70.05M

SESSION 2007

Filière MP (groupe I)

Épreuve commune aux ENS de Paris, Lyon et Cachan

Filière PC (groupe I)

Épreuve commune aux ENS de Paris et Lyon

MATHÉMATIQUES - INFORMATIQUE

Durée : 4 heures

L'usage de calculatrices électroniques de poche à alimentation autonome, non imprimantes et sans document d'accompagnement, est autorisé. Cependant, une seule calculatrice à la fois est admise sur la table ou le poste de travail, et aucun échange n'est autorisé entre les candidats.

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.

Un ensemble M muni d'une loi de composition interne $\odot$ sera noté $(M, \odot)$ ou simplement M lorsque la loi considérée est sans ambiguïté. Si la loi $\odot$ est associative et si M contient un élément neutre pour $\odot$ (noté 1_M), on dit que $(M, \odot)$ est un *monoïde*. 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 $(M, \odot)$ et $(N, \otimes)$ sont des monoïdes, un *morphisme* $\varphi : M \longrightarrow N$ 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. Un élément x d'un monoïde $(M, \odot)$ est dit *inversible* s'il existe $y \in M$ tel que $x \odot y = y \odot x = 1_M$. Dans ce cas, y est unique et est appelé l'*inverse* de x, noté x^{-1}. Rappelons qu'un *groupe* est un monoïde dont tout 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. On démontrera en particulier que tout sous-groupe d'un groupe libre est lui-même un groupe libre s'il est engendré par un nombre fini d'éléments.

Note : Quand on parle d'algorithmes ici, on demande de préciser les principes d'un algorithme et non de donner du pseudo-code.

1 – Préliminaires

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

Question 1.1 *Soient $(M, \odot)$ et $(N, \otimes)$ des monoïdes et $\varphi : M \longrightarrow N$ un morphisme.*

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

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

Soit $(M, \odot)$ un monoïde et N une partie de M. On dit que $(N, \odot)$ est un *sous-monoïde* de M si $1_M \in N$ et si pour tout $x, y \in N$, $x \odot y \in N$. Si, de plus, M est un groupe et pour tout $x \in N$, $x^{-1} \in N$, on dit que $(N, \odot)$ est un *sous-groupe* de M.

Question 1.2 *Soit R une partie d'un monoïde $(M, \odot)$.*

1.2.1 *Soit R^* l'ensemble consistant en l'élément neutre 1_M et les produits finis 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.*

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

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

2 – Mots réduits

Soit A un alphabet. 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 $\bar{\bar{a}} = a$ pour tout $a \in A$.

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

Question 2.1 *Montrer que pour tout mot $u \in \tilde{A}^*$, il existe un mot réduit v tel que $u \xrightarrow{\infty} v$. Calculer un tel mot v lorsque $u = ab\bar{a}a\bar{b}\bar{b}aab\bar{b}\bar{a}\bar{a}aab\bar{b}\bar{a}ab$.*

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 $y \xrightarrow{\leq 1} z$.*

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

Question 2.4 *Donner un algorithme qui, étant donné $u \in \tilde{A}^*$, calcule l'unique mot réduit v tel que $u \xrightarrow{\infty} v$. Estimer la complexité (le nombre d'opérations élémentaires) de cet algorithme en fonction de la longueur $n = |u|$. Essayer de réduire cette complexité autant que possible en ordre de grandeur.*

3 – Groupes libres

Soit A un alphabet. On note $F(A)$ l'ensemble des mots réduits de $\tilde{A}^*$ et $\rho : \tilde{A}^* \longrightarrow F(A)$ l'application qui à $u \in \tilde{A}^*$ associe $\rho(u)$ l'unique mot réduit tel que $u \xrightarrow{\infty} \rho(u)$. On définit une loi de composition interne sur $F(A)$ en posant $u \odot v = \rho(uv)$. Enfin, on étend l'application $a \longmapsto \bar{a}$ à $\tilde{A}^*$ en posant

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

Question 3.1 *Montrer que si $u, v, w \in \tilde{A}^*$ alors $u \odot (v \odot w) = \rho(uvw)$. En déduire que $(F(A), \odot)$ est un groupe et que, pour tout $u \in F(A)$, $u^{-1} = \bar{u}$.*

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 $u, v \in F(A)$) ?*

Question 3.3 *Soit G un groupe et soit $\varphi : A \longrightarrow G$ une application. Montrer qu'il existe un et un seul morphisme $\varphi_F : F(A) \longrightarrow G$ tel que $\varphi_F(a) = \varphi(a)$ pour tout $a \in A \subseteq F(A)$.*

Dans la situation de la question 3.3, on dit que le morphisme φ_F est *induit par* l'application φ, ou qu'il la *prolonge*. 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.

Question 3.4 *Soit A et B deux alphabets de même cardinal. Montrer que $F(A)$ et $F(B)$ sont isomorphes.*

4 – Rang d'un groupe libre

Soit X une partie finie non vide de $F(A)$. On dit que X *est une base de $F(A)$* s'il existe un alphabet B de même cardinal que X et une bijection $\varphi : B \longrightarrow X \subseteq F(A)$ tels que le morphisme $\varphi_F : F(B) \longrightarrow F(A)$ induit par φ est un isomorphisme.

Le but de cette partie est de montrer que toutes les bases de $F(A)$ ont le même cardinal.

Question 4.1 *Vérifier que A est une base de $F(A)$. Montrer que la condition pour qu'une partie X de $F(A)$ soit une base ne dépend pas du choix de l'alphabet B et de la bijection φ.*

Question 4.2 *Supposons que $A = \{a, b\}$.*

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

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

Question 4.3 *Soient A et B deux alphabets et soit $\varphi: F(A) \longrightarrow F(B)$ un morphisme. On considère un $\mathbb{R}$-espace vectoriel $V(A)$ de dimension $\mathsf{card}(A)$ et une base E_A de $V(A)$. Comme $V(A)$ muni de l'addition est un groupe, on peut définir un morphisme $\sigma_F: F(A) \longrightarrow V(A)$ induit par une bijection $\sigma: A \longrightarrow E_A$ (A et E_A ont même cardinal). De même, on définit $V(B)$, une base E_B de $V(B)$ et un morphisme $\rho_F: F(B) \longrightarrow V(B)$ à partir d'une bijection $\rho: B \longrightarrow E_B$.*

4.3.1 Montrer qu'il existe une application linéaire $\hat{\varphi}: V(A) \longrightarrow V(B)$ telle que $\rho_F \circ \varphi = \hat{\varphi} \circ \sigma_F$, comme ci-dessous :

$$\begin{array}{ccc} F(A) & \xrightarrow{\varphi} & F(B) \\ {\scriptstyle \sigma_F}\downarrow & & \downarrow{\scriptstyle \rho_F} \\ V(A) & \xrightarrow{\hat{\varphi}} & V(B) \end{array}$$

4.3.2 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.

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

Le cardinal commun des 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 $\varphi: G \longrightarrow F(A)$ 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 4.4 *Soit $A = \{a, b\}$, soit $C = \{c_1, \ldots, c_n\}$ un alphabet à n éléments, $n \geq 1$, et soit φ le morphisme $\varphi: F(C) \longrightarrow F(A)$ induit par l'application $c_i \longmapsto a^i b \bar{a}^i$ ($i \in \{1, \ldots, n\}$).*

4.4.1 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 $\bar{b}^{|k|}$.)

4.4.2 Montrer que φ est injectif.

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

5 – Mots cycliquement réduits et conjugaison

Soit $u \in \tilde{A}^*$. On dit que le mot u est *cycliquement réduit* si u est le mot vide ou si $u = a_1 a_2 \cdots a_n$ ($n \geq 1$ et $a_i \in \tilde{A}$ pour tout i) est réduit 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 5.1 *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. En déduire que si u n'est pas le mot vide, alors pour tout entier $n > 0$, $u^n \neq 1$.*

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

Question 5.3 *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 $v = sr$.*

Question 5.4 *Donner un algorithme pour décider si deux mots $u, u' \in F(A)$ sont conjugués.*

6 – 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 illustré figure 1.

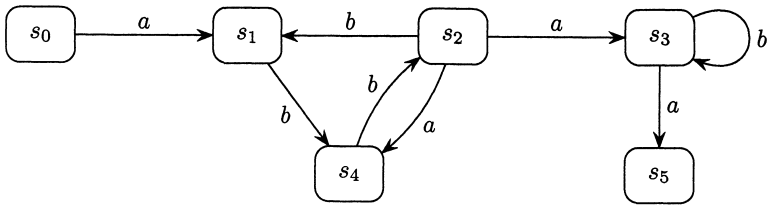

FIG. 1 – Un A-graphe à 6 sommets et 8 arêtes

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 $a_1 a_2 \cdots a_n \in \tilde{A}^*$. Par convention, on considère que, pour tout sommet u, il existe un chemin de longueur 0 de u à u, appelé *chemin vide en u*. Dans le A-graphe de la figure 1, 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.

Si un chemin ne comporte pas deux arêtes consécutives de la forme $(u, a, v)(v, \bar{a}, u)$ avec $(u, a, v) \in \tilde{E}$, on dit qu'il est *réduit*. 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 1 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 6.1 *Montrer que l'étiquette d'un chemin est réduite si et seulement si le chemin est réduit.*

Question 6.2 *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.*

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 6.3 *Montrer que $G(\Gamma, s_0)$ est un sous-groupe de $F(A)$.*

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 6.2). 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 6.4 *Que peut-on dire de $G(\Gamma, s_0)$ lorsque Γ est une forêt ?*

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

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 6.6 *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 $\overline{b_e}$.*

Indication. 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 factorisation $p = p_0 e_1 p_1 \cdots e_r p_r$ 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 $\bar{x}_{t_i} \odot x_{s_{i+1}}$ où t_i est le sommet final de e_i et s_{i+1} le sommet initial de e_{i+1}.

Question 6.7 *Soit $r = \mathrm{card}(E \setminus E_T)$. Montrer que $G(\Gamma, s_0)$ est isomorphe à un groupe libre de rang r de base $\{b_e \mid e \in E \setminus E_T\}$.*

7 – 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 $\rho(L(\mathcal{A}))$ l'ensemble $\rho(L(\mathcal{A})) = \{\rho(u) \mid u \in L(\mathcal{A})\}$.

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'. Plus précisément, 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. L'ensemble d'arêtes F est obtenu à partir de E en remplaçant partout v et v' par w et en ôtant les doublons éventuels. 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 7.1 *Montrer que si* $\mathcal{A} \xrightarrow{1} \mathcal{B}$, *alors*

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

Question 7.2 *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 $\mathcal{A}$.

Question 7.3 *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.*

8 – Représentations des groupes libres

Les questions de cette dernière 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 8.1 *Dans cette question, on suppose que $A = \{a, b\}$. Soit GL_2 le groupe des matrices carrées d'ordre 2 à coefficients réels, inversibles pour le produit de matrices, 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 considérera les quatre régions du plan Y_a, $Y_{\bar{a}}$, Y_b et $Y_{\bar{b}}$ décrites ci-dessous et représentées figure 2 :

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

On regardera dans quelles régions se situent les images de ces régions par les applications linéaires α, α^{-1}, β et β^{-1}. Enfin, pour $u \in F(A)$, $u = c_1 \ldots c_n$ et $\varphi(u) = \varphi(c_1) \circ \cdots \circ \varphi(c_n)$, on discutera de l'image de ces régions en fonction de $\varphi(c_1)$ et $\varphi(c_n)$.

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

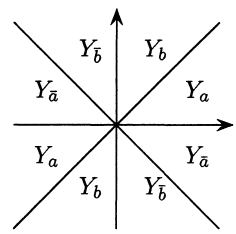

FIG. 2 – Les régions Y_a, $Y_{\bar{a}}$, Y_b et $Y_{\bar{b}}$

$$R+S=\sum_{w\in A^*}(R_w+S_w)w \qquad \text{et} \qquad RS=\sum_{w\in A^*}(\sum_{uv=w}R_uS_v)w.$$

On notera que dans la définition du produit RS, le coefficient de w, c'est-à-dire la somme des R_uS_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 $U(A)$ le groupe des éléments de $\mathbb{Z}[\![A]\!]$ inversibles pour la multiplication.

Question 8.2 *Montrer que pour chaque $a \in A$, la série formelle $1+a$ appartient à $U(A)$.*

Question 8.3 *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. On regroupera, dans l'écriture d'un mot réduit w de $F(A)$, les occurrences consécutives d'une même lettre, c'est-à-dire on écrira $w=c_1^{n_1}c_2^{n_2}\cdots c_r^{n_r}$ 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 $c_1c_2\cdots c_r$ dans $\varphi(w)$?