuvent pas être simultanément non réduits ($\bar{w}u$ est non réduit si et seulement si la première lettre de u est la même que la première lettre de w, disons a, mais dans ce cas, la dernière lettre de u n'est pas $\bar{a}$, donc wu est réduit). En revanche, comme v est cycliquement réduit et $v = \rho(\bar{w}uw)$, il faut bien qu'il y ait de la réduction. Supposons sans perte de généralité que $\bar{w}u$ n'est pas réduit et que uw l'est.

La réduction de $\bar{w}uw$ doit "consommer" tout w sans quoi $\rho(\bar{w}uw)$ ne sera pas cycliquement réduit. Il s'ensuit que w est un préfixe de uw, c'est-à-dire que $uw = wu'$ pour un mot u' (de même longueur que u).

Premier cas : $|w| < |u|$. Alors il existe w' tel que $u = ww'$ et $v = \rho(\bar{w}uw) = \rho(\bar{w}ww'w) = \rho(w'w)$. Comme $u = ww'$ est cycliquement réduit, $w'w$ est réduit et donc $v = w'w$. Il suffit de poser $r = w$ et $s = w'$ pour conclure.

Second cas : $|w| \geq |u|$. Alors $w = uu''$ et $v = \rho(\bar{u}''\bar{u}uuu'') = \rho(\bar{u}''uu'')$. Par minimalité de la longueur de w, on conclut à l'absurdité.

Question 6.5 *Donner un algorithme pour décider si deux mots $u, u' \in F(A)$ sont conjugués.*

Solution. La première étape de l'algorithme consiste à calculer la décomposition selon la question 6.1 des mots u et v.
Pour le mot u, ce calcul est effectué récursivement de la façon suivante : on lit la première et la dernière lettre de w, soient a et b (dans $\tilde{A}$). Si $b \neq \bar{a}$, alors la décomposition est donnée par $w = 1$ et $v = u$. Si $b = \bar{a}$, on calcule la décomposition (w', v') du mot obtenu à partir de u en supprimant la première et la dernière lettre, et la décomposition de u est donnée par $w = aw'$ et $v = v'$. Appelons *cœur cycliquement réduit* de u le mot v.
La seconde étape est de considérer les cœurs cycliquement réduits v et v' de u et u'. Alors u et v sont conjugués si et seulement si u' et v' sont conjugués et d'après la question précédente, c'est le cas si et seulement si v' est une permutation cyclique de u', ce qui se vérifie directement.

7 – Groupe fondamental d'un graphe

On définit un *graphe orienté A-étiqueté* (on dira simplement un *A-graphe*) comme une paire $\Gamma = (V, E)$ où V est un ensemble fini, appelé ensemble des *sommets*, et E est une partie de $V \times A \times V$, appelée ensemble des *arêtes*. Il est commode de représenter une arête (u, a, v) par une flèche du sommet u vers le sommet v étiquetée par la lettre a, comme dans la figure 3.

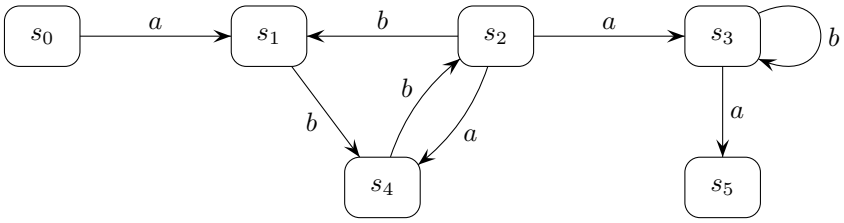


Fig. 3 – Un A-graphe à 6 sommets et 8 arêtes

Si $e = (u, a, v) \in E$, on note $\bar{e}$ le triplet $\bar{e} = (v, \bar{a}, u)$. Soit $\tilde{E} = E \cup \{\bar{e} \mid e \in E\}$. Un *chemin* dans le A-graphe Γ est une suite finie de la forme

$$p = (u_0, a_1, u_1)(u_1, a_2, u_2) \cdots (u_{n-1}, a_n, u_n),$$

($n \geq 1$) où chaque $(u_{i-1}, a_i, u_i) \in \tilde{E}$. On dit alors que p est un chemin de u_0 à u_n, de longueur n et d'*étiquette* le mot $a_1 a_2 \cdots a_n \in \tilde{A}^*$. Dans le A-graphe de la figure 3, il existe par exemple des chemins de s_0 à s_2 étiquetés $a\bar{b}$, abb, $ab\bar{a}$, $ab\bar{a}ab$ (il en existe une infinité d'autres), ainsi que des chemins étiquetés $ab\bar{a}b\bar{a}$ et $a\bar{b}aa\bar{a}b\bar{a}b\bar{a}$ de s_0 à s_0.

Pour chaque sommet u, on considère par convention qu'il existe un chemin de longueur 0 de u à u, appelé *chemin vide en u*.

On dit qu'un chemin p est *réduit* si p ne comporte pas deux arêtes consécutives de la forme $(u, a, v)(v, \bar{a}, u)$ avec $(u, a, v) \in \tilde{E}$. Enfin, on dit que le graphe Γ est *réduit* si, pour tout sommet u et toute lettre $a \in A$, E contient au plus une arête de la forme (u, a, v) et au plus une arête de la forme (v, a, u). Le A-graphe de la figure 3 n'est pas réduit puisque deux arêtes étiquetées a partent du sommet s_2.

Dans toute cette partie, on considère un A-graphe fini réduit $\Gamma = (V, E)$.

Question 7.1 *Montrer que l'étiquette d'un chemin est réduite si et seulement si le chemin est réduit.*

> **Solution**. Soit p un chemin d'étiquette x. Si x n'est pas réduit, $x = ya\bar{a}z$ avec $y, z \in \tilde{A}^*$ et $a \in \tilde{A}$. Les arêtes correspondantes aux lettres a et $\bar{a}$ sont de la forme $(u, a, v)(v, \bar{a}, w)$. Supposons que $a \in A$: alors E contient les arêtes (u, a, v) et (w, a, v) et comme le graphe est réduit, on a $u = w$, ce qui contredit le fait que le chemin p est réduit. (Même raisonnement si $\bar{a} \in A$.)
> La réciproque est plus facile : si le chemin n'est pas réduit, il contient deux arêtes consécutives de la forme $(u, a, v)(v, \bar{a}, u)$, donc x contient deux lettres consécutives de la forme $a\bar{a}$, ce qui contredit le fait que x est réduit.

Question 7.2 *Montrer que si x est l'étiquette d'un chemin du sommet s au sommet t, alors $\rho(x)$ est l'étiquette d'un chemin réduit de s à t.*

> **Solution**. Supposons que x est l'étiquette d'un chemin p de s à t et que $x \xrightarrow{1} y$. Alors $x = x'a\bar{a}x''$ avec $a \in \tilde{A}$ et $y = x'x''$. Alors p se factorise en $p = p'(u, a, v)(v, \bar{a}, w)p''$, où p' est d'étiquette x' et p'' d'étiquette x''. Comme Γ est réduit, on a $u = w$ et donc $p'p''$ est aussi un chemin, de s à t, d'étiquette $x'x'' = y$. On en déduit, par itération (ou par une récurrence sur la longueur de la dérivation de x à $\rho(x)$) que $\rho(x)$ aussi est l'étiquette d'un chemin de s à t.

Si $s_0 \in V$ est un sommet de Γ, on note $G(\Gamma, s_0)$ l'ensemble des étiquettes des chemins réduits de s_0 à s_0.

Question 7.3 *Montrer que $G(\Gamma, s_0)$ est un sous-groupe de $F(A)$ (c'est-à-dire que $G(\Gamma, s_0)$ contient les produits de ses éléments et contient les inverses de ses éléments).*

> **Solution**. Soient $x, y \in G(\Gamma, s_0)$ et soient p, q des chemins de s_0 à s_0, d'étiquettes respectives x et y. Le chemin $\bar{p}$ va encore de s_0 à s_0 et est étiqueté $\bar{x}$. Donc $\bar{x} \in G(\Gamma, s_0)$.
> Comme la concaténation pq est un chemin de s_0 à s_0, d'étiquette xy, il existe un chemin de s_0 à s_0 d'étiquette $x \odot y = \rho(xy)$ d'après la question 7.2 et donc $x \odot y \in G(\Gamma, s_0)$.

On dit que le A-graphe Γ est *connexe* si, pour tous sommets u, v de Γ, il existe au moins un chemin de u à v (et donc au moins un chemin réduit, d'après la question 7.2). On dit que Γ est une *forêt* si, pour tous sommets u, v de Γ, il existe au plus un chemin réduit de u à v. Une forêt connexe est appelée un *arbre*.

Question 7.4 *Calculer $G(\Gamma, s_0)$ lorsque Γ est une forêt.*

> **Solution**. Soit $x \in G(\Gamma, s_0)$ et soit p un chemin de s_0 à s_0 d'étiquette x. Si $x \neq 1$, soit $a \in \tilde{A}$ la première lettre de x et soit x' tel que $x = ax'$. La première arête du chemin p est de la forme (s_0, a, u) et x' étiquette un chemin réduit de u à s_0. Donc $\bar{x}'$ étiquette un chemin réduit de s_0 à u et par définition d'une forêt, ce chemin coïncide avec l'arête (s_0, a, u). Par conséquent $x' = \bar{a}$, ce qui contredit le fait que x est réduit.
> Donc $G(\Gamma, s_0)$ ne contient pas d'élément non trivial, $G(\Gamma, s_0) = \{1\}$.

Pour le reste de cette partie, le A-graphe fini réduit $\Gamma = (V, E)$ est supposé connexe et on fixe un sommet $s_0 \in V$ de Γ.

Si $V' \subseteq V$ et $E' \subseteq E \cap (V' \times A \times V')$, on dit que le graphe $\Gamma' = (V', E')$ est un *sous-graphe* de Γ, et qu'il est *couvrant* si $V = V'$. On parle enfin de *sous-arbre couvrant* si de plus Γ' est un arbre.

Question 7.5 *Montrer que* Γ *admet un sous-arbre couvrant et donner un algorithme de calcul d'un tel arbre.*

Solution. Plusieurs solutions sont possibles. La première donnée ci-dessous, est plus efficace (mais ce critère ne fait pas partie de la question), la seconde est plus facile à justifier.

L'algorithme construit une suite de sous-graphes de Γ comme suit : on part du sous-graphe $T' = (V', E')$ consistant en un seul sommet, s_0, et pas d'arêtes. A chaque étape, on passe en revue les arêtes de E jusqu'à ce qu'on en trouve une, disons (u, a, v), telle que $u \in V'$ et $v \notin V'$ (cas 1) ou $u \notin V'$ et $v \in V'$ (cas 2) ; on ajoute alors v dans le cas 1, u dans le cas 2 à V' ; on ajoute aussi (u, a, v) à E'.

Pour justifier cet algorithme, on va montrer qu'il ne s'arrête que lorsque T' contient tous les sommets de Γ, et qu'à chaque étape, T' est un arbre.

S'il existe un sommet $v \in V$ qui n'est pas dans V' et comme Γ est connexe, il existe un chemin réduit de s_0 à v. Soit u le premier sommet visité par ce chemin qui est hors de V' et soit (u', a, u) l'arête (dans $\tilde{E}$) qui mène à u. Alors $u' \in V'$ et $(u', a, u) \notin \tilde{E}'$. Ainsi, on a montré que si T' n'est pas couvrant, alors il existe une arête de E avec une extrêmité dans V' et l'autre hors de V'.

Soit maintenant T' le sous-arbre construit à une étape de l'algorithme et soit une arête $e = (w, a, w') \in E$ dont exactement une des extrêmités est dans V', disons sans perte de généralité que $w \in V'$ et $w' \notin V'$. On construit $T'' = (V'', E'')$ en ajoutant à V' le sommet w' et à E' l'arête e. Montrons que le T'' est encore un arbre. Sa connexité est immédiatement établie puisque T' est connexe et le nouveau sommet est relié à un sommet de T' par une arête. Si T'' n'est pas un arbre, il existe des états u et u' et des chemins réduits distincts p et q dans T'' de u à u'. Si $u \notin V'$, p et q commencent par $\bar{e}$, $u = w$, $p = \bar{e}p'$, $q = \bar{e}q'$ et p', q' sont des chemins réduits dans T'' de w à u'. De même, si $u' \notin V'$, p et q sont de la forme $p = p'e$ et $q = q'e$ avec p', q' des chemins réduits de u à w.

Donc on peut se ramener au cas où u et u' sont dans T'. Factorisons p en faisant apparaître les occurrences de e et $\bar{e}$: $p = p_0 e_1 p_1 \cdots e_n p_n$ avec les p_i des chemins vides ou dans T' et les e_i dans $\{e, \bar{e}\}$. Comme e n'est pas une boucle, le fait que p est réduit impose que p_i est non vide pour $1 \leq i < n$. Mais les chemins dans T' ont leurs deux extrêmités dans V', donc si $1 \leq i < n$, alors $e_{i-1} = \bar{e}$ et $e_i = e$ et p_i est un chemin reduit dans T' de w à w : nécessairement vide. Face à cette contradiction, on déduit que $n \leq 1$. Si $n = 1$, alors $e_1 = e$ et p_1 va de w' à un sommet de V' : contradiction. Donc $n = 0$, c'est-à-dire que p est un chemin dans T'. De même pour q, et donc $p = q$.

Autre algorithme : on part de $T' = \Gamma$. A chaque étape, on cherche une arête e qui figure dans un cycle de T', et on modifie T' en retirant cette

arête. A la fin, on a bien tous les sommets (puisqu'on n'en supprime jamais) et pas de cycle, donc un arbre couvrant – à condition que la connexité soit préservée. Mais si T'' est obtenu à partir de T en supprimant une arête (w, a, w') de T', il existe un chemin f dans T' de w à w' disjoint de cette arête, donc un chemin dans T''. Alors si $u, u' \in V$ et si p est un chemin de T' de u à u', on remplace chaque occurrence de e (resp. $\bar{e}$) dans p par f (resp. $\bar{f}$) et on obtient un chemin dans T'' de u à u'.

Soit $T = (V, E_T)$ un sous-arbre couvrant de Γ. Pour tout sommet s de Γ, soit x_s l'étiquette de l'unique chemin réduit de s_0 à s dans T. Pour chaque arête $e = (s, a, t)$ de Γ n'appartenant pas à T, posons $b_e = x_s a \overline{x_t}$. On notera que par construction, b_e est un mot réduit.

Question 7.6 *Montrer que tout élément de $G(\Gamma, s_0) \setminus \{1\}$ est le produit, dans $F(A)$, de mots de la forme b_e ou $\overline{b_e}$.*

On pourra pour cela considérer un élément $x \in G(\Gamma, s_0)$, un chemin réduit p d'étiquette x de s_0 à s_0, une factorization $p = p_0 e_1 p_1 \cdots e_r p_r$ où les p_i sont des chemins réduits dans T et les e_i sont des éléments de $\tilde{E} \setminus \tilde{E}_T$, puis montrer que l'étiquette de p_i $(0 < i < r)$ est égale à $\bar{x}_t x_s$ où t est le sommet final de e_i et s le sommet initial de e_{i+1}.

Solution. Soit $x \in G(\Gamma, s_0)$ et soit p un chemin réduit d'étiquette x de s_0 à s_0. Le chemin p est composé d'arêtes de $\tilde{E}_T$ et d'arêtes hors de cet ensemble. Si p ne comporte pas d'arêtes de $\tilde{E} \setminus \tilde{E}_T$, alors p est un chemin de T, donc est le chemin vide en s_0 (par définition des arbres), et finalement $x = 1$. Sinon, p se décompose en $p = p_0 e_1 p_1 \cdots e_r p_r$, où $r \geq 1$, les p_i sont des chemins réduits dans T et les e_i sont des éléments de $\tilde{E} \setminus \tilde{E}_T$. Si $e_i = (s_i, a_i, t_i)$ et si x_i est l'étiquette de p_i, alors $x = x_0 a_1 x_1 \cdots a_r x_r$ et chaque p_i est le chemin réduit (unique) dans T de t_{i-1} à s_i (p_0 de s_0 à s_1 et p_r de t_r à s_0).

En particulier, $p_0 = p_{s_1}$, $x_0 = x_{s_1}$, $p_r = \bar{p}_{t_r}$ et $x_r = \bar{x}_{t_r}$. Pour $1 \leq i < r$, notons que $p_{t_i} p_i \bar{p}_{s_{i+1}}$ est un chemin dans T de s_0 à s_0. Chaque réduction de ce chemin (élimination d'une consécution $e\bar{e}$ ou $\bar{e}e$, $e \in E$) et de son étiquette donne encore l'étiquette d'un chemin de s_0 à s_0 et comme T est un arbre, on en déduit que l'étiquette de ce chemin, $x_{t_i} x_i \bar{x}_{s_{i+1}}$, se réduit en le mot vide dans $F(A)$, c'est à dire que $x_i = \bar{x}_{t_i} \odot x_{s_{i+1}}$.

Par conséquent, $x = (x_{s_1} a_1 \bar{x}_{t_1}) \odot \cdots \odot (x_{s_r} a_r \bar{x}_{t_r})$. Finalement, on observe que si $e_i \in E_T$, alors $x_{s_i} a_i \bar{x}_{t_i} = b_{e_i}$ et si $e_i \in \tilde{E}_T \setminus E_T$, alors $x_{t_i} \bar{a}_i \bar{x}_{s_i} = \bar{b}_{\bar{e}_i}$, ce qui conclut la preuve.

Question 7.7 *Soit $r = \mathsf{card}(E \setminus E_T)$. Montrer que $G(\Gamma, s_0)$ est isomorphe à un groupe libre de rang r.*

Solution. Soit $E \setminus E_T = \{e_1, \ldots, e_r\}$, soit $Y = \{y_1, \ldots, y_r\}$ un alphabet de cardinal r et soit $\varphi : F(Y) \longrightarrow F(A)$ le morphisme induit par l'application $y_i \longmapsto b_{e_i}$. L'image de ce morphisme est le sous-groupe de $F(A)$ engendré par les b_{e_i}, c'est-à-dire $G(\Gamma, s_0)$ d'après la question précédente. Il suffit par conséquent de montrer que φ est injectif.

Par commodité, posons $\psi : F(Y) \longrightarrow F(E)$ le morphisme induit par l'application $y_i \longmapsto e_i$. Supposons que $y \in F(Y)$, $y \neq 1$ et $\varphi(y) = 1$. Disons

$y = z_1 \cdots z_n$ avec les $z_h \in \tilde{Y}$ et $z_h \neq \bar{z}_{h+1}$. Posons $(s_h, a_h, t_h) = \psi(z_h)$. Alors $\varphi(y) = \rho(x_{s_1} a_1 \bar{x}_{t_1} x_{s_2} \cdots a_n \bar{x}_{t_n})$. Soit alors $w_h = \rho(\bar{x}_{t_h} x_{s_{h+1}})$: on a donc $\varphi(y) = \rho(x_{s_1} a_1 w_1 a_2 \cdots w_{r-1} a_n \bar{x}_{t_n})$. Or ce dernier mot est l'étiquette d'un chemin réduit puisque les $\psi(z_h)$ ne sont pas dans T, alors que les x_h sont des étiquettes de chemins réduits dans T. Donc $\varphi(y) = x_{s_1} a_1 w_1 a_2 \cdots w_{r-1} a_n \bar{x}_{t_n}$, de longueur au moins n.

8 – Sous-groupes d'un groupe libre

Dans cette partie, on va montrer que tout sous-groupe finiment engendré d'un groupe libre est libre.

Soit $\mathcal{A} = (\Gamma, s_0)$ la paire consistant en un A-graphe $\Gamma = (V, E)$ et un sommet $s_0 \in V$ de Γ. On note $L(\mathcal{A})$ l'ensemble des étiquettes des chemins de s_0 à s_0 dans le A-graphe (V, E) et $\rho(L(\mathcal{A})) = \{\rho(u) \mid u \in L(\mathcal{A})\}$.

Si Γ n'est pas réduit, il existe deux arêtes de E de la forme (u, a, v) et (u, a, v'), ou bien (v, a, u) et (v', a, u). Soit alors $\mathcal{B}$ la paire $\mathcal{B} = (\Delta, t_0)$ obtenue à partir de $\mathcal{A}$ en "fusionnant" les sommets v et v'. Formellement, on définit $\Delta = (W, F)$ et t_0 de la façon suivante : l'ensemble W des sommets de Δ est $W = V \setminus \{v, v'\} \cup \{w\}$ où w est un nouveau symbole n'appartenant pas à V ; et son ensemble d'arêtes F est obtenu à partir de E en remplaçant partout v et v' par w. Le sommet t_0 est égal à s_0 si $s_0 \neq v, v'$, à w sinon. On dit alors que $\mathcal{A}$ *se réduit en une étape en* $\mathcal{B}$, noté $\mathcal{A} \xrightarrow{1} \mathcal{B}$.

On dit que la paire $\mathcal{A} = (\Gamma, s_0)$ est *réduite* si le A-graphe Γ est réduit.

Question 8.1 *Montrer que si* $\mathcal{A} \xrightarrow{1} \mathcal{B}$*, alors*

$$L(\mathcal{A}) \subseteq L(\mathcal{B}) \text{ et } \rho(L(\mathcal{A})) = \rho(L(\mathcal{B})).$$

Solution. Sans perte de généralité, on suppose que $\mathcal{B} = (\Delta, t_0)$ est construit à partir de $\mathcal{A} = (\Gamma, s_0)$ en considérant la paire d'arêtes $e = (u, a, v)$ et $e' = (u, a, v')$ et en fusionnant les sommets v et v'. Soit p un chemin de Γ de s_0 à s_0. On factorise p pour faire apparaître les successions $\bar{e}e'$ ou $\bar{e}'e$: $p = p_1 q_1 p_2 \cdots q_r p_r$ $(r \geq 0)$, où chaque q_i est égal soit à $\bar{e}e'$, soit à $\bar{e}'e$ et les p_i ne comportent pas de telles successions. Alors $p_1(\bar{e}e)p_2(\bar{e}e)\cdots(\bar{e}e)p_r$ est un chemin de t_0 à t_0 dans Δ (après avoir renommé les occurrences de v ou v' en w), de même étiquette que p. Donc $L(\mathcal{A}) \subseteq L(\mathcal{B})$ et bien sûr, $\rho(L(\mathcal{A})) \subseteq \rho(L(\mathcal{B}))$.

Soit maintenant p un chemin de t_0 à t_0 dans Δ. On factorise p pour faire apparaître les passages par w : $p = p_0 p_1 \cdots p_r$ où $q_i = f$ ou $\bar{f}$ et p_i est sans f ou $\bar{f}$. En particulier, les p_i sont des chemins de w à w (de s_0 à w pour p_0 et de w à s_0 pour p_r). Pour chaque p_i, le même chemin existe dans Γ de v ou v' à v ou v'. Si bien qu'il existe un chemin p'_i dans Γ de v à v, égal à l'un des chemins p_i, $\bar{e}e'p_i$, $p_i\bar{e}'e$ ou $\bar{e}e'p_i\bar{e}'e$. (On ajuste cet énoncé pour $i = 0$ et $i = r$.) Et alors $p' = p'_0 p'_1 \cdots p'_r$ est un chemin dans Γ, de s_0 à s_0. Finalement, il est clair que si x est l'étiquette de p et x' est l'étiquette de p', alors $x' \xrightarrow{\infty} x$, donc $\rho(x') = \rho(x)$ et ainsi, $\rho(L(\mathcal{B})) \subseteq \rho(L(\mathcal{A}))$.

Question 8.2 *Montrer que si* G *est le sous-groupe de* $F(A)$ *engendré par les mots* $h_1, \ldots, h_n \in F(A)$*, alors* G *est un groupe libre.*

Indication. Pour cela on pourra construire une paire $\mathcal{A} = (\Gamma, s_0)$ telle que $G = \rho(L(\mathcal{A}))$, puis réduire $\mathcal{A}$.

Solution. On commence par construire une paire $\mathcal{A} = (\Gamma, s_0)$ de la façon suivante. On commence en considérant le A-graphe Γ ayant un seul sommet, s_0 et aucune arête. Ensuite, pour chaque $1 \leq i \leq n$, on ajoute à V (m'ensemble des somments) $|h_i| - 1$ nouveaux sommets et $|h_i|$ nouvelles arêtes entre ces sommets et s_0 de telle façon que ces sommets et arêtes constituent un chemin (réduit) de s_0 à s_0 d'étiquette h_i.

On vérifie alors que $G = \rho(L(\mathcal{A}))$. Si $g \in G$, alors g est un produit de la forme $g = k_{i_1} \odot \cdots \odot k_{i_r}$ où $k_j \in \{h_j, \bar{h}_j\}$. On a donc $g = \rho(k_{i_1} \cdots k_{i_r})$. Il existe, par construction, un chemin de s_0 à s_0 dans Γ d'étiquette $k_{i_1} \cdots k_{i_r}$. Par conséquent, $k_{i_1} \cdots k_{i_r} \in L(\mathcal{A})$ et $g \in \rho(L(\mathcal{A}))$.

Réciproquement, soit p un chemin de s_0 à s_0 dans Γ. On factorise p selon les visites de s_0 : $p = p_1 \cdots p_m$, où chaque p_i est un chemin de s_0 à s_0, qui ne visite pas ce sommet hors de ses extrêmités : ainsi ce chemin est entièrement contenu dans l'une des boucles h_i et si x_i est l'étiquette de p_i, alors $\rho(x_i) \in \{1, h_i, \bar{h}_i\}$. Par conséquent, si x est l'étiquette de p, alors $\rho(x) = \rho(\rho(x_1) \cdots \rho(x_m)) = \rho(x_1) \odot \cdots \odot \rho(x_m) \in G$.

Posons $\mathcal{A} = \mathcal{A}_0$. On construit comme ci-dessous une suite finie $\mathcal{A}_i$ ($0 \leq i \leq r$) de paires tels que $\rho(L(\mathcal{A}_i)) = G$ pour tout i et $\mathcal{A}_r$ est réduit. Si $\mathcal{A}_i$ n'est pas réduit, on choisit une paire d'arêtes qui manifestent la non réduction, on construit $\mathcal{A}_{i+1}$ tel que $\mathcal{A}_i \xrightarrow{1} \mathcal{A}_{i+1}$ et on en déduit par la question 8.1 que $\rho(L(\mathcal{A}_{i+1})) = \rho(L(\mathcal{A}_i)) = G$. Le nombre de sommets diminue à chaque étape, donc le processus termine.

On a maintenant une paire réduite $\mathcal{B} = (\Gamma, s_0)$ tel que $\rho(L(\mathcal{B}))$ est égal à G. Mais la question 7.2 montre que si $u \in L(\mathcal{B})$, alors $\rho(u) \in L(\mathcal{B})$, donc $\rho(L(\mathcal{B})) \subseteq L(\mathcal{B})$ et par conséquent, $\rho(L(\mathcal{B})) = G(\Gamma, s_0)$ et la question 7.7 permet de conclure.

Question 8.3 *Soient $h_1, \ldots, h_n$ des éléments de $F(A)$ et soit G le sous-groupe de $F(A)$ qu'ils engendrent. Donner un algorithme pour trouver une base de G et en évaluer la complexité.*

Solution. L'algorithme de construction d'un automate réduit (Γ, s_0) tel que $G(\Gamma, s_0) = G$ est décrit dans la réponse à la question précédente. Ensuite on construit un arbre couvrant T de Γ. Pour chaque sommet s, on calcule le mot réduit qui étiquette un chemin dans T de s_0 à s. Et enfin, pour chaque arête $e = (s, a, t)$ dans E et pas dans T, on calcule $b_e = x_s a \bar{x}_t$. Les b_e ainsi construits forment une base de G.