ENS 2007 — math-info

Partie I — Préliminaires

Question I.1

I.1.a Soit x et y dans N. Notons $x' = \varphi^{-1}(x) \in M$ et $y' = \varphi^{-1}(y) \in M$. φ est un morphisme donc $\varphi(x' \odot y') = \varphi(x') \otimes \varphi(y') = x \otimes y$, ce qui signifie que $\varphi^{-1}(x \otimes y) = x' \odot y' = \varphi^{-1}(x) \odot \varphi^{-1}(y)$, et établit que φ^{-1} est également un morphisme.

I.1.b Il suffit d'évaluer $\varphi(x) \otimes \varphi(x^{-1}) = \varphi(x \odot x^{-1}) = \varphi(1_M) = 1_N$ pour assurer que $\varphi(x^{-1})$ est bien l'inverse (dans N) de $\varphi(x)$.

Question I.2

I.2.a La stabilité d'un sous-monoïde par $\odot$ entraîne que tout sous-monoïde contenant R doit contenir R^*, ce qui garantit la minimalité demandée.

Reste à vérifier que R^* est bien stable lui même : tout produit de deux produits finis est bien un produit fini.

I.2.b La stabilité d'un sous-groupe par inverse entraîne que tout sous-groupe contenant R doit contenir $R \cup R^{-1}$, donc, d'après la question précédente, doit contenir $(R \cup R^{-1})^*$, ce qui garantit la minimalité demandée.

Reste à vérifier que le sous-monoïde $(R \cup R^{-1})^*$ est bien un sous-groupe, c'est-à-dire sa stabilité par inverse. Or si on considère un produit fini $x = s_1 \odot s_2 \odot \cdots s_n$ avec $n \geqslant 1$ et chaque $s_i \in R \cup R^{-1}$, son inverse s'écrit $x^{-1} = s_n^{-1} \odot \cdots \odot s_2^{-1} \odot s_1^{-1}$, qui est également un produit fini d'éléments de $R \cup R^{-1}$, puisque pour tout $r \in R$, $(r^{-1})^{-1} = r$.

Partie II — Mots réduits

Question II.1

On raisonne par récurrence sur la longueur du mot.

1 est réduit.

Supposant démontré que pour tout mot u de longueur au plus égale à $n \geqslant 0$, il existe un mot réduit v tel que $u \xrightarrow{\infty} v$, on considère un mot u' de longueur $n+1$. Si u' est déjà réduit, alors $u' \xrightarrow{0} u'$ et le résultat est acquis. Sinon, il existe un mot u tel que $u' \xrightarrow{1} u$. Mais $|u| = |u'| - 2 < n$ donc l'hypothèse de récurrence s'applique et il existe un mot réduit v et un entier ℓ tels que $u \xrightarrow{\ell} v$. Finalement, on aura $u' \xrightarrow{\ell+1} v$ donc $u' \xrightarrow{\infty} v$. Là encore, la récurrence s'enclenche.

On a successivement $u \xrightarrow{5} ab\bar{b}\bar{b}aa\bar{a}ab \xrightarrow{2} a\bar{b}aab$ qui est réduit.

Question II.2

Supposons que $u \xrightarrow{1} x$ et $u \xrightarrow{1} y$. Si $x = y$, on peut poser $z = x = y$ et $x \xrightarrow{0} z$, $y \xrightarrow{0} z$.

Si $x \neq y$, c'est qu'on a obtenu ces deux mots en effaçant deux couples distincts de lettres contigües de u : si ces 4 lettres n'étaient pas distinctes, c'est qu'il existe $a \in \bar{A}$ tel que $a\bar{a}a$ soit un facteur du mot $u = u_1 a\bar{a}au_2$ et que $x = u_1 au_2 = y$, et on revient au cas précédents. Autrement dit, les 4 lettres concernées sont distinctes, $u = u_1 a\bar{a}u_2 b\bar{b}u_3$ où $a \in \bar{A}$ et $b \in \bar{A}$, et $x = u_1 u_2 b\bar{b}u_3$, $y = u_1 a\bar{a}u_2 u_3$. Mais alors $z = u_1 u_2 u_3$ répond à la question.

Question II.3

On raisonne par récurrence sur $|u|$, l'unicité de v étant évidente si $u = 1$.

Supposons qu'on ait démontré pour tout mot u de longueur au plus égale à $n \geqslant 0$ l'unicité du mot v tel que $u \xrightarrow{\infty} v$. Soit u' un mot de longueur $n+1$.

Si u' est déjà réduit, il n'y a rien à prouver.

Sinon, supposons que $u' \xrightarrow{\infty} v_1$ et $u' \xrightarrow{\infty} v_2$, où v_1 et v_2 sont des mots réduits. La première étape qui réduit u' en v_1 (*resp.* en v_2) conduit à un mot u_1 : $u' \xrightarrow{1} u_1 \xrightarrow{\infty} v_1$ (*resp.* à un mot u_2 : $u' \xrightarrow{1} u_2 \xrightarrow{\infty} v_2$). La question précédent montre qu'il existe alors un mot z tel que $u_1 \xrightarrow{\leqslant 1} z$ et $u_2 \xrightarrow{\leqslant 1} z$: on réduit ce mot z, obtenant un mot réduit v ($z \xrightarrow{\infty} v$). Alors $u_1 \xrightarrow{\leqslant 1} z \xrightarrow{\infty} v$ et $u_1 \xrightarrow{\infty} v_1$, donc, d'après l'hypothèse de récurrence appliquée à u_1, on a $v = v_1$. Le même raisonnement sur u_2 montre que $v = v_2$. Finalement $v_1 = v_2$ et la récurrence s'enclenche.

Question II.4
Soit $a\bar{a}$ la première paire qui apparaît dans le mot u : $u = u_1 a\bar{a} u_2$ où u_1 est un mot réduit. On écrit $u \xrightarrow{1} u_1 u_2$, et on itère le procédé sur u_2, opérant le maximum de réduction en une seule passe (une seule lecture du mot u). C'est ce qu'on a fait dans la première étape de la dernière réponse à la question II.1. On recommence alors une nouvelle passe, jusqu'à tomber sur un mot réduit.
Chaque passe complète à un coût linéaire en la taille du mot : si la première passe repère p couples de lettres contigües à effacer, on a écrit dans cette première passe $u \xrightarrow{p} u'$ avec $|u'| = |u| - 2p$, pour un coût $O(|u|)$.
Le pire des cas est celui du mot $u = w\bar{w}$ où w est un mot contenant p lettres distinctes de A. Il faudra p passes pour réduire $u \xrightarrow{p} 1$. La k-ème passe aura un coût $O(2k)$, donc au total, l'algorithme proposé aura un coût quadratique en la longueur du mot à réduire.

Partie III — Groupes libres

Question III.1
Bien sûr 1 est réduit, donc $1 \in F(A)$.
On a $u \odot (v \odot w) = \rho(u\rho(vw))$. Or puisque $vw \xrightarrow{\infty} \rho(vw)$ on a aussi $uvw \xrightarrow{\infty} u\rho(vw) \xrightarrow{\infty} \rho(u\rho(vw)) \in F(A)$ et l'unicité du mot réduit prouve que $\rho(uvw) = \rho(u\rho(vw))$, c'est-à-dire que $u \odot (v \odot w) = \rho(uvw)$.
On en déduit aussitôt l'associativité de la loi $\odot$ (puisque la concaténation des mots est évidemment associative) : $(F(A), \odot)$ est un monoïde.
En outre, la vérification $u\bar{u} \xrightarrow{|u|} 1$ est facile, ce qui prouve l'existence d'un inverse pour la loi $\odot$ et donc que $(F(A), \odot)$ est un groupe.

Question III.2
Si A contient au moins deux éléments a et b, $F(A)$ n'est pas commutatif : $ab = \rho(ab) = a \odot b \neq b \odot a = \rho(ba) = ba$.
Si $A = \{a\}$, si $u \in \bar{A}^*$, on a : $\rho(u) = \begin{cases} a^k, & \text{si } |u|_a - |u|_{\bar{a}} = k \geqslant 0; \\ \bar{a}^k, & \text{si } |u|_{\bar{a}} - |u|_a = k \geqslant 0. \end{cases}$ (On a noté $|u|_a$ (*resp.* $|u|_{\bar{a}}$) le nombre de a (*resp.* de $\bar{a}$) qui figurent dans u. Autrement dit $(F(A), \odot)$ est alors isomorphe au groupe $(\mathbb{Z}, +)$, et il est commutatif.

Question III.3
Notons $\otimes$ l'opération du groupe G.
Tout mot réduit $u = a_1 \dots a_n$ de $F(A)$ (où chaque a_i est une lettre de $\bar{A}$) peut s'écrire $u = a_1 \odot a_2 \odot \cdots \odot a_n$.
Si on impose que $\varphi_F(a) = \varphi(a)$ pour tout $a \in A$, on aura aussi $\varphi_F(\bar{a}) = \varphi(a)^{-1}$ puisque $\bar{a}$ est l'inverse de a dans $F(A)$. Autrement dit φ_F est ainsi déterminé de façon unique : $\varphi_F(u) = \tilde{\varphi}(a_1) \otimes \tilde{\varphi}(a_2) \otimes \cdots \otimes \tilde{\varphi}(a_n)$, où on a posé pour toute lettre $a \in A$: $\tilde{\varphi}(a) = \varphi(a)$ et $\tilde{\varphi}(\bar{a}) = \varphi(a)^{-1}$.
Reste à montrer que l'application φ_F ainsi définie est bien un morphisme, c'est-à-dire que pour tous mots u et v de $F(A)$, $\varphi_F(u \odot v) = \varphi_F(u) \otimes \varphi_F(v)$. On démontre cette propriété par récurrence sur $|u| + |v|$, le résultat étant clair si $u = v = 1$.
Supposons le résultat démontré pour $|u| + |v| \leqslant n$ et considérons deux mots u' et v' sur $F(A)$ tels que $|u'| + |v'| = n + 1$.
Ou bien $u'v'$ est réduit, donc $u' \odot v' = u'v'$, et alors, par construction même de φ_F, on a bien $\varphi_F(u'v') = \varphi_F(u') \otimes \varphi_F(v')$ ce qui est le résultat attendu.
Ou bien $u'v'$ peut se réduire : comme u' et v' sont eux-mêmes réduits, c'est que $u' = ua$ et $v' = \bar{a}v$ avec $a \in \bar{A}$.
Alors $\varphi_F(u') = \varphi_F(u) \otimes \tilde{\varphi}(a)$ et $\varphi_F(v') = \tilde{\varphi}(a)^{-1} \otimes \varphi_F(v)$.
On a donc $\varphi_F(u') \otimes \varphi_F(v') = \varphi_F(u) \otimes \varphi_F(v) = \varphi_F(u \odot v)$ par hypothèse de récurrence. Mais $u'v' \xrightarrow{1} uv$ donc $u' \odot v' = u \odot v$ et on a bien écrit que $\varphi_F(u' \odot v') = \varphi_F(u') \otimes \varphi_F(v')$.

Question III.4
Notons $A = \{a_1, a_2, \dots, a_p\}$ et $B = \{b_1, b_2, \dots, b_p\}$. Posons $\theta(a_i) = b_i$ et $\theta(\bar{a}_i) = \bar{b}_i$. θ est une bijection de $\bar{A}$ sur $\bar{B}$, qu'on prolonge naturellement en un isomorphisme du monoïde $\bar{A}^*$ sur le monoïde $\bar{B}^*$.
On vérifie sans difficulté que pour tous mots u et v de $\bar{A}^*$, si $u \xrightarrow{\ell} v$, alors $\theta(u) \xrightarrow{\ell} \theta(v)$. Notant ρ_A (*resp.* ρ_B) la réduction sur $\bar{A}^*$ (*resp.* sur $\bar{B}^*$), on dispose alors pour tout mot $u \in \bar{A}^*$: $\rho_B(\theta(u)) = \theta(\rho_A(u))$, ce qui revient à dire que θ réalise une isomorphisme de $F(A)$ sur $F(B)$.
En effet : $\theta(u \odot_A v) = \theta(\rho_A(uv)) = \rho_B(\theta(u)\theta(v)) = \theta(u) \odot_B \theta(v)$.

Partie IV — Rang d'un groupe libre

Remarque générale : pour montrer qu'un morphisme de groupe $\varphi : F \to G$ est injectif il suffit de prouver que $w \neq 1_F \Rightarrow \varphi(w) \neq 1_G$.

Question IV.1

Pour montrer que A est une base de $F(A)$, il suffit de considérer $B = A$, et $\varphi : A \to A$ application identique. Alors φ_F est l'application identique de $F(A)$.
Soit B et C deux alphabets de même cardinal que X et $\varphi : B \to X$ une bijection telle que φ_F soit un isomorphisme de $F(B)$ sur $F(A)$. La question III.4 fournit une bijection θ de B sur C qui se prolonge en un isomorphisme de $F(B)$ sur $F(C)$. Alors $\psi = \varphi \circ \theta^{-1}$ est une bijection de C sur X. Il suffit de remarquer que $\psi_F = \varphi_F \circ \theta^{-1}$ pour conclure, puisqu'il s'agit bien d'un isomorphisme de $F(C)$ sur $F(A)$, comme composée de deux isomorphismes.

Question IV.2

IV.2.a $a = x^{-1} \odot y$ et $b = y^{-1} \odot x \odot y^{-1}$.
Notons $B = \{c, d\}$, et $\varphi(c) = x = ab\bar{a}$, $\varphi(d) = y = ab$: φ est bien une bijection de B sur X.
Alors $\varphi_F(\bar{c}d) = a$ et $\varphi_F(\bar{d}c\bar{d}) = b$, et le morphisme φ_F est donc clairement surjectif.
Inverserment, notons $\psi : A \to F(B)$ définie par $\psi(a) = \bar{c}d$ et $\psi(b) = \bar{d}c\bar{d}$: il s'agit d'une bijection de A sur $F(B)$. Alors $\psi_F : F(A) \to F(B)$ est un morphisme de groupe. Et on dispose de : $\varphi_F(\psi_F(a)) = \varphi_F(\bar{c}d) = a$ et $\varphi_F(\psi_F(b)) = \varphi_F(\bar{d}c\bar{d}) = b$. C'est dire que φ_F et ψ_F sont des isomorphismes réciproques l'un de l'autre.
On en déduit que X est une base de $F(A)$.

IV.2.b Soit $Y = \{ab\bar{a}\bar{b}, b\bar{a}\bar{b}a\}$. Supposons qu'il s'agisse d'une base de $F(A)$: d'après le IV.1, je peux choisir $B = \{c, d\}$ et $\varphi : B \to F(A)$ définie par $\varphi(c) = ab\bar{a}\bar{b}$ et $\varphi(d) = b\bar{a}\bar{b}a$ et φ_F devrait être un isomorphisme.
Nous conclurons que Y n'est pas une base de $F(A)$ en démontrant que φ_F n'est pas surjectif.
Or on évalue facilement $\varphi_F(c^2) = ab\bar{a}\bar{b}ab\bar{a}\bar{b}$, $\varphi_F(cd) = ab\bar{a}\bar{a}\bar{b}a$, $\varphi_F(c\bar{d}) = ab\bar{a}\bar{b}\bar{a}ba\bar{b}$, $\varphi_F(\bar{c}^2) = ba\bar{b}\bar{a}ba\bar{b}\bar{a}$, $\varphi_F(\bar{c}d) = ba\bar{b}\bar{a}b\bar{a}\bar{b}a$, $\varphi_F(\bar{c}\bar{d}) = ba\bar{b}\bar{a}\bar{a}ba\bar{b}$, $\varphi_F(d^2) = b\bar{a}\bar{b}ab\bar{a}\bar{b}a$, $\varphi_F(dc) = b\bar{a}\bar{b}aab\bar{a}\bar{b}$, $\varphi_F(d\bar{c}) = b\bar{a}\bar{b}ab\bar{a}\bar{b}\bar{a})$, $\varphi_F(\bar{d}^2) = \bar{a}ba\bar{b}\bar{a}ba\bar{b}$, $\varphi_F(\bar{d}c) = b\bar{a}\bar{b}ab\bar{a}\bar{b}\bar{a}$ et $\varphi_F(\bar{d}\bar{c}) = \bar{a}baa\bar{b}\bar{a}$.
On constate que seules de rares réductions se sont produites (dans les calculs de cd et $\bar{d}\bar{c}$). On en déduit que pour tout mot non vide $u \in F(B)$, $|\varphi_F(u)| \geqslant 3|u|$.
En particulier, dans l'image de φ_F ne figurera aucun mot de longueur 1 ou 2, par exemple. φ_F n'est donc pas surjectif.

Question IV.3

IV.3.a On définit l'application linéaire $\tilde{\varphi}$ en fournissant l'image des vecteurs de la base E_A : $\forall a \in A, \tilde{\varphi}(\sigma(a)) = \rho_F(\varphi(a))$.
Alors les morphismes de groupes $\rho_F \circ \varphi$ et $\tilde{\varphi} \circ \sigma_F$ coïncident sur A, et donc sur tout $F(A)$.

IV.3.b Si φ est surjective, tout élément $b \in B$ admet un antécédent u_b dans $F(A)$. Mais alors $\rho_F(\varphi(u_b)) = \rho_F(b) = \rho(b) = \tilde{\varphi}(\sigma_F(u_b))$ et on a montré que tous les vecteurs de la base E_B (ce sont les $\rho(b)$) sont atteints dans l'image de $\tilde{\varphi}$, qui est donc surjective.
En dimension finie, on en déduit aussitôt que $\operatorname{Card} B = \dim V(B) \leqslant \dim V(A) = \operatorname{Card} A$.

IV.3.c Soit alors X une base de A, un alphabet B et $\varphi : B \to X$ une bijection telle que $\varphi_F : F(B) \to F(A)$ est un isomorphisme.
Appliquant le résultat précédent à φ_F et à φ_F^{-1} on obtient $\operatorname{Card} A \leqslant \operatorname{Card} X = \operatorname{Card} B$ puis $\operatorname{Card} X = \operatorname{Card} B \leqslant \operatorname{Card} A$. On a bien montré que X a le même cardinal que A, donc que toutes les bases de $F(A)$ ont le même cardinal.

Question IV.4

IV.4.a Une récurrence sur k, à i fixé, montre le résultat pour $k > 0$: $\varphi(c_i) = a^i b\bar{a}^i$ et si $\varphi(c_i^k) = a^i b^k \bar{a}^i$, alors $\varphi(c_i^{k+1}) = a^i b\bar{a}^i \odot a^i b^k \bar{a}^i = a^i b^{k+1} \bar{a}^i$.
Pour $k < 0$, on écrit $\varphi(c_i^k) = \varphi(c_i^{|k|})^{-1} = (a^i b^{|k|} \bar{a}^i)^{-1} = a^i \bar{b}^{|k|} \bar{a}^i$.

IV.4.b Si $i \neq j$, on a $\varphi(c_i c_j) = a^i b a^{j-i} b \bar{a}^j$ (toujours avec la convention, pour $k < 0$, $a^k = \bar{a}^{|k|}$), $\varphi(\bar{c}_i c_j) = \bar{a}^i \bar{b} a^{i+j} b \bar{a}^j$, $\varphi(c_i \bar{c}_j) = a^i b \bar{a}^{i+j} \bar{b} a^j$ et enfin $\varphi(\bar{c}_i \bar{c}_j) = \bar{a}^i b a^{i-j} b a^j$.
En observant quelles sont les seules réductions opérées, on en déduit que l'image de tout mot u non vide de $F(C)$ est un mot de $F(A)$ de longueur au moins égale à $|u| + 2$. En particulier, φ est injectif.

IV.4.c L'image $\varphi(F(C))$ est un sous-groupe de $F(A)$, qui, puisque φ est injectif, est isomorphe au groupe $F(C)$. Or $F(C)$ est de rang n, donc $F(A)$ admet des sous-groupes libres de tout rang fini $n \geqslant 1$.

Partie V — Mots cycliquement réduits et conjugaison

Question V.1
Le mot vide est égal à 1.1.1.
On montre l'existence de la factorisation par récurrence sur la taille du mot $|u|$: si $|u| = 1$, u est cycliquement réduit et $w = 1$ convient.
Supposons l'existence de la factorisation pour tous les mots réduits de longueur au plus égale à n et soit $u \in F(A)$ de longueur $n+1$, $u = u_1 u_2 \dots u_n u_{n+1}$.
Si $u_1 \neq \bar{u}_{n+1}$, u est cycliquement réduit et $w = 1$ convient.
Sinon, notons $u' = u_2 \dots u_n$, $|u'| = n-1$, donc par hypothèse de récurrence il existe une factorisation $u' = \bar{w}vw$ où v est cycliquement réduit. Mais $u = u_1 \bar{w} v w u_{n+1} = \overline{w u_{n+1}}.v.w u_{n+1}$ ce qui fournit une factorisation pour u.
Montrons maintenant l'unicité de cette factorisation, en supposant que $u = \bar{w}_1 v_1 w_1 = \bar{w}_2 v_2 w_2$ où v_1 et v_2 sont cycliquement réduits et $|w_1| < |w_2|$. Comme w_1 est suffixe de u, il est suffixe de w_2 qu'on peut écrire $w_2 = w w_1$ avec $|w| \geqslant 1$. Alors $v_1 = \bar{w}vw$ n'est pas cycliquement réduit, ce qui est la contradiction espérée.

Soit $u \in F(A)$ un mot réduit non vide, qu'on factorise : $u = \bar{w}vw$. On obtient facilement, pour $n > 0$, $u^n = \bar{w}v^n w$, qui est réduit, car v^n l'est (puisque v est cycliquement réduit) et car $\bar{w}v$ et vw aussi (puisque u est lui-même réduit). C'est bien dire que $u^n \neq 1$.

Question V.2
La réflexivité est évidente : $u = 1.u.1$.
La symétrie également car $v = \bar{w} \odot u \odot w \Rightarrow u = w \odot v \odot \bar{w}$, puisque $w^{-1} = \bar{w}$.
Enfin si $v = \bar{w} \odot u \odot w$ et $v' = \bar{w}' \odot v \odot w'$, alors $v' = \bar{w}' \odot \bar{w} \odot u \odot w \odot w' = \overline{w \odot w'} \odot u \odot w \odot w'$.
La conjugaison $\equiv$ est donc bien une relation d'équivalence sur $F(A)$.

Question V.3
Si $u = rs = r \odot s$ et $v = sr$, alors $s = v \odot \bar{r}$ et $u = r \odot v \odot \bar{r}$ donc $u \equiv v$.
Inversement, soit u et v deux mots cycliquement réduits conjugués non vides.
Si $u = v$ on a $u = 1.v$ et $v = v.1$.
Nous supposons désormais que $u \neq v$. On sait qu'il existe un mot $w \in F(A)$ tel que $v = \bar{w} \odot u \odot w$, et nous choisissons un tel mot w de longueur minimale. w n'est pas vide.
Comme v est cycliquement réduit, $v \neq \bar{w}uw$: il y a au moins une réduction, qui ne peut se produire, puisque u et w sont réduits, qu'au contact de $\bar{w}$ et u, ou de u et w.
Soit a la première lettre de w : la réduction se fait si u commence par a ou finit par $\bar{a}$. u étant cycliquement réduit, on est dans l'une ou l'autre de ces situations, pas dans les deux.

- ▷ Si u et w commencent par la même lettre a, les réductions successives se font à la jonction de $\bar{w}$ et u. Comme v est cycliquement réduit, et que $\bar{w}$ commence par $\bar{b}$ où b est la dernière lettre de w, ces réductions "consomment" complètement $\bar{w}$ ou u : si c'est u qui disparaît, c'est que $\bar{w} \odot u = \bar{w}'$ où $w = uw'$, mais alors $v = \bar{w}'uw'$ ce qui contredit la minimalité de w. Autrement dit, c'est $\bar{w}$ qui est effacé dans ces réductions, et $u = ws$ et $v = sw$, ce qui montre que u et v sont permutation cyclique l'un de l'autre.

- ▷ Si u finit par $\bar{a}$ et w commence par a, les réductions successives se font à la jonction de u et w. Là encore, u ne peut complètement être effacé, sans quoi $w = \bar{u}w'$ et $v = \bar{w}'uw'$ ce qui contredirait la minimalité de w. Comme v est cycliquement réduit, w est effacé dans ces réductions, et $u = r\bar{w}$ et $v = \bar{w}r$, ce qui montre que u et v sont permutation cyclique l'un de l'autre.

Question V.4
La factorisation décrite au V.1 se programme aisément : on utilise deux têtes de lecture, en tête et en queue de u, la lecture en tête se fait vers l'avant, et en arrière à la queue. On déplace les têtes tant que les caractères lus sont inverses l'un de l'autre, quand on s'arrête, on a isolé le mot v. Cet algorithme tourne en temps linéaire en la taille du mot u.
On considère deux mots u et u', qu'on factorise de cette manière : $u \equiv v$ et $u' \equiv v'$, où v et v' sont cycliquement réduits. Bien sûr, $u \equiv u' \iff v \equiv v'$: on s'est ramené à la situation de la question V.2. On peut déjà conclure si $|v| \neq |v'|$.
Cette fois, on cherche le plus long préfixe r de v qui est en même temps suffixe de v' (il suffit de lire v de gauche à droite et, en parallèle, v' de droite à gauche). Alors $v = rs$ et $v' = s'r$ et il suffit de regarder si oui ou non $s = s'$: là encore la complexité est linéaire en la taille des mots.

Partie VI — Groupe fondamental d'un graphe

Pour tout chemin $p = e_1 e_2 \dots e_n$, on notera dans la suite $\bar{p} = \bar{e}_n \dots \bar{e}_2 \bar{e}_1$.

Question VI.1
L'étiquette $w = a_1 a_2 \dots a_n$ d'un chemin $p = (u_0, a_1, u_1)(u_1, a_2, u_2) \dots (u_{n-1}, a_n, u_n)$ est réduite si et seulement si il n'y a pas d'indice i tel que $a_{i+1} = \bar{a}_i$. Or si $(u_i, a_i, u_{i+1}) \in \bar{E}$, comme le graphe est réduit, le **seul** triplet de $\bar{E}$ d'étiquette $\bar{a}_i$ et de premier élément u_{i+1} est $(u_{i+1}, \bar{a}_i, u_i)$. Autrement dit, l'étiquette w est réduite si et seulement si dans p n'existe pas de sous-chemin $(u_i, a_i, u_{i+1})(u_{i+1}, \bar{a}_i, u_{i+2} = u_i)$, c'est-à-dire si et seulement si p est réduit.

Question VI.2

Soit x l'étiquette d'un chemin p de s à t et y tel que $x \xrightarrow{1} y$. Montrons que y est l'étiquette d'un chemin de s à t.
Itérant les réductions, on aboutira à $\rho(x)$ qui étiquettera encore un chemin de s à t, chemin qui sera nécessairement réduit d'après la question précédente.
Or, notons $p = (u_0, x_1, u_1)(u_1, x_2, u_2) \dots (u_{n-1}, x_n, u_n)$ avec $u_0 = s$ et $u_n = t$.
Si la réduction a lieu en tête ($x_2 = \bar{x}_1$ donc $y = x_3 \dots x_n$) : l'étude précédente montre que $u_2 = u_0 = s$, et y étiquette le chemin $(u_2 = s, x_3, u_3) \dots (u_{n-1}, x_n, u_n = t)$.
De même, si la réduction a lieu en queue ($x_n = \bar{x}_{n-1}$ donc $y = x_1 \dots x_{n-2}$) : l'étude précédente montre que $u_{n-2} = u_n = t$, et y étiquette le chemin $(u_0 = s, x_1, u_1) \dots (u_{n-3} x_{n-2} u_{n-2} = t)$.
Enfin, si la réduction est au niveau d'un indice i tel que $2 \leqslant i \leqslant n-1$, y étiquette bien un chemin de s à t, ce qui achève la démonstration.

Question VI.3
Bien sûr, comme on ne conserve que des chemins réduits, d'après VI.1, $G(\Gamma, s_0) \subset F(A)$.
Par convention, on sait que $1 \in G(\Gamma, s_0)$.
Si x et y sont dans $G(\Gamma, s_0)$, x étiquette un chemin réduit p de s_0 à s_0, et y étiquette un chemin réduit q de s_0 à s_0.
Alors xy étiquette le chemin pq de s_0 à s_0, donc, $\rho(xy) = x \odot y$ étiquette un chemin réduit de s_0 à s_0 : $G(\Gamma, s_0)$ est bien stable par $\odot$.
Enfin $\bar{x}$ étiquette le chemin $\bar{p}$ de s_0 à s_0 donc $G(\Gamma, s_0)$ est stable par inverse.
On a bien montré que $(G(\Gamma, s_0), \odot)$ est un sous-groupe de $(F(A), \odot)$.

Question VI.4
Si Γ est une forêt, il n'y a qu'un chemin réduit de s_0 à s_0, qui est évidemment étiquetté par 1. Bref : $G(\Gamma, s_0) = \{1\}$.

Question VI.5
Démontrons par récurrence sur $\operatorname{Card} V$ l'existence d'un sous-arbre couvrant.
Bien sûr, si V est un singleton, il n'est pas difficile de trouver un sous-arbre couvrant !
Supposons l'existence du sous-arbre couvrant démontrée pour tout graphe connexe (V, E) tel que $\operatorname{Card} V \leqslant n$. Soit $\Gamma = (V, E)$ un graphe connexe possédant $n+1$ sommets s_0, s_1, …, s_n.
Notons $V' = \{s_0, s_1, \dots, s_{n-1}\}$ et $E' = E \cap (V' \times A \times V')$. Le graphe $\Gamma' = (V', E')$ n'est pas forcément connexe, appelons $\Gamma_1, \dots, \Gamma_q$ ses composantes connexes : pour chacun d'eux, on peut, par hypothèse de récurrence, trouver un sous-arbre couvrant $T_k = (V_k, E_k)$.
Choisissons dans chaque Γ_k un sommet u_k : Γ étant connexe, il existe une arête $e_k = (s_n, a_k, u_k) \in \bar{E}$.
Notons $T = (V, \{e_1, \dots, e_q\} \cup E_1 \cup \dots \cup E_q)$. Montrons que T est un sous-arbre (évidemment couvrant) de Γ.
Deux sommets qui sont dans le même T_k sont reliés par un chemin. S'ils sont dans deux sous-arbres distincts, il existe un chemin passant par s_n qui les relie. Donc T est connexe.
Un chemin réduit passant par s_n relie exactement deux sous-arbres distincts T_i et T_j. Donc si deux sommets x et y sont dans le même T_k, l'unique chemin réduit de T_k qui les relie est aussi le seul chemin dans T. S'ils sont dans deux sous-arbres distincts T_i et T_j, il faut utiliser les arêtes e_i et e_j, pour passer de l'un à l'autre, et il existe un seul chemin réduit de x à u_i dans T_i (*resp.* de u_j à y dans T_j), donc finalement un unique chemin réduit de x à y dans T, qui est donc bien un sous-arbre.
On propose l'algorithme incrémental du programme 1, page 6.

Question VI.6
Bien sûr tous les b_e (et $\bar{b}_e$) sont les étiquettes de chemins réduits de s_0 à s_0.
Soit alors $x \in G(\Gamma, s_0)$, et p un chemin réduit d'étiquette x reliant s_0 à s_0, qu'on factorise sous la forme $p = p_0 e_1 p_1 \dots e_r p_r$ où les p_i sont des chemins réduits dans T et e_i des arêtes de $\bar{E} \setminus \bar{E}_T$.

Recherche d'un arbre couvrant du graphe (V, E)*, avec* $V = \{s_0, s_1, \dots, s_n\}$

$A \leftarrow \{s_0\}$; $B \leftarrow V \setminus A$; $F \leftarrow \emptyset$.
Tant Que $B \neq \emptyset$
    Soit $e = (s, a, s') \in \bar{E}$ reliant un sommet $s \in A$ à un sommet $s' \in B$
    $A \leftarrow A \cup \{s'\}$; $B \leftarrow B \setminus \{s'\}$
    Si $a \in A$, alors $F \leftarrow F \cup \{(s, a, s')\}$ Sinon $F \leftarrow F \cup \{(s', \bar{a}, s)\}$ Fin Si
Fin Tant Que
On renvoie l'arbre $T = (A, F)$

Programme 1 la recherche du sous-arbre couvrant

Notons $e_i = (s_i, a_i, t_i)$, de sorte que p_i est un chemin réduit dans T reliant t_i à s_{i+1}.
Le mot réduit $\bar{x}_{t_i}$ est l'étiquette d'un chemin réduit de t_i à s_0 dans T ; le mot réduit $x_{s_{i+1}}$ est l'étiquette d'un chemin réduit de s_0 à s_{i+1} dans T ; donc $\bar{x}_{t_i} x_{s_{i+1}}$ est l'étiquette d'un chemin (pas forcément réduit) de t_i à s_{i+1} dans T.
Alors le mot réduit $\rho(\bar{x}_{t_i} x_{s_{i+1}}) = \bar{x}_{t_i} \odot x_{s_{i+1}}$ est l'étiquette d'un chemin réduit de t_i à s_{i+1} dans T. Comme t est un arbre, cet unique chemin ne peut être que p_i et on a bien montré que l'étiquette de p_i est $\bar{x}_{t_i} \odot x_{s_{i+1}}$.
En outre p_0 est un chemin réduit de s_0 à s_1 dans T : son étiquette est donc égale à x_{s_1} ; de même, p_r est un chemin réduit de t_r à s_0 dans T : son étiquette est donc égale à $\bar{x}_{t_r}$.
Finalement le mot réduit x se factorise sous la forme

$$\begin{aligned} x &= x_{s_1} a_1 (\bar{x}_{t_1} \odot x_{s_2}) a_2 (\bar{x}_{t_2} \odot x_{s_3}) a_2 \dots a_{r-1} (\bar{x}_{t_{r-1}} \odot x_{s_r}) a_r \bar{x}_{t_r} \\ &= \beta_{e_1} \odot \beta_{e_2} \odot \dots \odot \beta_{e_{r-1}} \odot \beta_{e_r}, \end{aligned}$$

où on a noté $\beta_e = b_e$ si $e \in E$ et $\beta_e = \bar{b}_{\bar{e}}$ si $e \in \bar{E}$.
On a bien factorisé x sous la forme requise.

Question VI.7
Notons $B = E \setminus E_T = \{e_1, \dots, e_r\}$. Posons $\varphi(e_i) = b_{e_i}$.
Il reste à démontrer que φ_F est un isomorphisme du groupe libre $F(B)$ de base B sur $G(\Gamma, s_0)$. La factorisation de la question précédente prouve qu'il s'agit d'un morphisme surjectif.
Soit $e = (s, a, t)$ et $e' = (s', a', t')$ deux arêtes de $\bar{E} \setminus \bar{E}_T$ avec $e \neq \bar{e}'$. Montrons que $|\beta_e \odot \beta_{e'}| \geqslant 2$: cela prouvera que pour tout mot $w \in F(B)$, on a $|\varphi_F(w)| \geqslant |w|$, et donc que φ_F est injectif.
Or $\beta_e = x_s a \bar{x}_t$ et $\beta_{e'} = x_{s'} a' \bar{x}_{t'}$. Si $x_t \neq x_{s'}$, alors la réduction conduit à $\beta_e \odot \beta_{e'} = x_s a y a' \bar{x}_{t'}$ qui est bien de longueur supérieure à 2. Si on avait $x_t = x'_s$, on aurait $s' = t$, et $\beta_e \odot \beta_{e'} = x_s a \odot a' x_{t'}$: $a \odot a' = aa'$ car sinon, $a = \bar{a}$, donc finalement comme $e' = (t, \bar{a}, t')$ et $\bar{e} = (t, \bar{a}, s)$ sont deux arêtes d'un graphe supposé réduit, on aurait $e' = \bar{e}$, ce qu'on a exclu.

Partie VII — Sous-groupes d'un groupe libre

Question VII.1
On utilise les notations proposées par l'énoncé.
Soit x l'étiquette d'un chemin p de s_0 à s_0 dans $\mathcal{A}$: x étiquette le chemin p' de t_0 à t_0 dans $\mathcal{B}$ obtenu en remplaçant dans p toute occurrence de v et v' par w. Donc $x \in L(\mathcal{B})$ et $L(\mathcal{A}) \subset L(\mathcal{B})$.
On en déduit bien sûr que $\rho(L(\mathcal{A})) \subset \rho(L(\mathcal{B}))$. Établissons l'inclusion réciproque.

Il suffit d'établir pour tout mot x qui étiquette un chemin p de t_0 à t_0 dans $\mathcal{B}$ qu'il existe un mot x' étiquettant un chemin de s_0 à s_0 dans $\mathcal{A}$ tel que $\rho(x) = \rho(x')$.
Or si p s'obtient simplement à partir d'un chemin p' de s_0 à s_0 dans $\mathcal{A}$ en remplaçant toute occurrence de v et v' par w, x étiquette bien sûr p' donc $x' = x$ convient.
Sinon, c'est qu'on peut décomposer p sous la forme $p_1 p_2 \dots p_r$, où chaque sous-chemin p_i est aussi (au remplacement près de v par w) un chemin p'_i de $\mathcal{A}$ qui aboutit à v, alors que p_{i+1} est également (au remplacement près de v' par w) un chemin p'_{i+1} de $\mathcal{A}$ mais qui démarre de v' (ou le contraire, bien sûr). Si x_i est l'étiquette de p_i (donc de p'_i également), on a donc $x = x_1 x_2 \dots x_r$. Mais si on intercale entre p'_i et p'_{i+1} le chemin $e'_i = (v, \bar{a}, u)(u, a, v')$ (ou bien $(v', \bar{a}, u)(u, a, v)$) on obtient un chemin $p' = p'_1 e'_1 p'_2 e'_2 \dots e'_{r-1} p'_r$ de $\mathcal{A}$, reliant s_0 à s_0 et d'étiquette $x' = x_1 \bar{a} a x_2 \bar{a} a \dots \bar{a} a x_r$. On a bien sûr $\rho(x') = \rho(x)$, ce qui achève la démonstration.

Question VII.2
On construit un graphe $\Gamma = (V, T)$ de la façon suivante : on introduit un ensemble de sommets $V = \{s_0\} \cup \bigcup_{i=1}^{n} \{s_{i,j}, 1 \leqslant j \leqslant |h_i| - 1\}$. On ajoute les arêtes suivantes : pour tout i dans $\{1, \dots, n\}$, si $|h_i| = 1$ on crée une arête de s_0 vers s_0 étiquettée par l'unique lettre de h_i ; sinon, on crée une arête de s_0 vers $s_{i,1}$, étiquettée par la première lettre de h_i, une arête de $s_{i,|h_i|-1}$ vers s_0 étiquettée par la dernière lettre de h_i, et pour tout $j \in \{2, \dots, |h_i| - 1\}$, on crée une arête de $s_{i,j-1}$ vers $s_{i,j}$ étiquettée par la j-ème lettre de h_i.
Bien sûr, par construction même, notant $\mathcal{A} = (\Gamma, s_0)$, on a $L(\mathcal{A}) = G$.
Les réductions consécutives transforment Γ en un A-graphe réduit Γ', et le sommet s_0 en un sommet éventuellement renommé t_0, tel que, d'après VII.1, on a : $G = L(\mathcal{A}) = L(\mathcal{B})$, où $\mathcal{B} = (\Gamma', t_0)$.
Mais on a vu en VI.7 que $L(\mathcal{B}) = G(\Gamma', t_0)$ est isomorphe à un groupe libre de rang fini. Finalement on a prouvé que G est isomorphe à un groupe libre de rang fini.

Question VII.3
On construit le graphe décrit en VII.2. On le réduit en appliquant successivement les réductions proposées par le préambule de la partie VII. On utilise alors l'algorithme décrit en VI.5 pour déterminer un sous-arbre couvrant. Il reste à appliquer VI.7 pour déterminer une base !

La figure 1 montre un premier exemple, le groupe G engendré par les mots aa, bb, cc, abc et bca.
À gauche, figure le graphe non réduit introduit en VII.2. À droite, figure le graphe réduit et, en rouge, l'arbre défini en partie VI. Le sommet s_0 (ou t_0) est marqué en bleu.
On lit sur la figure de droite une base de G : il suffit de considérer les arêtes qui sont restées noires, et une telle base est constituée des mots aa, abc, $c\bar{b}\bar{a}$, $a\bar{c}b$ et $bc\bar{a}$.

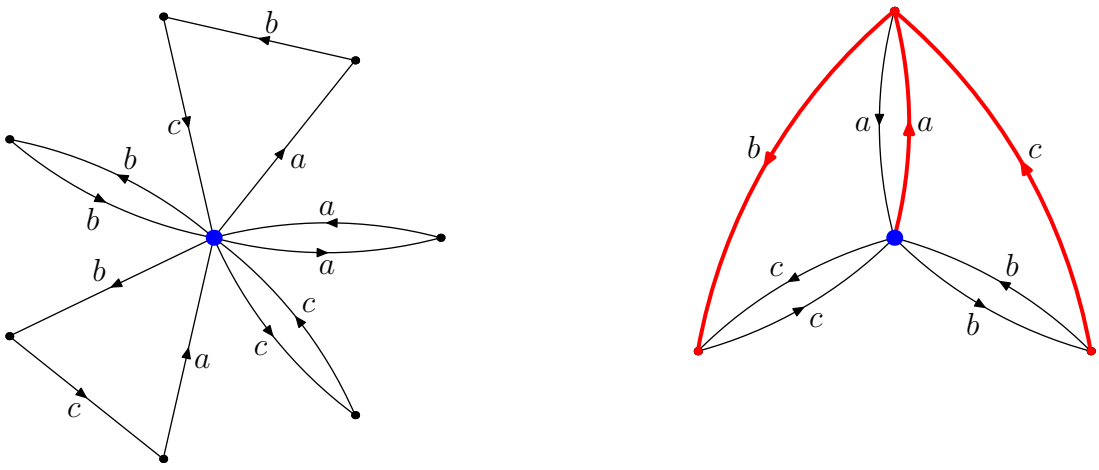

Figure 1 un premier exemple

Le deuxième exemple examine le cas du groupe engendré par $abba$ et $ab\bar{a}$, pour lequel on trouve une base constituée de aba et $ab\bar{a}$.

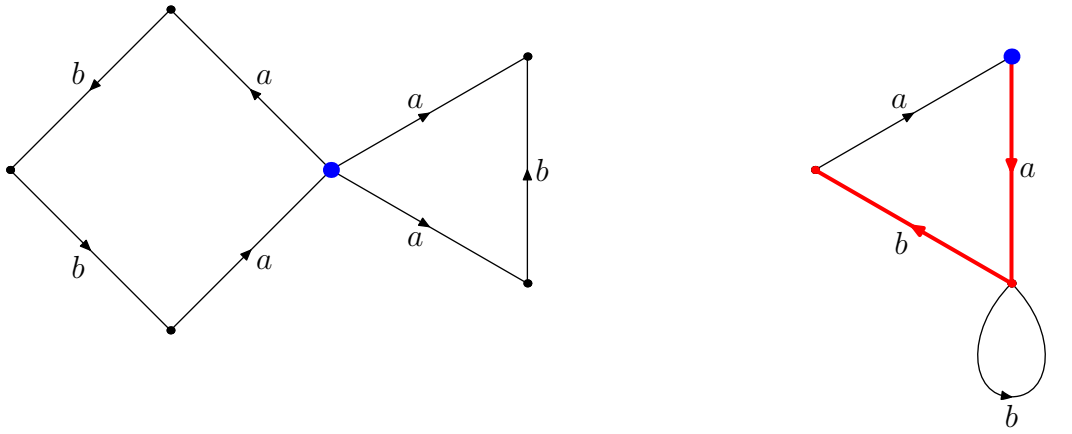

Figure 2 un deuxième exemple

L'exemple du groupe G engendré par $ab\bar{a}$ et ab est éclairant : on trouve la base $\{a, b\}$ de $F(A)$, ce qui est une autre façon de répondre au IV.2.a.

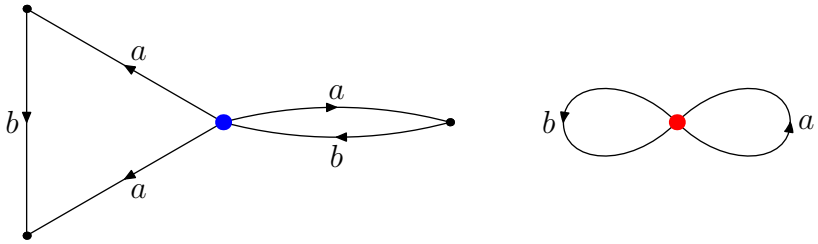

Figure 3 l'exemple du IV.2.a

Et voici encore l'exemple du groupe G engendré par $ab\bar{a}\bar{b}$ et $b\bar{a}\bar{b}a$, pour lequel on trouve qu'il s'agit d'une base du groupe G.

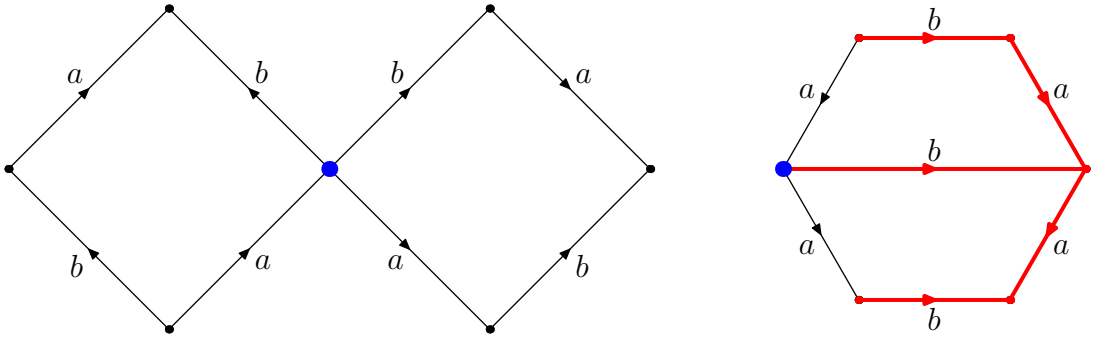

Figure 4 l'exemple du IV.2.b

Notons H la somme des longueurs des mots h_i : le graphe non réduit possède $O(H)$ arêtes et $O(H)$ sommets. Il y aura au plus H réductions, et on construit donc le graphe réduit avec une complexité $O(H^2)$. La recherche du sous-arbre couvrant est également de complexité $O(H^2)$. Enfin, il faut lister les arêtes non reprises dans cet arbre, et calculer le facteur b_e correspondant, ce qui a encore un coût quadratique.
La complexité est donc $O(H^2)$.

Partie VIII — Représentation des groupes libres

Question VIII.1
L'existence du morphisme de groupe φ découle du III.3.c (qui l'appelait φ_F).
On obtient les résultats ci-dessous concernant les images des quatre régions décrites par l'énoncé par α, β et leurs inverses.
On obtient, pour toute partie Z parmi Y_a, Y_b, $Y_{\bar{a}}$ et $Y_{\bar{b}}$, $\alpha(Z) \subset Y_a$, $\beta(Z) \subset Y_b$, $\alpha^{-1}(Z) \subset Y_{\bar{a}}$ et $\beta^{-1}(Z) \subset Y_{\bar{b}}$, à l'exception des inclusions suivantes : $\alpha(Y_{\bar{a}}) = Y_b \cup Y_{\bar{a}} \cup Y_{\bar{b}}$, $\beta(Y_{\bar{b}}) = Y_a \cup Y_{\bar{a}} \cup Y_{\bar{b}}$ et $\alpha^{-1}(Y_a) = Y_a \cup Y_b \cup Y_{\bar{b}}$, $\beta^{-1}(Y_b) = Y_a \cup Y_b \cup Y_{\bar{a}}$.
Notons $\tilde{a} = b$, $\tilde{b} = a$, $\tilde{\bar{a}} = \bar{b}$ et $\tilde{\bar{b}} = \bar{a}$.
On observe qu'avec ces notations, $\varphi(c)(Y_c)$, $\varphi(c)(Y_{\bar{c}})$ et $\varphi(c)(Y_{\tilde{\bar{c}}})$ sont tous les trois inclus dans Y_c, pour tout mot $c \in F(A)$ de longueur 1.
Pour montrer que φ est un morphisme injectif on va montrer que pour tout mot réduit $u \in F(A)$ qui n'est pas le mot vide, $\varphi(u)$ n'est pas l'application identique, en exhibant une partie du plan qui n'est pas égale à son image par $\varphi(u)$.
Soit donc u un mot réduit non vide, qui s'écrit $u = c_1 c_2 \dots c_n$. Observons que si $1 \leqslant i < n$, $c_i \neq \bar{c}_{i+1}$, puisque u est réduit.
Posons $c = c_n$ et $d = \tilde{c}$. Alors $\varphi(u)(Y_c)$ et $\varphi(u)(Y_d)$ sont inclus dans $\varphi(c_1 c_2 \dots c_{n-1})(Y_c)$.
Mais $c_{n-1} \neq \bar{c}$, donc $\varphi(c_1 c_2 \dots c_{n-1})(Y_c) \subset Y_{c_{n-1}}$.
Le même raisonnement, après plusieurs itérations, conduit à $\varphi(c_1 c_2 \dots c_{n-1})(Y_c) \subset Y_{c_1}$. Ainsi : $\varphi(u)(Y_c)$ et $\varphi(u)(Y_d)$ sont tous les deux inclus dans Y_{c_1}, et comme c_1 ne peut être à la fois égal à c et à d, on a bien prouvé que $\varphi(u)$ n'est pas l'application identique, donc que φ est un morphisme injectif.

Question VIII.2
Posons $S = 1 + \sum_{n=1}^{+\infty} (-1)^n a^n$, alors $(1+a)S = 1 + \sum_{k=0}^{+\infty} ((-1)^k + (-1)^{k-1}) a^k = 1$, et, de la même façon, $S(1+a) = 1$.
Donc $1 + a \in U(A)$.

Question VIII.3
Là encore, on note φ le morphisme dont l'existence (sous le nom φ_F) est garantie par III.3.c.
Soit $w = c_1^{n_1} \dots c_r^{n_r}$ un mot réduit non vide de $F(A)$, où chaque n_h est dans $\mathbb{Z}^*$ et où $c_h \neq c_{h+1}$ pour $1 \leqslant h < r$.
Remarquons que le mot $v = c_1 c_2 \dots c_r$ est également un mot réduit de $F(A)$.
Alors $\varphi(w) = \varphi(c_1)^{n_1} \dots \varphi(c_r)^{n_r} = (1 + c_1)^{n_1} \dots (1 + c_r)^{n_r}$ est une série formelle, élément de $U(A)$.
Une récurrence sur $n \geqslant 1$ permet de montrer que $(1+a)^n = 1 + na + \cdots$ et que $(1+a)^{-n} = \left((1+a)^{-1}\right)^n = 1 - na + \cdots$, ou, autrement dit que pour tout entier relatif non nul k, le coefficient de a dans $(1+a)^k$ vaut k.
On écrit alors une nouvelle récurrence sur l'entier $r \geqslant 1$ pour prouver que le coefficient de $c_1 c_2 \dots c_r$ dans $(1 + c_1)^{n_1} (1 + c_2)^{n_2} \dots (1 + c_r)^{n-r}$ est égal à $n_1 n_2 \dots n_r \neq 0$. C'est dire que pour tout mot w non vide, $\varphi(w) \neq 1$, donc que φ est un morphisme injectif, ce qu'il fallait démontrer.