Ce problème porte sur l'application de la théorie des automates au calcul d'invariants de certains objets algébriques, les sous-groupes du groupe libre.

Chaque question peut être traitée en admettant les résultats des questions précédentes, ce qui permet de les aborder dans un ordre différent de leur ordre d'apparition dans le sujet.

Définitions, notations et rappels

Dans tout le problème, A désigne un alphabet, c'est-à-dire un ensemble fini non vide. Le monoïde libre sur A, noté A^*, est l'ensemble des mots écrits sur l'alphabet A. On rappelle en particulier l'existence d'un unique mot de longueur 0, le mot vide, noté 1.

On rappelle qu'un automate déterministe sur A est un quadruplet $\mathcal{A} = (Q, I, \delta, F)$ où Q est un ensemble **fini** (l'ensemble des états), $I, F \subseteq Q$ sont respectivement les ensembles d'états initiaux et finaux de $\mathcal{A}$, et δ est une application de $Q \times A$ dans l'ensemble $\mathcal{P}(Q)$ des parties de Q, la fonction de transition de $\mathcal{A}$. La fonction δ pourra aussi être spécifiée par l'ensemble des transitions de $\mathcal{A}$, c'est-à-dire par l'ensemble des triplets $(p, a, q) \in Q \times A \times Q$ tels que $q \in \delta(p, a)$. La transition (p, a, q) sera parfois notée $p \xrightarrow{a} q$.

La fonction de transition δ est étendue à $Q \times A^*$ par récurrence, en posant, pour tout $q \in Q$, pour tout $u \in A^*$ et pour tout $a \in A$,

$$\delta(q, 1) = \{q\} \text{ et } \delta(q, ua) = \bigcup_{p \in \delta(q,u)} \delta(p, a).$$

Ainsi, un mot $u \in A^*$ est accepté par l'automate $\mathcal{A}$ s'il existe un état initial i et un état final f tels que $f \in \delta(i, u)$. Le langage accepté par $\mathcal{A}$ est noté $L(\mathcal{A})$.

On dit qu'un état $q \in Q$ est accessible s'il existe un état initial i et un mot $u \in A^*$ tels que $q \in \delta(i, u)$.

L'automate $\mathcal{A}$ est dit déterministe s'il admet un unique état initial i et si, pour chaque $(q, a) \in Q \times A$, l'ensemble $\delta(q, a)$ est de cardinalité 0 ou 1. Dans ce cas, on notera $\mathcal{A} = (Q, i, \delta, F)$ au lieu de $(Q, \{i\}, \delta, F)$, on utilisera (lorsqu'il n'y aura pas d'ambiguïté) la notation $q \cdot a$ pour désigner l'unique élément de $\delta(q, a)$ si ce dernier ensemble est non vide, et on dira que $q \cdot a$ n'est pas défini si $\delta(q, a) = \emptyset$.

1. Mots réduits

Soit $\bar{A} = \{\bar{a} \mid a \in A\}$ une copie de A, disjointe de A. On étend la bijection $a \mapsto \bar{a}$ à $(A \cup \bar{A})^*$ en posant $\bar{\bar{a}} = a$ pour tout $a \in A$, en posant $\bar{1} = 1$ et en posant, si $u \in (A \cup \bar{A})^*$ et $a \in A \cup \bar{A}$, $\overline{ua} = \bar{a}\bar{u}$.

On définit un système de réécriture $\longrightarrow_g$ dans $(A \cup \bar{A})^*$ en considérant les règles de la forme

$$u a \bar{a} v \longrightarrow_g uv \quad \text{and} \quad u \bar{a} a v \longrightarrow_g uv$$

pour tous les mots $u, v \in (A \cup \bar{A})^*$ et toutes les lettres $a \in A$. Remarquons que si un mot u contient plusieurs occurrences de facteurs de la forme $a\bar{a}$ ou $\bar{a}a$ $(a \in A)$, alors il existe plusieurs mots v tels que $u \longrightarrow_g v$.

On note $\longrightarrow_g^*$ la fermeture réflexive et transitive de la relation $\longrightarrow_g$. On a alors, pour tout $w, w' \in (A \cup \bar{A})^*$, $w \longrightarrow_g^* w'$ si et seulement s'il existe $n \geq 0$ et des éléments $w_0 = w, w_1, \ldots, w_n = w'$ de $(A \cup \bar{A})^*$ tels que $w_i \longrightarrow_g^* w_{i+1}$ pour $i = 0, \ldots, n-1$.

On dit qu'un mot $u \in (A \cup \bar{A})^*$ est réduit si $u \longrightarrow_g^* v$ entraîne $u = v$, c'est-à-dire si et seulement si u ne contient pas de facteur de la forme $a\bar{a}$ ou $\bar{a}a$ $(a \in A)$.

1.1 Montrer que si $u, v, v' \in (A \cup \bar{A})^*$ et si $u \longrightarrow_g v$ et $u \longrightarrow_g v'$, alors il existe un mot $w \in (A \cup \bar{A})^*$ tel que $v \longrightarrow_g^* w$ et $v' \longrightarrow_g^* w$.

1.2 Montrer que, pour tout mot $u \in (A \cup \bar{A})^*$, il existe un mot réduit $v \in (A \cup \bar{A})^*$ tel que $u \longrightarrow_g^* v$, et que ce mot est unique. [Pour démontrer l'unicité, on pourra procéder par récurrence sur la longueur de u.]

L'unique mot réduit v tel que $u \longrightarrow_g^* v$ est noté $\rho(u)$. L'ensemble des mots réduits, à savoir $\rho((A \cup \bar{A})^*)$, est noté $F(A)$.

1.3 Calculer $\rho(a\bar{b}b^2\bar{a}\,\bar{b}ba\bar{b}a\bar{b})$. Vérifier que ρ n'est pas un morphisme.

1.4 Montrer que si $u, v \in (A \cup \bar{A})^*$, alors $\rho(\rho(u)\rho(v)) = \rho(uv)$.

2. Automates inversifs réduits

Un *automate inversif* sur l'alphabet A est un automate déterministe $\mathcal{A} = (Q, i, \delta, \{i\})$ sur l'alphabet $A \cup \bar{A}$, dont tous les états sont accessibles et tel que, pour tout $p, q \in Q$ et $a \in A \cup \bar{A}$, $p \cdot a = q$ entraîne $q \cdot \bar{a} = p$. Il s'ensuit que la fonction de transition induite par chaque lettre $a \in A$, $\delta(-, a)$, est une bijection d'une partie de Q sur une autre. La réciproque de cette bijection est la fonction de transition induite par la lettre $\bar{a}$, $\delta(-, \bar{a})$.

Il est commode, lorsque l'on représente des automates inversifs sur A, de ne faire figurer que les transitions étiquetées par des lettres de A, puisque les transitions étiquetées par les lettres de $\bar{A}$ s'en déduisent sans ambiguïté. Voir la figure 1.

2.1 Soit $\mathcal{A}$ un automate inversif, soit $u \in (A \cup \bar{A})^*$ et soient p, q deux états de $\mathcal{A}$ tels que $p \cdot u = q$. Montrer que $p \cdot \rho(u) = q$. [On pourra montrer d'abord que si $u \longrightarrow_g v$, alors $p \cdot v = q$.]

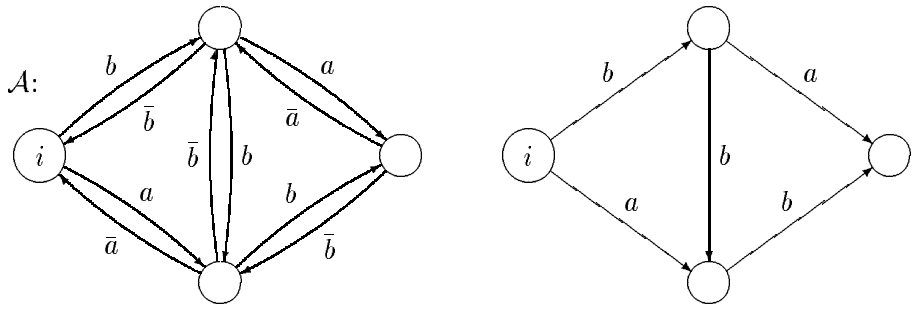

Figure 1: Un automate inversif sur l'alphabet $A = \{a, b\}$, d'abord avec toutes ses transitions, et ensuite présenté de façon plus compacte

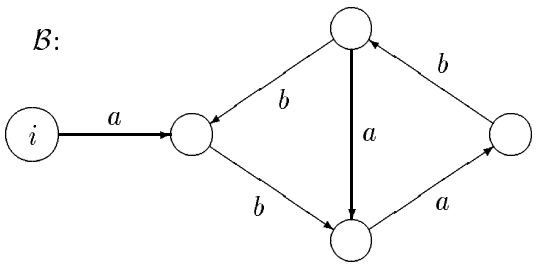

Figure 2: Encore un automate inversif réduit sur l'alphabet $A = \{a, b\}$

On dit que l'automate inversif $\mathcal{A} = (Q, i, \delta, \{i\})$ est *réduit* si, pour tout mot réduit $u \in (A \cup \bar{A})^*$ tel que $i \cdot u$ est défini dans $\mathcal{A}$ et $i \cdot u \neq i$, il existe un mot v tel que uv est réduit et $i \cdot (uv) = i$. Par exemple, les automates des figures 1 et 2 sont réduits.

2.2 Soit $\mathcal{A} = (Q, i, \delta, \{i\})$ un automate inversif. Montrer que $\mathcal{A}$ est réduit si et seulement si, pour tout état q tel que $q \neq i$, il existe deux lettres distinctes $a, b \in A \cup \bar{A}$ telles que $q \cdot a$ et $q \cdot b$ sont définis dans $\mathcal{A}$.

Soient $\mathcal{A} = (Q_\mathcal{A}, i, \delta, F_\mathcal{A})$ et $\mathcal{B} = (Q_\mathcal{B}, j, \varepsilon, F_\mathcal{B})$ deux automates déterministes sur l'alphabet A. Un *morphisme d'automates* de $\mathcal{A}$ dans $\mathcal{B}$ est une application $\kappa: Q_\mathcal{A} \longrightarrow Q_\mathcal{B}$ telle que $\kappa(i) = j$, $\kappa(F_\mathcal{A}) \subseteq \kappa(F_\mathcal{B})$ et telle que, si $q \in Q_\mathcal{A}$ et $a \in A \cup \bar{A}$ sont tels que $q \cdot a$ est défini dans $\mathcal{A}$, alors $\kappa(q) \cdot a$ est défini dans $\mathcal{B}$ et $\kappa(q \cdot a) = \kappa(q) \cdot a$. On dit que le morphisme κ est un *isomorphisme* si l'application κ est une bijection, et si κ^{-1} est un morphisme de $\mathcal{B}$ dans $\mathcal{A}$. Finalement, on dit que $\mathcal{A}$ et $\mathcal{B}$ sont *isomorphes* s'il existe un isomorphisme de $\mathcal{A}$ dans $\mathcal{B}$.

2.3 Soient $\mathcal{A}$ et $\mathcal{B}$ deux automates inversifs.

2.3.1 Montrer que s'il existe un morphisme de $\mathcal{A}$ dans $\mathcal{B}$, alors il en existe un seul.

2.3.2 Montrer que s'il existe un morphisme κ de $\mathcal{A}$ dans $\mathcal{B}$ et un morphisme λ de $\mathcal{B}$ dans $\mathcal{A}$, alors κ et λ sont des isomorphismes et $\kappa^{-1} = \lambda$.

3. Le groupe libre et ses sous-groupes

Soit $F(A)$ l'ensemble des mots réduits sur l'alphabet $A \cup \bar{A}$ (voir section 1). On définit un produit sur $F(A)$ (noté $\odot$) en posant, pour deux mots réduits $u, v \in F(A)$, $u \odot v = \rho(uv)$. Ainsi, on a $(a\bar{b}a) \odot (\bar{a}ba) = a^2$.

On rappelle qu'un monoïde $(M, \odot)$ est un groupe si pour chaque $m \in M$, il existe un élément $m' \in M$ tel que $m \odot m' = m' \odot m = 1$, où 1 est l'élément neutre de M. L'élément m', dont on peut démontrer facilement qu'il est unique, est appelé l'inverse de m et est noté m^{-1}. Si $(M, \odot)$ est un groupe et si N est une partie de M, alors N est un sous-groupe de M si $1 \in N$ et si, pour tout $m, m' \in N$, on a $mm', m^{-1} \in N$.

Si G et H sont des groupes, un morphisme de groupes de G dans H est une application $\varphi: G \longrightarrow H$ telle que, pour tout $g, g' \in G$, on a $\varphi(gg') = \varphi(g)\varphi(g')$. On admettra que si φ est un morphisme bijectif, alors l'application réciproque φ^{-1} est aussi un morphisme. On dit alors que φ est un isomorphisme.

3.1 Montrer que $(F(A), \odot)$ est un groupe. [On pourra utiliser la question 1.4.]

Le groupe $(F(A), \odot)$ (ou plus simplement le groupe $F(A)$) est appelé le groupe libre sur A. On admettra le résultat suivant : *si A et B sont deux alphabets, les groupes $F(A)$ et $F(B)$ sont isomorphes si et seulement si A et B ont même cardinalité.*

La cardinalité d'un ensemble X est notée $\mathrm{Card}(X)$.

La cardinalité de A est appelée rang du groupe libre $F(A)$, et l'ensemble A est appelé une base de $F(A)$. Plus généralement, si G est un groupe et $\varphi: F(A) \longrightarrow G$ est un isomorphisme, on dira que G est un groupe libre de rang $\mathrm{Card}(A)$ et que $\varphi(A)$ est une base de G.

3.2 Montrer que, pour toute application $\beta: A \to G$ de A dans un groupe G, il existe un unique morphisme de groupe $\bar{\beta}: F(A) \to G$ tel que la restriction de $\bar{\beta}$ à A coïncide avec β.

3.3 Soit $\mathcal{A}$ un automate inversif. Montrer que $\rho(L(\mathcal{A})) = L(\mathcal{A}) \cap F(A)$ et que $\rho(L(\mathcal{A}))$ est un sous-groupe de $F(A)$.

Le sous-groupe $\rho(L(\mathcal{A}))$ est noté $\mathcal{H}(\mathcal{A})$.

3.4 Montrer que si $\mathcal{A}$ et $\mathcal{B}$ sont deux automates inversifs réduits et si $\mathcal{H}(\mathcal{A}) = \mathcal{H}(\mathcal{B})$, alors $\mathcal{A}$ et $\mathcal{B}$ sont isomorphes. [On pourra utiliser la question 2.3.2.]

4. Sous-arbres des automates inversifs

Soit $\mathcal{T} = (Q, i, \delta, \{i\})$ un automate inversif. On dit que $\mathcal{T}$ est un arbre si, pour tout $q \in Q$ et pour tout $u \in (A \cup \bar{A})^*$, $\delta(q, u) = q$ entraîne $\rho(u) = 1$.

4.1 Montrer que si $\mathcal{T} = (Q, i, \delta, \{i\})$ est un arbre, alors pour toute paire d'états $(p, q) \in Q \times Q$, il existe un mot réduit u tel que $\delta(p, u) = q$, et que ce mot est unique.

4.2 Montrer que si $\mathcal{T} = (Q, i, \delta, \{i\})$ est un arbre, et si

$$E_{\mathcal{T}} = \{(q, a) \in Q \times A \mid \delta(q, a) \text{ est défini}\},$$

alors $\mathrm{Card}(E_{\mathcal{T}}) = \mathrm{Card}(Q) - 1$.

Soit $\mathcal{A} = (Q, i, \delta, \{i\})$ et $\mathcal{B} = (P, j, \varepsilon, \{j\})$ deux automates inversifs. On dit que $\mathcal{B}$ est un sous-automate de $\mathcal{A}$, ou que $\mathcal{B}$ est inclus dans $\mathcal{A}$, et on note $\mathcal{B} \subseteq \mathcal{A}$, si $P \subseteq Q$, $j = i$, et si, pour tout $q \in P$ et $a \in A \cup \bar{A}$ tel que $\varepsilon(q, a)$ est défini, on a $\varepsilon(q, a) = \delta(q, a)$.

Si $\mathcal{B}$ est à la fois un sous-automate de $\mathcal{A}$ et un arbre, on dira que c'est un sous-arbre de $\mathcal{A}$. Enfin, on dit que $\mathcal{B}$ est un arbre couvrant de $\mathcal{A}$ si $\mathcal{B}$ est un sous-arbre de $\mathcal{A}$ tel que $P = Q$.

4.3 Donner des arbres couvrants des deux automates des figures 1 et 2. Aucune justification n'est demandée.

4.4 Soit $\mathcal{A}$ un automate inversif réduit. Donner et justifier un algorithme pour construire un arbre couvrant de $\mathcal{A}$ (démontrant ainsi l'existence d'un arbre couvrant de $\mathcal{A}$). L'algorithme sera décrit de façon informelle.

5. Base de $\mathcal{H}(\mathcal{A})$

Soit $\mathcal{A} = (Q, i, \delta, \{i\})$ un automate inversif réduit, et soit $\mathcal{T} = (Q, i, \varepsilon, \{i\})$ un arbre couvrant de $\mathcal{A}$. Pour tout état $q \in Q$, notons t_q l'unique mot réduit tel que $\varepsilon(i, t_q) = q$ (voir question 4.1). Soit

$$\begin{aligned} D &= \{(q, a) \in Q \times A \mid \delta(q, a) \text{ est défini}\} \\ E &= \{(q, a) \in Q \times A \mid \delta(q, a) \text{ est défini et } \varepsilon(q, a) \text{ n'est pas défini}\}. \end{aligned}$$

Pour tout $(q, a) \in E$, on pose $h_{q,a} = t_q a \bar{t}_{\delta(q,a)}$.

5.1 Montrer que pour tout $(q, a) \in E$, le mot $h_{q,a}$ est réduit et $i \cdot h_{q,a} = i$. Montrer que $\mathcal{H}(\mathcal{A})$ est engendré par $\{h_{q,a} \mid (q, a) \in E\}$.

5.2 On considère le morphisme $\beta: F(E) \longrightarrow F(A)$, déterminé de façon unique par le fait que, pour tout $b = (q, a) \in B$, $\beta(b) = h_{q,a}$ (voir question 3.2). Montrer que $\beta(F(E)) = \mathcal{H}(\mathcal{A})$ et que β est injectif.

5.3 Montrer que $\mathcal{H}(\mathcal{A})$ est un groupe libre de rang $\mathrm{Card}(D) - \mathrm{Card}(Q) + 1$.

5.4 Donner le rang et une base de chacun des deux automates des figures 1 et 2. Aucune justification n'est demandée.

6. Construction effective

Soit X une partie de $F(A)$. On appelle sous-groupe engendré par X le plus petit sous-groupe de $F(A)$ contenant X. On admettra que ce sous-groupe existe, et qu'il est constitué du mot vide 1 et de tous les produits de la forme $x_1 \odot x_2 \odot \ldots \odot x_n$ $(n \geq 1)$ où pour tout i, x_i ou $\bar{x}_i$ appartient à X.

On démontre dans cette partie que tout sous-groupe H de $F(A)$ engendré par une partie finie X est de la forme $\mathcal{H}(\mathcal{A})$, pour un automate inversif réduit $\mathcal{A}$ uniquement déterminé et effectivement calculable à partir de la donnée de X. On en déduira qu'un tel sous-groupe est libre et que l'on peut en calculer le rang et une base.

Soient $h_1, \ldots, h_r$ des mots de $(A \cup \bar{A})^*$ et soit H le sous-groupe de $F(A)$ engendré par $\rho(h_1)$, ..., $\rho(h_r)$. A partir de la donnée des h_i, on construit un automate $\mathcal{A}_1 = (Q_1, 1, \delta_1, \{1\})$ de la façon suivante. On pose

$$Q_1 = \{1\} \cup \{(i, u) \mid 1 \leq i \leq r,\ u \in (A \cup \bar{A})^+,\ \exists v \in (A \cup \bar{A})^+,\ uv = h_i\}.$$

Les transitions de $\mathcal{A}_1$ sont définies en posant, pour toute lettre $a \in A \cup \bar{A}$, une transition $(i, u) \xrightarrow{a} (i, ua)$ si (i, u) et (i, ua) sont des éléments de Q_1, une transition $(i, u) \xrightarrow{a} 1$ si $(i, u) \in Q_1$ et $ua = h_i$, une transition $1 \xrightarrow{a} (i, a)$ pour tout i tel que a est la première lettre de h_i, et une transition $1 \xrightarrow{a} 1$ s'il existe i tel que $h_i = a$. Enfin, pour toute transition $p \xrightarrow{a} q$ ainsi définie, on rajoute une transition $q \xrightarrow{\bar{a}} p$.

On construit ensuite par récurrence une suite d'automates $\mathcal{A}_n$ de la façon suivante. Si $n \geq 1$ et $\mathcal{A}_n = (Q_n, 1, \delta_n, \{1\})$ est défini, et si dans $\mathcal{A}_n$ il existe des états p, q, r et une lettre $a \in A \cup \bar{A}$ tels que $p \neq q$, $q \neq 1$, et $p, q \in \delta_n(r, a)$, alors on définit $\mathcal{A}_{n+1}$ comme suit (sinon $\mathcal{A}_{n+1}$ n'est pas défini et la construction s'arrête) : on fixe un tel quadruplet (p, q, r, a) et on identifie p et q. Formellement, on pose $Q_{n+1} = Q_n \setminus \{q\}$ (si R et S sont

deux ensembles, $R \setminus S$ désigne l'ensemble des éléments de R qui ne sont pas dans S). Pour tout $s \in Q_n$ et tout $b \in A \cup \bar{A}$, on pose

$$\delta'_n(s,b) = \begin{cases} (\delta_n(s,b) \setminus \{q\}) \cup \{p\} & \text{si } q \in \delta_n(s,b) \\ \delta_n(s,b) & \text{sinon.} \end{cases}$$

Enfin, si $s \in Q_{n+1}$ et $b \in A \cup \bar{A}$, on pose

$$\delta_{n+1}(s,b) = \begin{cases} \delta'_n(s,b) & \text{si } s \neq p \\ \delta'_n(p,b) \cup \delta'_n(q,b) & \text{si } s = p. \end{cases}$$

Il faut noter que la définition de $\mathcal{A}_{n+1}$ à partir de $\mathcal{A}_n$ repose sur un choix arbitraire : il peut y avoir plusieurs quadruplets de la forme (p,q,r,a) appelant une identification d'états.

6.1 Montrer que la construction de la suite $\mathcal{A}_n$ s'arrête au bout d'un nombre fini d'étapes.

6.2 Calculer le dernier des $\mathcal{A}_n$ lorsque H est le sous-groupe de $F(\{a,b\})$ engendré par $bab^{-1}a^{-1}$, $b^3a^{-1}ba^{-1}$ et b^2a^{-1}.

6.3 Montrer que $\rho(L(\mathcal{A}_1)) = H$.

6.4 Montrer que si $\mathcal{A}_n$ est défini, alors $\rho(L(\mathcal{A}_n)) = H$.

6.5 Montrer que le dernier automate de la suite ainsi construite, appelons-le $\mathcal{B}_1$, est un automate inversif tel que $\mathcal{H}(\mathcal{B}_1) = H$.

Posons maintenant $\mathcal{B}_1 = (P_1, 1, \varepsilon_1, \{1\})$. Si $n \geq 1$, si $\mathcal{B}_n = (P_n, 1, \varepsilon_n, \{1\})$ est défini, et si $\mathcal{B}_n$ n'est pas réduit, il existe un état $q \neq 1$ dans P_n tel que $\varepsilon_n(q,a)$ est défini pour une unique lettre $a \in A \cup \bar{A}$ (voir la question 2.2). Soit $p = \varepsilon_n(q,a)$. On définit alors un automate $\mathcal{B}_{n+1} = (P_{n+1}, 1, \varepsilon_{n+1}, \{1\})$ de la façon suivante. On pose d'abord $P_{n+1} = P_n \setminus \{q\}$. Ensuite, pour tout $r \in P_{n+1}$ et tout $b \in A \cup \bar{A}$, on pose $\varepsilon_{n+1}(r,b) = \varepsilon_n(r,b)$ si $r \neq p$ ou $b \neq \bar{a}$. Par contre, $\varepsilon_{n+1}(p,\bar{a})$ n'est pas défini.

Il faut noter qu'ici encore, la construction de $\mathcal{B}_{n+1}$ à partir de $\mathcal{B}_n$ dépend d'un choix : il peut y avoir plusieurs paires (q,a) comme ci-dessus.

6.6 Montrer que la construction de la suite $\mathcal{B}_n$ s'arrête au bout d'un nombre fini d'étapes. Montrer que le dernier automate ainsi construit, appelons-le $\mathcal{C}$, est un automate inversif réduit.

6.7 Calculer $\mathcal{C}$ lorsque H est le sous-groupe H de la question 6.2.

6.8 Montrer que l'automate $\mathcal{C}$ ne dépend pas des choix faits lors du passage de chaque $\mathcal{A}_n$ à l'automate $\mathcal{A}_{n+1}$ suivant, ni des choix faits pour passer de $\mathcal{B}_n$ à $\mathcal{B}_{n+1}$. Montrer qu'en fait, si H est également engendré par des éléments $k_1, \ldots, k_s \in F(A)$, alors la construction ci-dessus opérée sur les k_i au lieu des h_j mène au même automate $\mathcal{C}$.

Ainsi, si X est une partie finie de $(A \cup \bar{A})^*$ et si H est le sous-groupe de $F(A)$ engendré par $\rho(X)$, les résultats des sections 5 et 6 montrent que H est un groupe libre, et donnent des algorithmes pour calculer son rang et une base.