Solutions des exercices du livre « Le calcul des tresses »

(Calvage & Mounet, 2019)

Patrick Dehornoy

Les références à trois chiffres (« 1.4.3 ») concernent le chapitre local. Comme dans le livre, les références à quatre chiffres (« IV.2.2.2 ») concernent les autres chapitres.

Exercices du chapitre I

Exercice 1 (**décalage**).— (i) En suivant le même schéma qu'en 1.4.7, montrer que l'ajout d'un premier brin non tressé définit, pour tout n, un plongement dec_n (comme « décalage ») de l'espace B_n dans B_{n+1}. Ce plongement est-il surjectif ? Anticipant sur 2.3.3, quelle est l'image de σ_i par dec_n ? (ii) Montrer que les plongements dec_n sont compatibles entre eux, et en déduire qu'ils induisent un plongement dec de B_∞ dans lui-même. □

Solution. (i) La construction est symétrique de celle de 1.4.7 : au lieu d'ajouter un $(n+1)^{\text{ième}}$ brin trivial à la droite des n brins, on l'ajoute à gauche. Du coup, la condition technique qui évite toute incursion intempestive de brins est de se restreindre à des tresses triviales hors du prisme $[0,1]\times]1.5,+\infty[\times\mathbb{R}$.

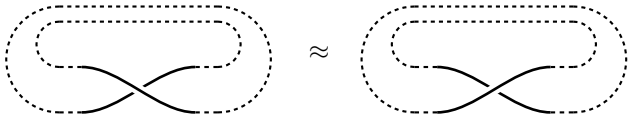
Le plongement dec_n n'est pas surjectif : par construction, σ_1 ne peut appartenir à l'image de dec_n. L'image de σ_i par dec_n est σ_{i+1}, et, symétriquement, celle de $\overline{\sigma}_i$ est $\overline{\sigma}_{i+1}$.

(ii) Les deux opérations d'ajouter un brin sur la droite par e_n et d'ajouter un brin sur la gauche par dec_n commutent : pour toute tresse géométrique β satisfaisant des « contraintes de prisme » *ad hoc*, on a $\mathsf{dec}_n(e_n(\beta)) \approx e_n(\mathsf{dec}_n(\beta))$. De ce fait, si g appartient à B_n, il n'y a pas d'ambiguïté à définir $\mathsf{dec}(g)$ par $\mathsf{dec}(g) := \mathsf{dec}_n(g)$. □

Exercice 2 (**clôture**).— Montrer que les clôtures de deux diagrammes de tresse isotopes sont des diagrammes de nœud isotopes, mais que des diagrammes de tresse non isotopes peuvent avoir des clôtures qui sont des diagrammes d'entrelacs isotopes. [Indication : Comparer les clôtures des tresses de 3.2.7.] □

Solution. Une isotopie entre des sous-diagrammes se prolonge trivialement en une isotopie des diagrammes, de sorte que $\beta \approx \beta'$ implique $\widehat{\beta} \approx \widehat{\beta}'$.

D'un autre côté, les tresses géométriques σ_1 et $\overline{\sigma}_1$ ne sont pas isotopes car leurs nombres d'enlacement sont distincts, respectivement $1/2$ et $-1/2$, mais leurs clôtures sont isotopes, ainsi que le suggèrent les diagrammes suivants :



(ces deux diagrammes étant tous deux isotopes à une simple boucle, c'est-à-dire à un nœud trivial). □

Exercice 3 (**symétrie de l'enlacement**).— Montrer que, pour toute tresse géométrique β et tous i, j, on a $\lambda_{j,i}(\beta) = \lambda_{i,j}(\beta)$. □

Solution. Par définition, pour $i < j$, on a $\theta_{j,i}(t) = \theta_{i,j}(t) + \pi$ pour tout t. On déduit l'égalité des dérivées $\theta'_{j,i} = \theta'_{i,j}$, d'où $\lambda_{j,i}(\beta) = \lambda_{i,j}(\beta)$ par intégration. □

Exercices du chapitre II

Exercice 4 (**sous-monoïde**).— (i) Montrer qu'une partie M' d'un monoïde M est un sous-monoïde de M si, et seulement si, M' contient 1 et est clos par produit (le produit de deux éléments de M' appartient à M'). (ii) En déduire qu'une partie X de M engendre un monoïde M si, et seulement, si tout élément de $M \setminus \{1\}$ peut s'écrire comme produit fini d'éléments de X. □

Solution. (i) Supposons que M' est un sous-monoïde de M, c'est-à-dire que M' muni des opérations induites par celles de M est un monoïde. Notons $\cdot'$ la restriction de $\cdot$ à M. Par hypothèse, $(M', \cdot', 1)$ est un monoïde. Donc, par hypothèse-même, 1 est dans M'. D'autre part, puisque $\cdot'$ est une opération binaire sur M, donc, $a \cdot' b$ est dans M' pour tous a, b dans M' : mais c'est aussi dire que $a \cdot b$ est dans M'.

Réciproquement, supposons que 1 est dans M' et que M' est clos par produit. Alors, par hypothèse, la restriction $\cdot'$ de $\cdot$ à M' est une opération binaire partout définie sur M'. Alors, pour tous a, b, c dans M', on a

$$a \cdot' (b \cdot' c) = a \cdot (b \cdot c) = (a \cdot b) \cdot c = (a \cdot' b) \cdot' c,$$

donc $\cdot'$ est associative. D'autre part, pour tout a dans M', on a

$$a \cdot' 1 = a \cdot 1 = a \quad \text{et} \quad 1 \cdot' a = 1 \cdot a = a,$$

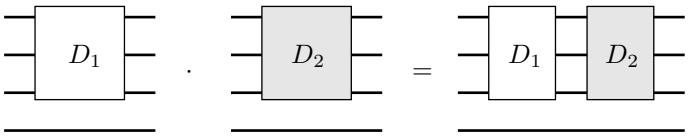
donc $(M', \cdot', 1)$ est un monoïde, donc, par définition, un sous-monoïde de M.

(ii) Supposons que X engendre M, et que a est élément de $M \setminus \{1\}$. Par hypothèse, a appartient au plus petit sous-monoïde incluant X, qui, par (i), est la réunion de $\{1\}$ et de l'ensemble des produits finis d'éléments de X. Donc a est un produit fini d'éléments de X. Inversement, supposons que tout élément de $M \setminus \{1\}$ est produit fini d'éléments de X. Alors tout élément de $M \setminus \{1\}$ est élément de la clôture par produit de X, donc, par (i), élément du plus petit sous-monoïde de M incluant X : c'est dire que X engendre M. □

Exercice 5 (**décalage**).— (i) Montrer que le plongement dec_n de B_n dans B_{n+1} défini dans l'exercice 1 est un homomorphisme. (ii) En déduire que le plongement dec est un endomorphisme non surjectif de B_∞ dans lui-même, et qu'il est caractérisé par le fait qu'il envoie σ_i sur σ_{i+1} pour tout i. □

Solution. (i) Soient D_1 et D_2 des diagrammes de tresse à n brins. Le diagramme ci-dessus exprime que dec_n (ici pour $n = 3$) est un

homomorphisme de B_n dans B_{n+1} :

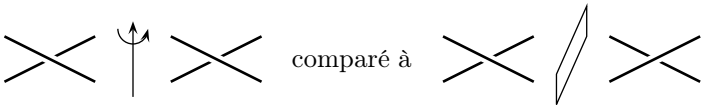


(et l'ajout symétrique d'un brin à droite — c'est-à-dire « au-dessus » — correspondrait au fait que e_n est également un homomorphisme de B_n dans B_{n+1}).

(ii) Comme dans l'exercice 1, les deux opérations d'ajouter un brin sur la droite par e_n et d'ajouter un brin sur la gauche par dec_n commutent : en termes de diagramme de tresse, on a la relation $\mathsf{dec}_n(e_n(D)) \simeq e_n(\mathsf{dec}_n(D))$. De ce fait, si g appartient à B_n, il n'y a pas d'ambiguïté à définir $\mathsf{dec}(g)$ par $\mathsf{dec}(g) := \mathsf{dec}_n(g)$. Par (i), l'application dec est compatible avec le produit, c'est-à-dire qu'il est un endomorphisme de B_∞. Par construction, dec envoie σ_i sur σ_{i+1} pour tout i, et, puisque le groupe B_∞ est engendré par les tresses σ_i, c'est le seul endomorphisme à posséder cette propriété. Cet endomorphisme n'est pas surjectif, car σ_1 n'appartient pas à l'image de dec. □

Exercice 7 (**renversement**).— À quelle transformation des tresses géométriques correspond le renversement ? □

Solution. En termes de tresses géométriques, le renversement correspond à une rotation d'axe vertical passant par le point médian $(1/2, (n+1)/2, 0)$ et d'angle $\pi/2$ — alors que l'inversion (opération $\beta \mapsto \beta^{-1}$) correspond à une symétrie par rapport au plan $\{1/2\}\times\mathbb{R}^2$: dans les deux cas, le fait qu'il y ait antiautomorphisme correspond à une inversion de l'ordre des générateurs, mais le renversement de σ_i est σ_i, alors que l'inversion de σ_i est $\overline{\sigma}_i$, comme le suggèrent les diagrammes



□

Exercice 8 (**présentation de Coxeter de $\mathfrak{S}_3$**).— Montrer que le quotient G du groupe B_3 par la congruence engendré par les relations supplémentaires $\sigma_1^2 = \sigma_2^2 = 1$ est (isomorphe) au groupe symétrique $\mathfrak{S}_3$. [Indication : Utiliser les relations pour montrer que le cardinal de G est au plus 6.] □

Solution. Soit G le groupe $\langle \mathtt{a}, \mathtt{b} \mid \mathtt{a}^2 = \mathtt{b}^2 = 1, \mathtt{aba} = \mathtt{bab} \rangle$. Soit $\equiv$ la congruence engendrée par les relations de la présentation, y compris les relations de groupe libre $\mathtt{aA} = 1$, etc. Premièrement, $\mathtt{a}^2 \equiv 1$ implique $\mathtt{A} \equiv \mathtt{a}$ et, de façon anlogue, $\mathtt{b}^2 \equiv 1$ implique $\mathtt{B} \equiv \mathtt{b}$. Donc tout mot sur $\{\mathtt{a}, \mathtt{b}, \mathtt{A}, \mathtt{B}\}$ est $\equiv$-équivalent à un mot sur $\{\mathtt{a}, \mathtt{b}\}$.

Ensuite, tout tel mot est $\equiv$-équivalent à au moins un des six mots ε, $\mathtt{a}$, $\mathtt{b}$, $\mathtt{ab}$, $\mathtt{ba}$, ou $\mathtt{aba}$. La raison est que, si on concatène $\mathtt{a}$ ou $\mathtt{b}$ à la droite de n'importe lequel de ces six mots, le mot résultant est à nouveau $\equiv$-équivalent à un des ces six mots : par exemple, on trouve $\mathtt{ab} \cdot \mathtt{b} \equiv \mathtt{a}$, et $\mathtt{aba} \cdot \mathtt{b} \equiv \mathtt{aaba} \equiv \mathtt{ba}$. Donc, $\equiv$ a au plus six classes d'équivalence, et G a au plus six éléments.

Prouver que G a exactement six éléments, et reconnaître G exige de montrer que les six mots ε, $\mathtt{a}$, $\mathtt{b}$, $\mathtt{ab}$, $\mathtt{ba}$, et $\mathtt{aba}$ sont deux à deux non $\equiv$-équivalents. On peut utiliser pour cela un $\equiv$-invariant. Définissons $I : \{\mathtt{a}, \mathtt{b}\} \to \mathfrak{S}_3$ par $I(\mathtt{a}) = (1,2)$ et $I(\mathtt{b}) = (2,3)$. Les transpositions $(1,2)$ et $(2,3)$ satisfont les relations de la présentation : nous avons $(1,2)^2 = (2,3)^2 = \mathsf{id}$ et $(1,2)(2,3)(1,2) = (2,3)(1,2)(2,3)$, donc I induit un homomorphisme de G dans $\mathfrak{S}_3$. On vérifie alors que les images par I des mots ε, $\mathtt{a}$, $\mathtt{b}$, $\mathtt{ab}$, $\mathtt{ba}$, et $\mathtt{aba}$ sont des permutations distinctes de $\{1,2,3\}$, donc ces mots sont deux à deux non $\equiv$-équivalents. Donc G a exactement six éléments. Comme I est surjective, elle est aussi injective, et I est un isomorphisme de G sur $\mathfrak{S}_3$. En d'autres termes,

$$\langle \mathtt{a}, \mathtt{b} \mid \mathtt{a}^2 = \mathtt{b}^2 = 1, \mathtt{aba} = \mathtt{bab} \rangle$$

est une présentation du groupe symétrique $\mathfrak{S}_3$. □

Exercice 9 (**neutre**).— Montrer qu'un monoïde ne peut posséder qu'un élément neutre. □

Solution. Si M est un monoïde, et si 1 et $1'$ sont éléments neutres de M, les hypothèses impliquent $1 = 1 \cdot 1' = 1'$. □

Exercice 10 (**monoïde**).— Montrer que $(S^*, \cdot, \varepsilon)$ est un monoïde (proposition 2.1.4). □

Solution. Pour tout S-mot w et pour $1 \leqslant i \leqslant |w|$, notons $w[i]$ la $i^{\text{ième}}$ lettre de w, c'est-à-dire le $i^{\text{ième}}$ élément de w vu comme une suite de longueur $|w|$, donc encore comme une application de $\{1, ..., |w|\}$ dans S. Soient u, v, w des mots sur S. Comme l'addition des entiers est associative, on a d'abord

$$\begin{aligned} |u(vw)| = |u| + |uv| &= |u| + (|v| + |w|) \\ &= (|u| + |v|) + |w| = |uv| + |w| = |(uv)w|, \end{aligned}$$

donc $u(vw)$ et $(uv)w$ ont même longueur.

Ensuite, pour $1 \leqslant i \leqslant |u|$, on trouve

$$(u(vw))[i] = u[i] = (uv)[i] = ((uv)w)[i].$$

De même, pour $|u| + 1 \leqslant i \leqslant |u| + |v|$, on trouve

$$(u(vw))[i] = (vw)[i - |u|] = v[i - |u|] = (uv)[i].$$

Enfin, pour $|u| + |v| + 1 \leqslant i \leqslant |u| + |v| + |w|$, on trouve

$$(u(vw))[i] = (vw)[i-|u|] = w[(i-|u|)-|v|] = w[i-|uv|] = (uv)w[i].$$

Donc les mots $u(vw)$ et $(uv)w$ coïncident toujours, et, par conséquent, la concaténation est associative.

Enfin, soit w un S-mot quelconque. Alors la longueur du mot $w\varepsilon$ est $|w| + |\varepsilon|$, donc est $|w|$. De plus, pour $1 \leqslant i|w|$, on a, par définition, $(w\varepsilon)[i] = w[i]$, donc les mots $w\varepsilon$ et w coïncident. Un vérification similaire montre que εw et w coïncident de même. Par conséquent, ε est élément neutre pour la concaténation et, finalement, $(S^*, \cdot, \varepsilon)$ est un monoïde. □

Exercice 11 (**parties génératrices de** S^*).— Montrer qu'une partie X d'un monoïde S^* est génératrice dans S^* si, et seulement si, X inclut S. □

Solution. Un S-mot de longueur ℓ, disons $s_1 \cdots s_\ell$, est le produit des ℓ mots $s_1, ..., s_\ell$, de longueur 1. Donc, dès que X inclut S, tout mot non vide de S^* est produit fini d'éléments de X, et, par conséquent, X engendre S^*.

Inversement, supposons que X engendre M, et soit s un élément de S. Il doit donc exister $w_1, ..., w_m$ dans X vérifiant $s = w_1 \cdots w_m$,

donc, en particulier, $1 = |w_1| + \cdots + |w_m|$: la seule possibilité est que tous les mots w_i soient vides, sauf l'un d'entre eux, disons w_{i_0}, qui est égal à s. Mais alors on a $w_{i_0} = s$, donc $s \in X$, et S est inclus dans X. □

Exercice 12 (**monoïde libre**).— Démontrer la proposition 2.2.1 : « Pour toute application ϕ de S dans un monoïde M, il existe un unique homomorphisme $\widehat{\phi}$ de S^* dans M étendant ϕ, défini par $\widehat{\phi}(\varepsilon) := 1$ et, pour $w = s_1 \cdots s_\ell$ avec $s_1, ..., s_\ell \in S$, par $\widehat{\phi}(w) := \phi(s_1) \cdots \phi(s_\ell)$. ». □

Solution. La définition de $\widehat{\phi}$ fait sens car un mot dans S^* n'admet qu'une décomposition en produit de lettres de S : si on a $w = s_1 \cdots s_\ell = t_1 \cdots t_m$ avec $s_1, ..., t_m$ dans S, on a nécessairement $\ell = |w| = m$, et $s_i = w(i) = t_i$ pour $1 \leqslant i \leqslant \ell$. Ensuite, $\widehat{\phi}$ prolonge ϕ, et c'est est un homomorphisme car, pour $u = s_1 \cdots s_\ell$ et pour $v = t_1 \cdots t_m$, on trouve

$$\begin{aligned}\widehat{\phi}(uv) = \widehat{\phi}(s_1 \cdots s_\ell t_1 \cdots t_m) &= \phi(s_1) \cdots \phi(s_\ell)\phi(t_1) \cdots \phi(t_m) \\ &= (\phi(s_1) \cdots \phi(s_\ell))\phi((t_1) \cdots \phi(t_m)) = \widehat{\phi}(u)\widehat{\phi}(v),\end{aligned}$$

et, de même,

$$\widehat{\phi}(u\varepsilon) = \widehat{\phi}(u) = \widehat{\phi}(u)\widehat{\phi}(\varepsilon) \quad \text{et} \quad \widehat{\phi}(\varepsilon u) = \widehat{\phi}(u) = \widehat{\phi}(\varepsilon)\widehat{\phi}(u).$$

Enfin, $\widehat{\phi}$ est unique car, s'il prolonge ϕ sur S et est un homomorphisme, il doit obéir à la relation $\phi^*(w) := \phi(s_1) \cdots \phi(s_\ell)$. □

Exercice 13 (**monoïde-quotient**).— Démontrer le lemme 2.2.4 : « Si M est un monoïde et si $\equiv$ une relation d'équivalence sur M, alors l'application envoyant un élément sur sa classe pour $\equiv$ induit une structure de monoïde-quotient sur $M/\equiv$ si, et seulement si, $\equiv$ est une congruence sur M ». □

Solution. Notons $[a]$ la classe d'un élément a de M vis-à-vis de $\equiv$. Supposons que $\equiv$ induit une structure de monoïde-quotient $(M/\equiv, *)$, c'est-à-dire, par définition, que l'application $\phi : a \mapsto [a]$ définit un homomorphisme de M à valeurs dans $(M/\equiv, *)$. Le produit $*$ sur $M/\equiv$ doit donc vérifier

$$[a] * [b] = [ab].$$

Pour que cette égalité ait un sens, il faut que $[ab]$ reste le même quand a et b sont remplacés par d'autres éléments de la même

classe d'équivalence, c'est-à-dire que, si on a $a' \equiv a$ et $b' \equiv b$, on ait aussi $a'b' \equiv ab$. Autrement dit, il faut que $\equiv$ soit une congruence.

Réciproquement, supposons que $\equiv$ est une congruence sur M. Alors (**??**) donne une opération binaire bien définie sur $M/\equiv$. On a alors, pour tous a, b, c dans M,

$$([a] * [b]) * [c] = [ab] * [c] = [abc] = [a] * [bc] = [a] * ([b] * [c]),$$

et $[a] * [1] = [a1] = [a] = [1a] = [1] * [a]$, et $(M/\equiv, *, [1])$ est un monoïde. □

Exercice 14 (**image**).— Montrer que, si M, M' sont des monoïdes, l'existence d'un homorphisme surjectif de M sur M' équivaut à celle d'une congruence $\equiv$ sur M telle que M' soit isomorphe au quotient $M/\equiv$. □

Solution. Supposons que ϕ est un homorphisme surjectif de M sur M'. Soit $\equiv$ la relation binaire sur M par $a \equiv a' \Leftrightarrow \phi(a) = \phi(a')$. Alors $\equiv$ est une congruence sur M (le vérifier !), et ϕ induit une application bien définie $\overline{\phi}$ du quotient $M/\equiv$ dans M' puisque deux éléments d'une même classe ont la même image. Par construction $\overline{\phi}$ est un homomorphisme, et il est bijectif (le varifier !).

Inversement, supposons que $\equiv$ est une congruence sur M. Alors l'application qui à tout élément de M associe sa classe pour $\equiv$ est, par définition, un homomorphisme surjectif de M sur le monoïde-quotient $M/\equiv$. Il existe donc un homomorphisme surjectif de M sur $M/\equiv$ donc, de là, sur tout monoïde isomorphe à $M/\equiv$. □

Exercice 15.— Démontrer le lemme 2.3.4 : « Si M est un monoïde, alors, pour tout sous-ensemble R de $M \times M$, il existe une plus petite congruence incluant R, à savoir la relation « il existe une R-dérivation de a à a' ». □

Solution. Notons $a \equiv_R a'$ pour « il existe une R-dérivation de a à a' ». Alors $\equiv_R$ est réflexive, car, pour tout a, la suite (a) est une R-dérivation de a à a. Elle est symétrique, car, si $(a_0, ..., a_m)$ est une R-dérivation de a à a', alors $(a_m, ..., a_0)$ est une R-dérivation de a' à a. Enfin, $\equiv_R$ est transitive car, si $(a_0, ..., a_m)$ est une R-dérivation de a à a' et si $(b_0, ..., b_p)$ est une R-dérivation

de a' à a'', alors on a $a_m = a' = b_0$, et si $(a_0, ..., a_m, b_1, ..., b_p)$ est une R-dérivation de a à a''. En outre, $\equiv_R$ est compatible avec la multiplication à gauche et à droite, car, si $(a_0, ..., a_m)$ est une R-dérivation de a à a', alors, pour tous x, y dans M, la suite $(xa_0y, ..., xa_my)$ est une R-dérivation de xay à $xa'y$. Donc $\equiv_R$ est une congruence sur M. Enfin, si (b, b') appartient à R, alors (b, b') est une R-dérivation de b à b' : donc $\equiv_R$ inclut R (en tant qu'ensemble de couples).

Inversement, supposons que $\sim$ est une congruence sur M qui inclut R, et supposons que $(a_0, ..., a_m)$ est une R-dérivation de a à a'. Pour chaque i, il existe (b, b') dans R et x, y dans M vérifiant $a_{i-1} = xby$ et $a_i = xb'y$, ou *vice versa*. Puisque $\sim$ inclut R et est symétrique, on a $b \widetilde{b} b'$, et, puisque $\sim$ est compatible avec le produit, on a aussi $xby\widetilde{x}b'y$, d'où $a_{i-1} \sim a_i$. Puisque $\sim$ est transitive, on déduit $a \sim a'$. De là, $\sim$ inclut $\equiv_R$. □

Exercice 16 (**congruence engendrée**).— Montrer que, dans le cas de 2.3.3, la congruence engendrée par le couple $(\mathtt{ab}, \mathtt{ba})$ est la relation « avoir le même nombre de lettres $\mathtt{a}$ et de lettres $\mathtt{b}$ ». □

Solution. Notons $\equiv$ la congruence engendrée, et notons $|w|_s$ le nombre de lettres s dans le mot w. On a $|\mathtt{ab}|_\mathtt{a} = |\mathtt{ba}|_\mathtt{a} = 1$, et $|\mathtt{ab}|_\mathtt{b} = |\mathtt{ba}|_\mathtt{b} = 1$. De là, par induction sur le longueur d'une dérivation, $w \equiv w'$ implique $|w|_\mathtt{a} = |w'|_\mathtt{a}$ et $|w|_\mathtt{b} = |w'|_\mathtt{b}$.

Réciproquement, on montre par induction sur $|w|$ l'équivalence $w \equiv \mathtt{a}^{|w|_\mathtt{a}}\mathtt{b}^{|w|_\mathtt{b}}$ pour tout mot w sur $\{\mathtt{a}, \mathtt{b}\}$. Donc la conjonction de $|w|_\mathtt{a} = |w'|_\mathtt{a}$ et $|w|_\mathtt{b} = |w'|_\mathtt{b}$ implique

$$w \equiv \mathtt{a}^{|w|_\mathtt{a}}\mathtt{b}^{|w|_\mathtt{b}} \equiv \mathtt{a}^{|w'|_\mathtt{a}}\mathtt{b}^{|w'|_\mathtt{b}} \equiv w'.$$ □

Exercice 17 (**monoïdes présentés**).— (i) Soit S quelconque, et soit R l'ensemble des relations $s = 1$ pour s dans S. Montrer que $\langle S \mid R\rangle^+$ est le monoïde trivial à un élément. (ii) Soit S non vide, et soit R l'ensemble des relations $s = t$ pour s, t dans S. En déduire que $\langle S \mid R\rangle^+$ est isomorphe à $(\mathbb{N}, +)$. [Indication : Montrer que la congruence sur S^* engendrée par R est la relation « avoir même longueur ».] (iii) Montrer que $\langle \mathtt{a}, \mathtt{b} \mid \mathtt{ab} = \mathtt{ba}\rangle^+$ est le produit

direct de deux copies du monoïde $(\mathbb{N}, +)$. [Indication : Utiliser l'exercice 16 et montrer que l'application $w \mapsto (|w|_{\mathtt{a}}, |w|_{\mathtt{b}})$, où $|w|_s$ désigne le nombre de s dans w, induit une bijection de $\{\mathtt{a}, \mathtt{b}\}^*/\equiv$ sur $\mathbb{N}^2$, puis que cette bijection est un homomorphisme lorsque $\mathbb{N}^2$ est muni de l'addition coordonnée par coordonnée.]. (iv) Montrer que le monoïde $\langle \mathtt{a} \mid \mathtt{a}^p = 1 \rangle^+$ est isomorphe au groupe cyclique $\mathbb{Z}/p\mathbb{Z}$. [Indication : Montrer que la congruence $\equiv$ sur $\{\mathtt{a}\}^*$ engendrée par $(\mathtt{a}^p, \varepsilon)$ est la relation $|w| = |w'| \pmod p$.] Décrire de même le monoïde $\langle \mathtt{a} \mid \mathtt{a}^p = \mathtt{a}^q \rangle^+$ pour $p, q \geqslant 0$ fixés. □

Solution. (i) Soit $\equiv$ la congruence sur S^* engendrée par $S \times \{\varepsilon\}$, c'est-à-dire par toutes les relations $s = 1$ pour s dans S. Une induction sur $|w|$ montre $w \equiv \varepsilon$ pour tout S-mot w. La relation $\equiv$ n'a donc qu'une seule classe, d'où $\langle S \mid S^* \times \{\varepsilon\} \rangle^+ = \{1\}$.

(ii) Soit $\equiv$ le congruence engendrée, et soit $\mathtt{a}$ une lettre fixée de S. Pour tout mot w, par induction sur $|w|$, on a $w \equiv \mathtt{a}^{|w|}$. Donc la relation $w \equiv w'$ est équivalente à $|w| = |w'|$. L'application qui, à p dans $\mathbb{N}$ associe $\mathtt{a}^p$, est surjective sur $\langle S \mid R \rangle^+$ parce que tout mot est $\equiv$-équivalent à un mot $\mathtt{a}^p$, et elle est injective parce que deux mots de longueurs distinctes ne sont pas $\equiv$-équivalents.

(iii) Soit $\equiv$ la congruence sur $\{\mathtt{a}, \mathtt{b}\}^*$ engendrée par l'unique couple $(\mathtt{ab}, \mathtt{ba})$. On a vu dans l'exercice 16 que $w \equiv w'$ est vérifié si, et seulement si, w et w' ont le même nombre de $\mathtt{a}$ et le même nombre de $\mathtt{b}$. Soit alors ϕ l'application $w \mapsto (|w|_{\mathtt{a}}, |w|_{\mathtt{b}})$, où $|w|_s$ désigne le nombre de s dans w. Alors ϕ induit une bijection de $\{\mathtt{a}, \mathtt{b}\}^*/\equiv$ sur $\mathbb{N}^2$. Ensuite, on a $\phi(uv) = (|uv|_{\mathtt{a}}, |uv|_{\mathtt{b}}) = (|u|_{\mathtt{a}}, |u|_{\mathtt{b}}) + (|v|_{\mathtt{a}}, |v|_{\mathtt{b}})$, donc ϕ est un homomorphisme et, de là, un isomorphisme d'image $(\mathbb{N}, +) \times (\mathbb{N}, +)$.

(iv) Soit $\equiv$ la congruence sur $\{\mathtt{a}\}^*$ engendrée par l'unique couple $(\mathtt{a}^p, \varepsilon)$. Par induction sur la longueur d'une dérivation, on montre que $w \equiv w'$ implique $|w| = |w'| \pmod p$, et réciproquement tout mot w est $\equiv$-équivalent à $\mathtt{a}^q$, où q est l'unique entier de $\{0, 1, ..., p-1\}$ congru à $|w| \bmod p$. Alors l'application ϕ qui associe q à $\mathtt{a}^q$ pour $0 \leqslant q < p$ induit un isomorphisme de $\langle \mathtt{a} \mid \mathtt{a}^p = 1 \rangle^+$ sur le groupe cyclique $\mathbb{Z}/p\mathbb{Z}$.

Soit de même $\equiv$ la congruence sur $\{\mathtt{a}\}^*$ engendrée par l'unique couple $(\mathtt{a}^p, \mathtt{a}^q)$, où l'on suppose $q > p$. Par induction sur la longueur d'une dérivation, on montre que $w \equiv w'$ implique $|w| = |w'|$

mod$(q-p)$. Pour une raison de longueur, les mots ε, $\mathtt{a}$, ..., $\mathtt{a}^{p-1}$ sont isolés, c'est-à-dire sont les seuls éléments de leur classe d'équivalence : en effet, si un mot w a une longueur strictement inférieure à p, et donc à q, aucune relation ne s'applique à w. D'un autre côté, tout mot w de longueur $\geqslant p$ est $\equiv$-équivalent à $\mathtt{a}^{p+r}$, où r est l'unique entier de $\{0, 1, ..., (q-p-1)\}$ congru à $|w|$ mod $(q-p)$. Le monoïde $\langle S \,|\, R\rangle^+$ a donc q éléments, qui sont les classes de ε, $\mathtt{a}$, ..., $\mathtt{a}^{q-1}$, et la table de multiplication est donnée par $[a^r] \cdot [\mathtt{a}^s] := [\mathtt{a}^{f(r+s)}]$ où

$$f(t) := \begin{cases} t & \text{pour } t < p, \\ \text{l'unique élément de } p, ..., q-1 & \\ \qquad \text{congru à } t \text{ mod } (q-p) & \text{sinon.} \end{cases}$$

□

Exercice 18.— Montrer la proposition 2.3.8 : « Un monoïde M engendré par un ensemble S est un quotient du monoïde $\langle S \,|\, R\rangle^+$ si, et seulement si, toutes les relations de R sont vérifiées dans M. »
□

Solution. Si $\equiv$ est la congruence sur S^* engendrée par R, et si $\sim$ est la congruence sur S^* telle que $u \sim v$ est vérifiée si, et seulement si, u et v ont même évaluation dans M, alors les deux conditions équivalent à l'inclusion de $\equiv$ dans $\sim$ (en tant qu'ensembles de couples). □

Exercice 19.— Montrer le lemme 2.3.9 : « Un homomorphisme ϕ défini sur un monoïde S^* vers un monoïde M induit un homomorphisme de $\langle S \,|\, R\rangle^+$ dans M si, et seulement si, on a $\phi(u) = \phi(v)$ pour chaque relation $u = v$ de R. » □

Solution. Notons π la projection canonique de S^* sur $\langle S \,|\, R\rangle^+$, c'est-à-dire sur $S^*/\equiv_R$. La question est de savoir si ϕ *factorise* par π, c'est-à-dire s'il existe un homomorphisme $\dot{\phi}$ vérifiant $\phi = \dot{\phi} \circ \pi$. Or, notant $[w]$ la classe d'un mot w pour la congruence $\equiv$ engendré par R, si $\dot{\phi}$ existe, la seule définition possible est $\dot{\phi}([w]) := \phi(w)$. Le problème est de savoir si la valeur ainsi définie dépend seulement de $[w]$: c'est le cas si, et seulement si, $\pi(w) = \pi(w')$, c'est-à-dire $w \equiv w'$, implique $\phi(w) = \phi(w')$. □

Exercice 20.— Démontrer la proposition 2.4.4 : « Supposons que M est un monoïde engendré par un ensemble S, et que L est un sous-ensemble de S^* contenant exactement un élément par classe de la congruence $\sim$ telle que M est $S^*/\sim$. Pour w dans S^*, soit $\textsc{nf}(w)$ est l'unique élément $\sim$-equivalent à w dans L. Alors M est isomorphe à $(L, *, \textsc{nf}(\varepsilon))$, avec $*$ définie par $u * v := \textsc{nf}(uv)$. De plus, si $\textsc{nf}$ est calculable, le problème de mot de M vis-à-vis de S est décidable. ». □

Solution. Notons $[w]$ l'élément de M représenté par un S-mot w. Alors, par hypothèse, l'application $w \mapsto [w]$ induit une bijection ι de L dans M. Alors, pour tous u, v dans L, on a $[u] \cdot [v] = [uv] = [\textsc{nf}(uv)]$, ce qui est dire que ι est un isomorphisme de $(L, *)$ sur $(M, *)$. Enfin, par construction, on a $[\varepsilon] = 1 = [\textsc{nf}(\varepsilon)]$, et, de là, $\textsc{nf}(\varepsilon)$ est l'élément-unité de $(L, *)$.

Si l'application $\textsc{nf}$ est calculable, elle fournit une solution directe au problème de mot : deux mots u, v représentent le même élément de M si, et seulement si, on a $\textsc{nf}(u) = \textsc{nf}(v)$. Il suffit donc de calculer les mots $\textsc{nf}(u)$ et $\textsc{nf}(v)$, et de tester s'ils sont égaux ou non. □

Exercice 21 (**forme normale**).— Décrire le monoïde $\langle \mathtt{a}, \mathtt{b} \mid \mathtt{ab}^2 = \mathtt{ba} \rangle^+$ en suivant le canevas de 2.4.5. □

Solution. Soit $M := \langle \mathtt{a}, \mathtt{b} \mid \mathtt{ab}^2 = r\mathtt{ba} \rangle^+$. Soit $\equiv$ la congruence engendrée par $\mathtt{ab}^2 = \mathtt{ba}$, et posons $L := \{\mathtt{a}^p\mathtt{b}^q \mid p, q \geqslant 0\}$. Par induction sur la longueur, tout mot est $\equiv$-équivalent à un mot de L.

Il faut montrer que deux mots distincts de L ne sont pas $\equiv$-équivalents. Un premier $\equiv$-invariant est $I_1(w) := |w|_{\mathtt{a}}$. Définissons alors $I_2(w)$ comme la somme de $|w|_{\mathtt{a}}$ (nombre de lettres $\mathtt{a}$ dans w) et, pour chaque lettre $\mathtt{b}$, de 2^n où n est le nombre de $\mathtt{a}$ à la droite de la lettre $\mathtt{b}$ considérée. Par exemple, on trouve $I_2(\mathtt{a}^2\mathtt{baba}) = 1 + 1 + 4 + 1 + 2 + 1 = 10$. Alors I_2 est un $\equiv$-invariant car on a $I_2(\mathtt{ab}^2) = I_2(\mathtt{ba}) = 3$ et, plus généralement, $I_2(u\mathtt{ab}^2v) = I_2(u\mathtt{ba}v)$ pour tous mots u, v : la contribution de $\mathtt{a}$ est dans les deux cas $+1$, et les contribution sde $\mathtt{b}^2$ et de $\mathtt{b}$ sont $2 \times 2^{|v|_{\mathtt{b}}}$. Il en résulte que deux mots distincts de L sont non $\equiv$-équivalents, car $I_1(\mathtt{a}^r\mathtt{b}^s) = r$, et $I_2(\mathtt{a}^r\mathtt{b}^s) = r + s$.

Le monoïde M est le produit semi-direct de deux copies de $(\mathbb{N},+)$, où l'action de la seconde copie sur la premiŕee est par multiplication par 2, c'est-à-dire que la loi de multiplication est donnée par $\mathtt{a}^r\mathtt{b}^s \cdot \mathtt{a}^{r'}\mathtt{b}^{s'} := \mathtt{a}^{r+r'}\mathtt{b}^{s2^{r'}+s'}$. □

Exercice 22.— Démontrer la proposition 3.1.3 : « Pour tout ensemble S, le monoïde F_S est un groupe, et, en tant que groupe, il est engendré par $[S]$. De plus, l'application $x \mapsto [x]$ est une injection de $S \cup \overline{S}$ dans F_S ». □

Solution. Soit w un mot sur $S \cup \overline{S}$, disons $w = x_1 \cdots x_\ell$ avec $x_1, ..., x_\ell$ dans $S \cup \overline{S}$. Dans F_S, on trouve

$$[w] \cdot [\overline{w}] = [x_1] \cdots [x_\ell] \cdot [\overline{x_\ell}] \cdots [\overline{x_1}]. \tag{0.1}$$

Or, comme noté plus haut, pour toute lettre x de $S \cup \overline{S}$, on a $[x] \cdot [\overline{x}] = 1$ dans F_S : les relations de (3.1) ont été choisies pour cela. Par conséquent, $[x_\ell]$ et $[\overline{x_\ell}]$ s'éliminent, suivis de même de $[x_{\ell-1}]$ et $[\overline{x_{\ell-1}}]$, *etc.*, et, finalement, on arrive à $[w] \cdot [\overline{w}] = 1$. Le calcul est semblable pour $[\overline{w}] \cdot \overline{w}$. De là, $[\overline{w}]$ est un inverse pour $[w]$, et F_S est un groupe.

Par définition, une partie X engendre un groupe G si G est le plus petit sous-groupe de G incluant X. Ce dernier étant l'ensemble des éléments de G qui peuvent s'écrire comme produits d'éléments de X et d'inverses d'éléments de X, on déduit que X engendre G si, et seulement si, tout élément de G peut s'écrire comme produits d'éléments de X et d'inverses d'éléments de X. Ici, tout élément g de F_S est la classe d'un mot sur $S \cup \overline{S}$, disons $[x_1 \cdots x_\ell]$ avec $x_1, ..., x_\ell$ dans $S \cup \overline{S}$. Par définition, on a $g = g_1 \cdots g_\ell$ avec $g_i = [s]$ si x_i est une lettre s de S, et $g_i = [s]^{-1}$ si x_i est une lettre $\overline{s}$ de $\overline{S}$. Donc F_S est engendré par $[S]$.

Enfin, soit w un mot vérifiant $[w] = [x]$ avec x dans $S \cup \overline{S}$. Suivant 2.3.4, w est relié à x par une dérivation vis-à-vis des relations de (3.1). Notons $|w|_s$ le nombre de lettres s dans un mot w. Une induction sur la longueur de la dérivation implique, pour tout mot w ainsi relié à x,

$$|w|_x = |w|_{\overline{x}} + 1 \quad \text{et} \quad |w|_s = |w|_{\overline{s}} \quad \text{pour } s \neq x \text{ dans } S \cup \overline{S}.$$

Or, ces égalités ne sont vérifiées par aucune lettre s distincte de x. L'application $s \mapsto [s]$, de $S \cup \overline{S}$ dans F_S, est donc injective. □

Exercice 23.— Démontrer la proposition 3.1.3 : « Pour toute application ϕ de S dans un groupe G, il existe un unique homomorphisme $\widehat{\phi}$ de F_S dans G étendant ϕ. Il est défini par $\widehat{\phi}(1) := 1$, $\widehat{\phi}(\overline{s}) := \phi(s)^{-1}$, et $\widehat{\phi}(w) := \phi(x_1)\cdots\phi(x_\ell)$ pour $w = x_1\cdots x_\ell$ avec $x_1, ..., x_\ell \in S \cup \overline{S}$. ». □

Solution. Soit ϕ une application de S dans un groupe G. On étend d'abord ϕ à $S \cup \overline{S}$ en posant $\phi(\overline{s}) := \phi(s)^{-1}$ pour $\overline{s}$ dans $\overline{S}$. Suivant 2.2.1, il existe alors un unique homomorphisme, qu'on notera ici ϕ^*, du monoïde $(S \cup \overline{S})^*$ dans G (vu comme monoïde) étendant ϕ. On remarque alors que, pour tout s dans S, on a, par construction,

$$\phi^*(s\overline{s}) = \phi(s)\phi(\overline{s}) = \phi(s)\phi(s)^{-1} = 1 = \phi^*(\varepsilon),$$
$$\text{et} \quad \phi^*(\overline{s}s) = \phi(\overline{s})\phi(s) = \phi(s)^{-1}\phi(s) = 1 = \phi^*(\varepsilon).$$

Appliquant 2.2.1 à nouveau, on déduit que ϕ^* induit un homomorphisme $\widehat{\phi}$ du monoïde F_S dans G. Cet homomorphisme est automatiquement un homomorphisme de groupe puisque, pour tout g dans F_S, on a

$$\widehat{\phi}(g)\widehat{\phi}(g^{-1}) = \widehat{\phi}(gg^{-1}) = \widehat{\phi}(1) = 1,$$

donc, nécessairement, $\widehat{\phi}(g^{-1}) = \widehat{\phi}(g)^{-1}$. Enfin, l'unicité de $\widehat{\phi}$ vient de ce que tout homomorphisme ψ du groupe F_S dans G étendant ϕ doit vérifier $\psi(1) := 1$, $\psi(\overline{s}) := \psi(s)^{-1}$, et $\psi(w) := \psi(x_1)\cdots\psi(x_\ell)$ pour $w = x_1\cdots x_\ell$ avec $x_1, ..., x_\ell \in S \cup \overline{S}$. □

Exercice 24 (**groupes cycliques**).— (i) Montrer que $\mathbb{Z}$ est un groupe libre à un générateur. (ii) Montrer que $\mathbb{Z}/n\mathbb{Z}$ n'est pas libre. □

Solution. (i) Par le définition 3.1.1, le groupe libre monogène est le monoïde $M := \langle \mathtt{a}, \mathtt{A} \mid \mathtt{aA} = \mathtt{Aa} = 1\rangle^+$, et, par 3.4.5, les mots réduits constituent une (unique) forme normale pour M. Définissons alors $\phi : \mathsf{Red}_{\mathtt{a}} \to \mathbb{Z}$ par

$$\phi(\mathtt{a}^p) := p, \quad \phi(\varepsilon) := 0, \quad \phi(\mathtt{A}^p) := -p.$$

L'application ϕ est bijective, et elle est un homomorphisme. Neuf combinaisons sont à considérer en fonction des lettres $\mathtt{a}$, ε, ou $\mathtt{A}$.

Typiquement, pour $\mathtt{a}$ et $\mathtt{A}$, on trouve

$$\phi(\mathtt{a}^p) * \phi(\mathtt{A}^q) = \begin{cases} \mathtt{a}^{p-q} & \text{pour } p > q, \\ \varepsilon & \text{pour } p = q, \\ \mathtt{A}^{q-p} & \text{pour } p < q, \end{cases}$$

et, partant, $\phi(\mathtt{a}^p) * \phi(\mathtt{A}^q) = \phi(p-q)$ dans les trois cas. Les huit autres combinaisons sont analogues, et donc ϕ est un isomorphisme. Par conséquent, $(\mathbb{Z}, +)$ est un groupe libre à un générateur.

(ii) On a $[p] = [0]$, alors que, dans le groupe $\mathbb{Z}$, on n'a pas $p = 0$: il ne peut donc exister d'homomorphisme de $\mathbb{Z}/p\mathbb{Z}$ sur $\mathbb{Z}$, et la propriété universelle d'un groupe libre n'est pas respectée. □

Exercice 25 (congruence).— Montrer que, si G est un groupe et si $\equiv$ est une congruence de monoïde sur G, alors $\equiv$ est une congruence de groupe, c'est-à-dire qu'elle est nécessairement compatible avec l'opération d'inverse. □

Solution. Supposons $g \equiv g'$. On déduit

$$g^{-1} = g^{-1}g'g'^{-1} \equiv g^{-1}gg'^{-1} = g'^{-1},$$

donc $\equiv$ est compatible avec l'opération d'inverse. □

Exercice 26.— Démontrer la proposition 3.1.7 : « Soit G un groupe. (i) Si $\equiv$ est une congruence sur G, la classe d'équivalence de 1 est un sous-groupe distingué H de G, et, pour tous g, g' dans G, la relation $g \equiv g'$ équivaut à $g^{-1}g' \in H$. (ii) Inversement, si H est un sous-groupe distingué de G, la relation $\equiv_H$ définie par $g^{-1}g' \in H$ est une congruence sur G, et H est alors la classe de 1. ». □

Solution. La démonstration est bien connue.

(i) Soit H la classe de 1 pour $\equiv$. Pour $g \equiv 1$ et $g \equiv 1$, on a $gh \equiv 1$ et $h^{-1} \equiv 1$ (voir exercice 25). Donc H est un sous-groupe de G. De plus, pour $g \equiv 1$ et h quelconque, on a $hgh^{-1} \equiv hh^{-1} \equiv 1$, donc H est distingué dans G. Alors, pour tous g, g', la relation $g \equiv g'$ équivaut à $g^{-1}g \equiv g^{-1}g'$, donc à $g^{-1}g \equiv 1$, soit à $g^{-1}g' \in H$.

(ii) Soit H un sous-groupe distingué de G, et g, g', g'' quelconques dans G. On a $g^{-1}g = 1 \in H$, donc $g \equiv_H g$, et $\equiv_H$ est réflexive. Si

on a $g^{-1}g' \in H$, on a aussi ${g'}^{-1}g = (g^{-1}g')^{-1} \in H$, donc $g' \equiv_H g$, et $\equiv_H$ est symétrique. Si on a $g^{-1}g' \in H$ et ${g'}^{-1}g'' \in H$, on a aussi $(g^{-1}g')({g'}^{-1}g'') = g^{-1}g'' \in H$, donc $g \equiv_H g''$, et $\equiv_H$ est transitive. Ensuite, supposons $g \equiv_H g'$, et soient h, h' quelconques dans G. On trouve $(hgh')^{-1}(hg'h') = {h'}^{-1}g^{-1}g'h'$, et l'hypothèse que $g^{-1}g'$ appartient à H et que H est distingué implique que $(hgh')^{-1}(hg'h')$ est dans H, donc on a $hgh' \equiv_H hg'h'$. Donc $\equiv_H$ est une congruence. Finalement, $g \equiv_H 1$ équivaut par définition à $g^{-1} \in H$, donc aussi à $g \in H$.

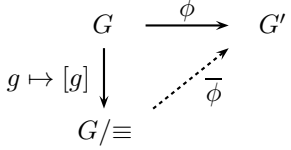
On laisse au lecteur la vérification, très facile, que les deux correspondances sous-groupes distingués $\leftrightarrow$ congruences sont inverses l'une de l'autre. □

Exercice 27 (image et quotient).— Montrer que, si G et G' sont des groupes, alors il existe un homomorphisme surjectif de G sur G' si, et seulement si, il existe une congruence $\equiv$ sur G telle que G' est isomorphe à $G/\equiv$. □

Solution. Supposons que ϕ est un homomorphisme surjectif de G sur G', et définissons $g \equiv g'$ par $\phi(g) = \phi(g')$. Par définition, $\equiv$ est une relation d'équivalence. Supposons $g \equiv g'$ et soit h, h' quelconque. Alors on a

$$\phi(hgh') = \phi(h)\phi(g)\phi(h') = \phi(h)\phi(g')\phi(h') = \phi(hg'h'),$$

donc $hgh' \equiv hg'h'$, et $\equiv$ est une congruence. Ensuite, notons $[g]$ la classe pour $\equiv$ de g. L'application $\overline{\phi} : [g] \mapsto \phi(g)$ est bien définie et injective car $g \equiv g'$ équivaut à $\phi(g) = \phi(g')$. Elle est surjective car tout élément de G' est dans l'image, et elle est un homomorphisme parce que l'on a $\overline{\phi}([gg']) = \phi(gg') = \phi(g) \cdot \phi(g') = \overline{\phi}([g]) \cdot \overline{\phi}([g'])$. Donc G est isomorphe à $G/\equiv$.



Réciproquement, supposons que G' est isomorphe à $G/\equiv$, et considérons $\phi : g \mapsto [g]$. Par construction, l'application ϕ de G dans $G/\equiv$ est surjective. Et, puisque $\equiv$ est une congruence, ϕ est un homomorphisme de G dans $G/\equiv$: en effet, la conjonction de $g \equiv g'$ et

de $h \equiv h'$ implique $gh \equiv g'h \equiv g'h'$, donc $gh \equiv g'h'$, et, par conséquent, $[g] \cdot [h] = [gh]$. Donc il existe un homomorphisme surjectif de G sur G'. □

Exercice 28.— Montrer le lemme 3.1.9 : « Deux S-mots signés représentant le même élément de F_S ont même évaluation dans tout groupe incluant S. ». □

Solution. Par définition, pour toute lettre s de S, on a

$$\mathsf{eval}_G(s\overline{s}) = ss^{-1} = 1 = \mathsf{eval}_G(\varepsilon)$$
$$\mathsf{eval}_G(\overline{s}s) = s^{-1}s = 1 = \mathsf{eval}_G(\varepsilon).$$

Appliquant 2.2.6 à l'alphabet $S \cup \overline{S}$ et à eval_G, on déduit que eval_G induit un homomorphisme bien défini sur $\langle S \cup \overline{S} \,|\, \mathsf{Sym}(S)\rangle^+$, c'est-à-dire sur F_S. □

Exercice 29.— Montrer le lemme 3.1.11 : « Un homomorphisme ϕ défini sur un monoïde $(S \cup \overline{S})^*$ vers un groupe G induit un homomorphisme de $\langle S \,|\, R\rangle$ dans G si, et seulement si, on a $\phi(u) = \phi(v)$ pour chaque relation $u = v$ de R et chaque relation de groupe libre. ». □

Démonstration. Il suffit d'utiliser le lemme 2.3.9 (exercice 19) : si G est un groupe engendré par une famille S, les relations de groupe libre $\mathsf{Sym}(S)$ sont automatiquement vérifiées. □

Exercice 30 (groupes présentés).— Reprendre les présentations de l'exercice 17 et, dans chaque cas, identifier le groupe $\langle S \,|\, R\rangle$ correspondant. □

Solution. (i) Soit $\equiv$ la congruence sur $(S \cup \overline{S})^*$ engendrée par $S \times \{\varepsilon\}$, c'est-à-dire par toutes les relations $s = 1$ pour s dans S, et $\mathsf{Sym}(S)$. Pour toute lettre s, on a $\overline{s} \equiv \overline{s}s \equiv 1$, par $s \equiv 1$ et par $\mathsf{Sym}(S)$. Une induction sur $|w|$ montre alors $w \equiv \varepsilon$ pour tout S-mot signé w. La relation $\equiv$ n'a donc qu'une seule classe, d'où $\langle S \,|\, S^* \times \{\varepsilon\}\rangle = \{1\}$.

(ii) Soit $\equiv$ le congruence engendrée, et soit $\mathtt{a}$ une lettre fixée de S. Pour toute lettre s, on a $\overline{s}s \equiv \mathtt{Aa} \equiv 1$ par $\mathsf{Sym}(S)$ puis $\overline{s}s \equiv \overline{s}\mathtt{a}$ par les relations, d'où $\overline{s}\mathtt{a} \equiv \mathtt{Aa}$, puis $\overline{s} \equiv \overline{s}\mathtt{aA} \equiv \mathtt{AaA} \equiv \mathtt{A}$. Pour tout

mot w, par induction sur $|w|$, on a $w \equiv \mathtt{a}^p$ si le nombre de lettres de S dans w est supérieur de p strictement positif au nombre de lettres de $\overline{S}$, et $w \equiv \varepsilon$ si le nombre de lettres de S dans w est égal au nombre de lettres de $\overline{S}$, et $w \equiv \mathtt{A}^q$ si le nombre de lettres de $\overline{S}$ dans w est supérieur de q strictement positif au nombre de lettres de S. L'application qui, à p dans $\mathbb{Z}$ associe $\mathtt{a}^p$ pour $p > 0$, ε pour $p = 0$, et $\mathtt{A}^{|p|}$ pour $p < 0$, est surjective sur $\langle S \,|\, R\rangle$ parce que tout mot est $\equiv$-équivalent à un mot $\mathtt{a}^p$, ε, ou $\mathtt{A}^q$, et elle est injective parce que deux mots de longueurs distinctes ne sont pas $\equiv$-équivalents.

(iii) Soit $\equiv$ la congruence sur $\{\mathtt{a}, \mathtt{b}, \mathtt{A}, \mathtt{B}\}^*$ engendrée par l'unique couple $(\mathtt{ab}, \mathtt{ba})$. Reprenant l'exercice 16, on montre que $w \equiv w'$ est vérifié si, et seulement si, w et w' ont les mêmes valeurs des différences algébriques $|w|_\mathtt{a} - |w|_\mathtt{A}$ et $|w|_\mathtt{b} - |w|_\mathtt{B}$. Soit alors ϕ l'application $w \mapsto (|w|_\mathtt{a} - |w|_\mathtt{A}, |w|_\mathtt{b} - |w|_\mathtt{B})$. Alors ϕ induit une bijection de $\{\mathtt{a}, \mathtt{b}, \mathtt{A}, \mathtt{B}\}^*/\equiv$ sur $\mathbb{Z}^2$, et $\phi(uv)$ est facilement montré égal à $\phi(u) + \phi(v)$ (tout est addtif). De là, ϕ est un isomorphisme d'image $(\mathbb{Z}, +) \times (\mathbb{Z}, +)$.

(iv) Soit $\equiv$ la congruence sur $\{\mathtt{a}, \mathtt{A}\}^*$ engendrée par l'unique couple $(\mathtt{a}^p, \varepsilon)$ et par $\mathsf{Sym}(\mathtt{a})$. Par induction sur la longueur de w, on montre que tout w est $\equiv$-équivalent à ε ou à un mot $\mathtt{a}^r$ pour $r \in \{1, ..., p-1\}$. Autrement dit, il est loisible d'ignorer la lettre $\mathtt{A}$. Alors la suite est identique au cas du monoïde $\langle \mathtt{a} \,|\, \mathtt{a}^p = 1\rangle^+$, et on trouve à nouveau le groupe cyclique $\mathbb{Z}/p\mathbb{Z}$.

Soit de même $\equiv$ la congruence sur $\{\mathtt{a}, \mathtt{A}\}^*$ engendrée par l'unique couple $(\mathtt{a}^p, \mathtt{a}^q)$ et par $\mathsf{Sym}(\mathtt{a})$. On suppose $q > p$. Par induction sur la longueur de w, on montre que tout w est $\equiv$-équivalent à ε ou à un mot $\mathtt{a}^r$ pour $r \in \{1, ..., q-1\}$, donc il est loisible d'ignorer la lettre $\mathtt{A}$. Cette fois, la suite est identique au cas du monoïde $\langle \mathtt{a} \,|\, \mathtt{a}^p = \mathtt{a}^q\rangle^+$, et on trouve à nouveau la description de l'exercice 17(iv). □

Exercice 31.— Démontrer la proposition 3.2.2 : « Pour toute présentation (S, R), le groupe $\langle S \,|\, R\rangle$ est isomorphe à $F_S/\approx_R$, où $\approx_R$ est la congruence sur F_S engendrée par les relations $[u] = [v]$ pour $u = v$ dans R ». □

Solution. Comme d'habitude, soit $\equiv$ la congruence sur les S-mots signés engendrée par $\mathsf{Sym}(S)$ et soit $\equiv_R$ celle qui est engendrée par $R \cup \mathsf{Sym}(S)$. On va montrer que $w \equiv_R w'$ équivaut à $[w] \approx_R [w']$. Supposons d'abord $w \equiv_R w'$. Il existe donc une $(R \cup \mathsf{Sym}(S))$-dérivation joignant w à $w'0$, disons $(w_0, ..., w_m)$. Dans une telle dérivation, les étapes élémentaires mettent en jeu soit des relations de $\mathsf{Sym}(S)$, soit des relations de R, auquel cas on écrira $\to_R$ (« appliquer une relation de R »). Regroupant les étapes par type, on obtient des indices $i_0 = 0$, j_0, $i_1 = j_0 + 1$, j_1, ..., $i_p = j_{p-1} + 1$, $j_p = m$ vérifiant

$$w = w_{i_0} \equiv w_{j_0} \to_R w_{i_1} \equiv w_{j_1} \to_R \cdots \to_R w_{i_p} \equiv w_{j_p} = w'.$$

Projetant dans F_S, on déduit

$$[w] = [w_{i_0}] = [w_{j_0}] \to_{[R]} [w_{i_1}] = [w_{j_1}] \to_{[R]} \cdots \to_{[R]} [w_{i_p}] = [w_{j_p}] = [w'],$$

donc $[w] \approx_R [w']$.

Inversement, supposons $[w] \approx_R [w']$. Il existe donc une $[R]$-dérivation de $[w]$ à $[w']$ dans le groupe F_S, disons $([w_0], ..., [w_p])$ avec $[w_0] = [w]$ et $[w_p] = [w']$. L'égalité $[w_0] = [w]$ entraîne $w \equiv w_0$, et $[w_p] = [w']$ entraîne $w_p \equiv w'$. Ensuite, pour $0 \leqslant k < p$, on a $[w_k] \to_{[R]} [w_{k+1}]$: par définition, cela signifie qu'il existe des S-mots signés u_k et v_k vérifiant $w_k \equiv u_k \to_R v_k \equiv w_{k+1}$. Alors la suite

$$(w, w_0, w_1, u_1, v_1, w_2, ..., w_{p-1}, u_{p-1}, v_{p-1}, w_p, w')$$

est une $(R \cup \mathsf{Sym}(S))$-dérivation de w à w', et on déduit $w \equiv_R w'$.

De là, on déduit que le monoïde-quotient $(S \cup \overline{S})^*/\equiv_R$, c'est-à-dire le groupe $\langle S \,|\, R\rangle$, est isomorphe au groupe-quotient $F_S/\approx_R$. □

Exercice 32.— Démontrer la proposition 3.2.4 : « Un groupe G engendré par un ensemble S est un quotient du groupe $\langle S \,|\, R\rangle$ si, et seulement si, toutes les relations de R sont vérifiées dans G. ». □

Solution. Par 2.3.8, le groupe G vu comme monoïde est quotient du monoïde $\langle S \cup \overline{S} \,|\, R \cup \mathsf{Sym}(S)\rangle^+$ si, et seulement si, les relations de R et celles de $\mathsf{Sym}(S)$ sont vérifiées dans G. Puisque G est un groupe, les relations de $\mathsf{Sym}(S)$ sont vérifiées par hypothèse, et il ne reste que celles de R. □

Exercice 33.— Montrer la proposition 3.2.5 : « Supposons que G est un groupe engendré par un sous-ensemble S, que R est une liste de relations vérifiées dans G, et qu'il existe un ensemble E de S-mots signés tels que

(i) tout S-mot signé est R-équivalent à un mot de E,

(ii) l'application eval_G est injective sur E.

Alors G admet la présentation $\langle S \,|\, R\rangle$. ». □

Solution. Soit $\equiv$ la congruence sur les S-mots signés telle que le groupe $\langle S \,|\, R\rangle$ est $(S \cup \overline{S})^*/\equiv$, et, de même, soit $\sim$ la congruence telle que $\langle S \,|\, R\rangle$ est $(S \cup \overline{S})^*/\sim$. Puisque les relations de R sont vérifiées dans G, la relation $w \equiv w$ implique $w \sim w'$ (et donc G est quotient de $\langle S \,|\, R\rangle$). Inversement, supposons $w \sim w'$. Par (i), il existe w_0 et w'_0 dans E vérifiant $w \equiv w_0$ et $w' \equiv w'_0$. Puisque $\equiv$ est incluse dans $\sim$, on a également $w \sim w_0$ et $w' \sim w'_0$, donc $w_0 \sim w'_0$. Par (ii), on déduit $w_0 = w'_0$, et, de là, $w \equiv w_0 = w'_0 \equiv w'$, d'où $w \equiv w'$. Par conséquent, les congruences $\equiv$ et $\sim$ coïncident, et G et $\langle S \,|\, R\rangle$ sont isomorphes. □

Exercice 34.— Sur le modèle de l'algorithme 5, donner une solution au problème de mot pour le groupe présenté $\langle \mathtt{a}, \mathtt{b} \,|\, \mathtt{ab} = \mathtt{ba}\rangle$. □

Solution. Il suffit de remplacer le nombre de $\mathtt{a}$ dans le mot w considéré par la différence algébrique $|w|_{\mathtt{a}} - |w|_{\mathtt{A}}$ et, de même, le nombre de $\mathtt{b}$ dans w par la différence algébrique $|w|_{\mathtt{b}} - |w|_{\mathtt{B}}$. Voici une proposition :

Algorithme : PROBLÈME DE MOT POUR $\langle \mathtt{a}, \mathtt{b} \,|\, \mathtt{ab} = \mathtt{ba}\rangle$

Entrée : un mot signé w dans $\{\mathtt{a}, \mathtt{b}, \mathtt{A}, \mathtt{B}\}^*$
Sortie : **oui** si w représente 1 dans $\langle \mathtt{a}, \mathtt{b} \,|\, \mathtt{ab} = \mathtt{ba}\rangle$, **non** sinon

```
1 : POSER p := |w|_a − |w|_A
2 : POSER q := |w|_b − |w|_B
3 : si p = 0 et q = 0 alors
4 :     RENVOYER oui
5 : sinon
6 :     RENVOYER non
```

□

Exercice 35.— Démontrer le lemme 3.4.3 : « Tout mot de $(S \cup \overline{S})^*$ se réduit à un unique mot réduit ». □

Solution. On va établir par induction sur $\ell \geqslant 0$ la propriété

$(\mathcal{P}_\ell)$ Si on a $w \to^* w'$ et $w \to^* w''$ avec w' réduit et $|w| - |w'| = 2\ell$, alors a $w'' \to^* w'$.

Supposons d'abord $\ell = 0$. On a donc $w' = w$, donc w est réduit, et, de là, $w \to^* w''$ entraîne $w'' = w$, d'où, trivialement, $w'' \to^* w'$.

Supposons maintenant $\ell > 0$. Soit $w \to w'_1 \to^* w'$ une réduction de w à w'. Si on a $w'' = w$, alors $w'' \to^* w'$ est vérifié par hypothèse. Sinon, soit $w \to w''_1 \to^* w''$ une réduction de w à w''. Si les mots w'_1 et w''_1 coïncident, on a $w'_1 \to^* w'$ et $w'_1 \to^* w''$ avec w' réduit et $|w'_1| - |w'| = 2\ell - 2$, et $(\mathcal{P}_{\ell-1})$, qui est vérifiée par hypothèse d'induction, entraîne $w'' \to^* w'$.

Reste le cas $w'_1 \neq w''_1$. Ceci ne peut se produire que on a réduit deux facteurs différents pour aller de w à w'_1 et de w à w''_1. Deux cas sont possibles *a priori*. Ou bien les deux facteurs réduits se chevauchent, auquel cas ils sont nécessairement du type $s\overline{s}$ et $\overline{s}s$ avec la lettre $\overline{s}$ en commun, et il existe alors deux mots x et y vérifiant $w = xs\overline{s}sy$, menant à $w'_1 = xsy = w''_1$, qui contredit l'hypothèse $w'_1 \neq w''_1$.

Ou bien, et c'est le seul cas restant, les deux facteurs réduits ne se chevauchent pas. Il existe alors deux lettres s, t de $S \cup \overline{S}$ et des mots x, y, z vérifiant $w = xs\overline{s}yt\overline{t}z$, $w'_1 = xyt\overline{t}z$, et $w'_2 = xs\overline{s}yz$, ou *vice versa*. On a alors $w'_1 \to xyz$ et $w''_1 \to xyz$. Puisqu'on a $w'_1 \to^* w_1$ et $w'_1 \to xyz$ avec w_1 irreductible et $|w'_1| - |w'| = 2\ell - 2$, la propriété $(\mathcal{P}_{\ell-1})$, qui est vérifiée par hypothèse d'induction, entraîne $xyz \to^* w'$. Par transitivité, on en déduit $w''_1 \to^* w'$. Mais alors, on a $w''_1 \to^* w'$ et $w''_1 \to w''$ avec w' irreductible et $|w''_1| - |w'| = 2\ell - 2$, un nouvel appel à l'hypothèse d'induction $(\mathcal{P}_{\ell-1})$ donne $w'' \to^* w'$, comme escompté.

Oubliant l'indice ℓ dans $(\mathcal{P}_\ell)$, on déduit que, si on a $w \to^* w'$ et $w \to^* w''$ avec w' réduit, alors on a $w'' \to^* w'$. L'unicité cherchée en résulte. En effet, supposons que l'on a à la fois $w \to^* w'$ et $w \to^* w''$ avec w' et w'' réduits. Par ce qu'on vient de voir, on doit avoir $w'' \to^* w'$. Puisque w'' est réduit, la seule possibilité est $w'' = w'$. □

Exercice 36.— Démontrer la proposition : « Les mots réduits forment une forme normale pour F_S ». □

Solution. Notons $\equiv$ la congruence sur le monoïde $(S \cup \overline{S})^*$ engendrée par les relations de (3.1). Il s'agit de montrer que chaque classe d'équivalence pour $\equiv$ contient un et un seul mot réduit.

D'abord, par définition, on a $s\overline{s} \equiv \varepsilon$ et $\overline{s}s \equiv \varepsilon$ pour toute lettre s, d'où il résulte que $w \to w'$, puis, par une induction immédiate, $w \to^* w'$ entraînent $w \equiv w$. Par conséquent, les réductions se passent sans changer de classe d'équivalence et, puisque tout mot se réduit à un mot réduit, toute classe d'équivalence contient au moins un mot réduit. Le point est de montrer qu'elle n'en contient qu'un seul.

Pour cela, notons $w \sim w'$ pour $\mathsf{red}(w) = \mathsf{red}(w')$, où red est la fonction introduite en 3.4.4. Alors $\sim$ est une relation d'équivalence sur $(S \cup \overline{S})^*$. On va maintenant montrer que c'est même une congruence, c'est-à-dire qu'elle est compatible avec le produit à gauche et à droite. Supposons donc $u \sim u'$ et $v \sim v'$. On a alors $uv \to^* \mathsf{red}(u)\mathsf{red}(v)$, donc, par 3.4.3, $\mathsf{red}(uv) = \mathsf{red}(\mathsf{red}(u)\mathsf{red}(v))$ et, de même, $\mathsf{red}(u'v') = \mathsf{red}(\mathsf{red}(u')\mathsf{red}(v'))$, d'où $\mathsf{red}(uv) = \mathsf{red}(u'v')$, soit $uv \sim u'v'$.

De plus, on a $\mathsf{red}(s\overline{s}) = \mathsf{red}(\overline{s}s) = \varepsilon = \mathsf{red}(\varepsilon)$, soit $s\overline{s} \sim \varepsilon$ et $\overline{s}s \sim \varepsilon$ pour toute lettre s de S. Donc $\sim$ est une congruence sur $(S \cup \overline{S})^*$ qui contient toutes les paires $(s\overline{s}, \varepsilon)$ et $(\overline{s}s, \varepsilon)$. Puisque $\equiv$ est la plus petite des congruences ayant ces propriétés, on déduit que $\sim$ inclut $\equiv$, c'est-à-dire que $w \equiv w'$ entraîne $w \sim w'$, soit $\mathsf{red}(w) = \mathsf{red}(w')$. Par conséquent, une classe d'équivalence pour $\equiv$ ne contient qu'un seul mot réduit. □

Exercice 37 (**groupe présenté**).— Montrer que le groupe $\langle S \mid R \rangle$ est quotient du groupe libre F_S par le sous-groupe distingué engendré par les éléments $\mathsf{red}(u^{-1}v)$ pour $u = v$ relation de R. □

Solution. Soit $\equiv$ la congruence telle que $\langle S \mid R \rangle$ est $F_S/\equiv$, et soit H le sous-groupe distingué engendré par les éléments $\mathsf{red}(u^{-1}v)$ pour $u = v$ relation de R. Par induction sur la longueur ℓ d'une dérivation de g à g', on montre que $g^{-1}g'$ appartient à H^ℓ, donc à H, autrement dit que $g \equiv g'$ implique $g^{-1}g' \in H$.

Inversement, $g^{-1}g' \in H$ implique l'existence d'une suite finie d'éléments de la forme $h_i^{-1}\mathsf{red}(u_i^{-1}v_i)h_i$ avec $u_i = v_i$ relation de R dont $g^{-1}g'$ est le produit : pour chaque relation $u_i = v_i$ de R, on a

$$\mathsf{red}(u_i) \equiv u_i \equiv v_i \equiv \mathsf{red}(v_i),$$

et, par conséquent, $\mathsf{red}(u_i^{-1}v_i) \equiv 1$, et, par suite, $h_i^{-1}\mathsf{red}(u_i^{-1}v_i)h_i \equiv 1$, et, par produit, $g^{-1}g' \equiv 1$, soit $g \equiv g'$.

On remarque en outre que, par la proposition 3.1.7 (exercice 26), le sous-groupe H coïncide avec le sous-groupe canoniquement associé à la congruence $\equiv$. □

Solutions aux exercices du chapitre III

Exercice 38 (inverse).— Montrer que l'élément-unité 1 est le seul élément inversible de B_n^+ pour tout $n \leqslant \infty$. □

Solution. Soit $a \neq 1$ dans B_n^+. Pour tout élément b, on a alors $|ab| = |a| + |b| \geqslant |a| > 0$, donc $ab \neq 1$, ce qui montre que a n'a pas d'inverse dans B_n^+. □

Exercice 39 (problème de mot).— Écrire la solution ci-dessus sous la forme d'un algorithme en pseudo-code. □

Solution. Le principe est de construire exhaustivement la classe d'équivalence $[w]^+$ de w par saturation de l'application des relations de tresse, indépendamment du mot w', et de finalement tester si w' appartient à $[w]^+$. On remarque que, étant donné que le nombre de mots de tresse de $\mathcal{BW}_n^+$ de longueur ℓ est fini et égal à $(n-1)^\ell$, le nombre d'étapes menant à la saturation est borné par $(n-1)^\ell$, correspondant à une simple boucle **pour** sans qu'il soit besoin d'une boucle **tant que**.

Pour u, v mots de tresse positifs, notons $u \to v$ s'il existe une relation de tresse s'appliquant à u et dont le résultat est v (il n'y a pas unicité en général : plusieurs applications d'une relation de tresse à u sont possibles). Une proposition d'implémentation est :

Algorithme : PROBLÈME DE MOT POUR B_∞^+

Entrée : deux mots w, w' de $\mathcal{BW}_\infty^+$
Sortie : **oui** si w et w' représentent le même élément de B_∞^+, **non** sinon

```
1 : CHOISIR n tel que w ∈ BW_n^+
2 : POSER ℓ := |w| et m := (n−1)^ℓ
3 : POSER C := {w}
4 : pour k := 1 à m faire
5 :     POSER C := C ∪ {v ∈ BW_n^+ | u ∈ C et u → v}
            [à ce stade, C est la classe d'équivalence complète de w]
6 : si w' ∈ C alors
7 :     RENVOYER oui
8 : sinon
9 :     RENVOYER non
```

□

Exercice 40 (**décalage**).— (i) Montrer que l'application $\sigma_i \mapsto \sigma_{i+1}$ imduit un endomorphisme dec^+ de B_∞^+ dans lui-même. (ii) Montrer que dec^+ est injectif, mais non surjectif. □

Solution. (i) Si (u, v) est une paire de mots de tresse de la forme $(\sigma_i\sigma_{i+1}\sigma_i, \sigma_{i+1}\sigma_i\sigma_{i+1})$ ou $(\sigma_i\sigma_j, \sigma_j\sigma_i)$ avec $|i-j| \geqslant 2$, il en est de même de $(\mathsf{dec}^+(u), \mathsf{dec}^+(v))$. Il en résulte, par induction sur le nombre de relations de tresse mis en jeu, que $u \equiv^+ v$ implique $\mathsf{dec}^+(u) \equiv^+ \mathsf{dec}^+(v)$. Par II.2.2.1, il s'ensuit que dec^+ induit un endomorphisme de B_∞^+.

(ii) Par construction, σ_1 n'est pas dans l'image de dec^+.

D'un autre côté, soit $\mathcal{BW}_{\geqslant 2}^+$ l'ensemble des mots de tresse positifs dont σ_1 est absent et, pour w dans $\mathcal{BW}_{\geqslant 2}^+$, soit $f(w)$ l'image de w par $\sigma_i \mapsto \sigma_{i-1}$. Comme ci-dessus *mutatis mutandis*, $w \equiv^+ w'$ implique $f(w) \equiv^+ f(w')$. Supposons alors $\mathsf{dec}^+(u) \equiv^+ \mathsf{dec}^+(v)$. Par construction, $\mathsf{dec}^+(u)$ et $\mathsf{dec}^+(v)$ appartiennent à $\mathcal{BW}_{\geqslant 2}^+$, et on a $u = f(\mathsf{dec}^+(u)) \equiv^+ f(\mathsf{dec}^+(v)) = v$. □

Exercice 41 (**groupe envelopant**).— (i) Montrer que, pour toute présentation de monoïde (S, R), l'identité de S induit un homomorphisme ι du monoïde $\langle S \mid R\rangle^+$ dans le groupe $\langle S \mid R\rangle$. (ii)

Montrer qu'alors tout homomorphisme de $\langle S \,|\, R\rangle^+$ vers un groupe se factorise par ι. □

Solution. (i) Toutes les relations de R étant satisfaites dans $\langle S \,|\, R\rangle$, il résulte de 2.3.8 que l'identité de S induit un homomorphisme ι du monoïde $\langle S \,|\, R\rangle^+$ dans le groupe $\langle S \,|\, R\rangle$.

(ii) Soit ϕ un homomorphisme du monoïde $\langle S \,|\, R\rangle^+$ vers un groupe G. Notons $\equiv^+$ et $\equiv$ les congruences mises en jeu. Pour voir que ϕ se factorise par $\langle S \,|\, R\rangle$, il suffit de montrer que $[g] = [g']$, c'est-à-dire $g \equiv g'$, implique $\phi(g) = \phi(g')$. Or, si on a $g \equiv g'$, il existe une $R \cup \mathsf{Sym}(S)$-dérivation de g à g'. Dans le cas d'une seule relation, dans le cas de R, on a $\phi(g) = \phi(g')$ par hypothèse, et, dans le cas de $\mathsf{Sym}(S)$ et pour $g = hs\overline{s}h'$ et $g' = hh'$ (et autres cas analogues), on a, parce que ϕ est à valeurs dans un groupe,

$$\phi(g) = \phi(hs\overline{s}h') = \phi(h)\phi(s)\phi(s)^{-1}\phi(h') = \phi(hh') = \phi(g').$$

Par induction sur la longueur d'une dérivation de g à g', on déduit que $g \equiv g'$ implique $\phi(g) = \phi(g')$.

$$\begin{array}{ccc} \langle S \,|\, R\rangle^+ & \xrightarrow{\ \phi\ } & G \\ {\scriptstyle [g]^+ \mapsto [g]}\big\downarrow & \nearrow_{\overline{\phi}} & \\ \langle S \,|\, R\rangle & & \end{array}$$

□

Exercice 42 (non-plongement).— Soit M le monoïde présenté $\langle \mathtt{a}, \mathtt{b}, \mathtt{c} \,|\, \mathtt{ab} = \mathtt{ac}\rangle^+$ et G le groupe présenté $\langle \mathtt{a}, \mathtt{b}, \mathtt{c} \,|\, \mathtt{ab} = \mathtt{ac}\rangle$. Montrer que M ne se plonge pas dans G. [Indication : Montrer que, dans le groupe, on a $\mathtt{b} = \mathtt{c}$, alors que, dans le monoïde, on a $\mathtt{b} \neq \mathtt{c}$.] □

Solution. Dans le groupe G, on a $\mathtt{ab} = \mathtt{ac}$, donc $\mathtt{b} = \mathtt{c}$, alors que, dans le monoïde M, on n'a pas l'égalité $\mathtt{b} = \mathtt{c}$, et le morphisme induit par l'identité sur $\{\mathtt{a}, \mathtt{b}, \mathtt{c}\}$ n'est pas injectif. En effet, notant $\equiv^+$ et $\equiv$ les congruences de monoïde et de groupe impliquées, on obtient $\mathtt{b} \equiv \mathtt{a}^{-1}\mathtt{ab} \equiv \mathtt{a}^{-1}\mathtt{ac} \equiv \mathtt{c}$, tandis que $\mathtt{b} \equiv^+ \mathtt{c}$ est faux puisqu'aucune dérivation ne s'applique ici aux mots de longueur un. □

Exercice 43 (**simplifiable**).— Montrer qu'un monoïde libre est simplifiable. □

Solution. Soit S^* le monoïde libre engendré par S. Il suffit, par induction sur la longueur du mot à simplifier sur la gauche, de montrer que, pour toute lettre de S et tous mots u, v de S^*, la relation $su = sv$ implique $u = v$. Or, u est le suffixe de longueur $|su| - 1$ du mot su, et v est le suffixe de longueur $|sv| - 1$ du mot sv : l'hypothèse $su = sv$ implique donc $u = v$. L'argument est symétrique à droite. □

Exercice 44 (**automorphisme**).— Montrer que, pour tout a dans B_n^+, on a $a\Delta_n = \Delta_n \phi_n(a)$. □

Solution. Le lemme 1.3.6 donne le résultat pour a de longueur 1. Pour le cas général, on procède par induction sur la longueur de a. Supposant $a = b\sigma_i$, on obtient

$$\begin{aligned} a\Delta_n = b\sigma_i\Delta_n &= b\Delta_n\sigma_{n-i} && \text{par (1.13)} \\ &= \Delta_n\phi_n(b)\sigma_{n-i} && \text{par hypothèse d'induction} \\ &= \Delta_n\phi_n(a). \end{aligned}$$

□

Exercice 45 (**mots $\underline{\partial}_n(\sigma_i)$**).— Déterminer les mots $\underline{\partial}_4(n)\sigma_i$ pour $n \geqslant 5$ et $i < n$. □

Solution. Mis à part les premières valeurs, les mots $\underline{\partial}_n(\sigma_i)$ ne sont pas uniques. On va calculer ici les valeurs issues de la démonstration inductive de 1.3.7. Pour commencer, on trouve $\underline{\Delta}_3 := \sigma_1\sigma_2\sigma_1$, impliquant directement $\underline{\partial}_3(\sigma_1) := \sigma_2\sigma_1$ et $\underline{\partial}_3(\sigma_2) := \sigma_1\sigma_2$ (valeurs uniques).

Supposons $n := 4$, et d'abord $i \leqslant 2$. La démonstration donne alors la solution $\underline{\partial}_4(\sigma_i) := \underline{\partial}_3(\sigma_i)\,\underline{\sigma}_{4,1}$, soit

$\underline{\partial}_4(\sigma_1) := \sigma_2\sigma_1 \cdot \sigma_3\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_3\sigma_2\sigma_1$,
$\underline{\partial}_4(\sigma_2) := \sigma_1\sigma_2 \cdot \sigma_3\sigma_2\sigma_1 = \sigma_1\sigma_2\sigma_3\sigma_2\sigma_1$.

D'un autre côté, supposons $i := 3$. Soit $\mathsf{dec}(\underline{\Delta}_3)$ le mot obtenu à partir de $\underline{\Delta}_3$ en décalant tous les indices des générateurs σ_i de $+1$, à savoir $\sigma_2\sigma_3\sigma_2$. La démonstration donne maintenant la solution $\underline{\partial}_4(\sigma_3) := \underline{\sigma}_{3,1}\mathsf{dec}(\underline{\Delta}_3)$, soit

$\underline{\partial}_4(\sigma_3) := \sigma_2\sigma_1 \cdot \sigma_2\sigma_3\sigma_2 = \sigma_2\sigma_1\sigma_3\sigma_2\sigma_1$.

Le cas $n := 5$ est similaire. Pour $i \leqslant 3$, on trouve

$$\underline{\partial}_5(\sigma_1) := \underline{\partial}_4(\sigma_1)\,\underline{\sigma}_{5,1} = \sigma_2\sigma_1\sigma_3\sigma_2\sigma_1\sigma_4\sigma_3\sigma_2\sigma_1,$$
$$\underline{\partial}_5(\sigma_2) := \underline{\partial}_4(\sigma_2)\,\underline{\sigma}_{5,1} = \sigma_1\sigma_2\sigma_3\sigma_2\sigma_1\sigma_4\sigma_3\sigma_2\sigma_1,$$
$$\underline{\partial}_5(\sigma_3) := \underline{\partial}_4(\sigma_3)\,\underline{\sigma}_{5,1} = \sigma_2\sigma_1\sigma_3\sigma_2\sigma_1\sigma_4\sigma_3\sigma_2\sigma_1,$$

et, pour $i := 4$, on trouve

$$\underline{\partial}_5(\sigma_4) := \underline{\sigma}_{4,1}\mathsf{dec}(\underline{\Delta}_4) = \sigma_3\sigma_2\sigma_1\sigma_2\sigma_3\sigma_4\sigma_2\sigma_3\sigma_2. \qquad \square$$

Exercice 46 (**décalage**).— Montrer la compatibilité entre l'endomorphisme dec^+ du monoïde B_∞^+ et l'endomorphisme dec du groupe B_∞. $\square$

Solution. Par 3.1.1 , le plongement ι de B_∞^+ dans B_∞ est injectif, et tout est immédiat : pour a dans B_∞^+, on a $\iota(\mathsf{dec}^+(a)) = \mathsf{dec}(a)$. Il n'y a donc pas de risque à identifier dec^+ à la restriction de dec à B_∞^+. $\square$

Exercice 47 (**centre**).— (i) Montrer que, pour tout n, l'élément Δ_n^2 est central dans le monoïde B_n^+ (c'est-à-dire commute avec tout élément). (ii) Montrer qu'un élément g de B_n est central si, et seulement si, il s'écrit $\Delta_n^{2m}a$ avec a central dans B_n^+. $\square$

Solution. (i) Pour $1 \leqslant i \leqslant n-1$, (1.13) implique

$$\sigma_i\underline{\Delta}_n^2 \equiv^+ \underline{\Delta}_n\sigma_{n-i}\underline{\Delta}_n \equiv^+ \underline{\Delta}_n^2\sigma_{n-(n-i)} = \underline{\Delta}_n^2\sigma_i,$$

d'où $\sigma_i\Delta_n^2 = \Delta_n^2\sigma_i$ dans B_n^+ : ainsi, Δ_n^2 commute avec $\sigma_1, ..., \sigma_{n-1}$. De là, Δ_n^2 commute avec tout élément de B_n^+, puisque tout tel élément est un produit fini d'éléments de $\{\sigma_1, ..., \sigma_{n-1}\}$.

(ii) On vient de voir que Δ_n^2 est central dans B_n^+. De là, il est central dans B_n, puisque B_n est groupe de fractions de B_n^+. Donc la condition est suffisante. Inversement, supposons que g est central dans B_n. Par 3.1.7, il existe m dans $\mathbb{Z}$ et a dans B_n^+ vérifiant $g = \Delta_n^{2m}a$: la démonstration de 3.1.7 montre qu'il est loisible de choisir un exposant de Δ_n pair puisque, si $\Delta_n^m a$ est une expression de g, alors $\Delta_n^{m-1}(\Delta_n a)$ en est une autre.

Soit alors b quelconque dans B_n^+. On a donc $\Delta_n^2 ab = b\Delta_n^2 a$, d'où $\Delta_n^2 ab = \Delta_n^2 ba$, puis $ab = ba$, ce qui montre que a est central dans B_n^+. $\square$

Exercice 48 (**automorphisme**).— Montrer que $\sigma_i \mapsto \sigma_{n-i}$ s'étend en un automorphisme du monoïde B_n^+, puis en un automorphisme du groupe B_n, lequel est l'automorphisme intérieur associé à la conjugaison par Δ_n. □

Solution. Notons ϕ_n^+ l'involution de $\mathcal{BW}_n^+$ qui remplace tout générateur σ_i par σ_{n-i}. Par appel direct au lemme 1.1.9, ϕ_n^+ induit un automorphisme involutif de B_n^+.

Soit g dans B_n. Il existe a, b dans B_n^+ vérifiant $g = ab^{-1}$. Définissons alors $\phi_n(g)$ par $\phi_n(g) := \phi_n^+(a)\phi_n^+(b)^{-1}$. La définition fait sens. En effet, la décomposition fractionnaire n'est pas unique, mais $g = ab^{-1} = a'b'^{-1}$ équivaut à l'existence de c, c' dans B_n^+ vérifiant $ac = a'c'$ et $bc = b'c'$ (voir démonstration du théorème de Ore). Alors supposons $g = ab^{-1} = a'b'^{-1}$. Il existe c, c' vérifiant $ac = a'c'$ et $bc = b'c'$. On déduit $\phi_n^+(a)\phi_n^+(c) = \phi_n^+(a')\phi_n^+(c')$ et $\phi_n^+(b)\phi_n^+(c) = \phi_n^+(b')\phi_n^+(c')$, puis $\phi_n^+(a)\phi_n^+(b)^{-1} = \phi_n^+(a')\phi_n^+(b')^{-1}$.

Ensuite, ϕ_n est involutif, donc bijectif. Soient g, h dans B_n^+. Il existe a, b, c, d dans B_n^+ vérifiant $g = ab^{-1}$ et $h = cd^{-1}$. On a alors $gh = aef^{-1}d^{-1}$ où $be = cf$. Il vient

$$\phi_n(gh) = \phi_n^+(a)\phi_n^+(e)\phi_n^+(f)^{-1}\phi_n^+(b)^{-1},$$
$$\phi_n(g)\phi_n(h) = \phi_n^+(a)\phi_n^+(b)^{-1}\phi_n^+(c)\phi_n^+(b)^{-1}.$$

Comme $be = cf$ implique $\phi_n^+(b)\phi_n^+(e) = \phi_n^+(c)\phi_n^+(f)$, le rapprochement des égalités ci-dessus implique $\phi_n(gh) = \phi_n(g)\phi_n(h)$, et ϕ_n est automorphisme de B_n.

Enfin, par 1.3.6, on a $g\Delta_n = \Delta_n\phi_n(g)$ quand g est un unique générateur σ_i, et, par conséquent, quand g est quelconque dans B_n car ϕ_n est un homomorphisme. On déduit $\phi_n(g) = \Delta_n^{-1}g\Delta_n$.

Remarque : Au lieu de prolonger ϕ_n^+ en revenant au fait que B_n est groupe de fractions de B_n^+, on pourrait raisonner directement au niveau de B_n : par 1.3.6, l'automorphisme intérieur associé à Δ_n envoie σ_i sur σ_{n-i}, et il coïncide nécessairement avec ϕ_n. □

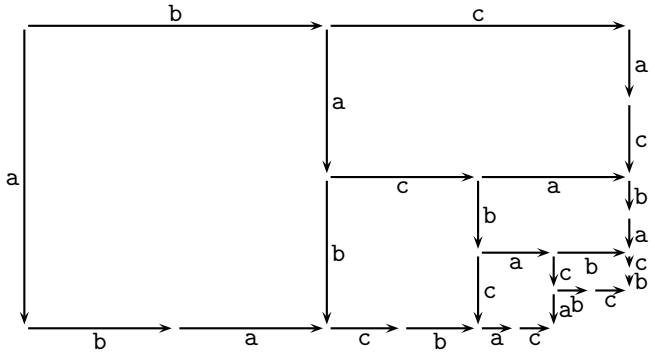
Exercice 49 (**pas de grille**).— Montrer qu'il n'existe pas de grille de source $(\mathtt{a}, \mathtt{bc})$ vis-à-vis de la présentation

$$\langle \mathtt{a}, \mathtt{b}, \mathtt{c} \mid \mathtt{aba} = \mathtt{bab}, \mathtt{bcb} = \mathtt{cbc}, \mathtt{cac} = \mathtt{aca} \rangle^+.$$

□

Solution. On note que, comme avec la présentation de B_4^+, il y a exactement une relation du type $s... = t...$ pour chaque paire de lettres. Donc, pour tout couple de mots (u, v), soit il existe une unique grille de source (u, v), soit une telle grille n'existe pas.

Cherchons une éventuelle grille de source $(\mathtt{a}, \mathtt{bc})$, c'est-à-dire considérons le retournement de `Abc` :



... et on est entré dans une boucle infinie : le motif `Abc` réapparaît. Précisément, si on pose $u := \mathtt{bacbac}$ et $v := \mathtt{acbacb}$, on obtient $\mathtt{Abc} \curvearrowright u(\mathtt{Abc})\overline{v}$, et par suite, pour tout k,

$$\mathtt{Abc} \curvearrowright u^k(\mathtt{Abc})\overline{v}^k :$$

il est clair que le processus ne se termine pas. Il n'existe donc pas de grille de source $(\mathtt{a}, \mathtt{bc})$.

Ainsi, on pourra remarquer que des modifications de présentation paraissant mineures ont pour résultat des comportements très différents de la relation de retournement : on rappelle que, pour la présentation de B_4^+, le retournement se termine toujours en temps fini, par exemple $\mathtt{Abc} \curvearrowright \mathtt{bacbCBA}$. □

Exercices du chapitre IV

Exercice 50 (pgcd).— Montrer que toute famille non vide (finie ou infinie) de tresses positives admet un pgcd à gauche. □

Solution. Soit S une famille non vide de tresses. Soit $\mathcal{X}$ l'ensemble des diviseurs à gauche de tous les éléments de S. Comme 1 est dans $\mathcal{X}$, l'ensemble $\mathcal{X}$ n'est pas vide. Soit alors a un élément

de longueur maximale dans $\mathcal{X}$, et b quelconque dans $\mathcal{X}$. Les éléments a et b ont un ppcm à droite, disons $ab' = ba' = c$. Par construction, c appartient à $\mathcal{X}$: pour tout s dans $\mathcal{S}$, on a $a \preccurlyeq s$ et $b \preccurlyeq s$, donc $c \preccurlyeq s$. Par maximalité de la longueur, on a alors $|c| \leqslant |a|$, qui implique $c \preccurlyeq a$, c'est-à-dire $c = a$. Autrement dit, on a $b \preccurlyeq a$ pour tout b dans $\mathcal{X}$. Par définition, cela signifie que a est pgcd à gauche de toute la famille S. □

Exercice 51.— Démontrer le résultat : « Pour tout $n \leqslant \infty$, deux éléments quelconques de B_n^+ admettent un unique ppcm à gauche, et un unique pgcd à droite. ». □

Solution. On utilise l'antiautomorphisme $\widetilde{\ }$ de III.1.1.8. Soient a, b quelconques dans B_∞^+. Les éléments $\widetilde{a}$ et $\widetilde{b}$ ont un pgcd à gauche c, ce qui signifie que l'on a

$$\widetilde{a} \preccurlyeq c, \quad \widetilde{b} \preccurlyeq c \quad \text{et} \quad \forall x \in B_\infty^+ \, ((x \preccurlyeq a) \,\&\, (x \preccurlyeq b) \Rightarrow x \preccurlyeq c).$$

Utilisons $\widetilde{\preccurlyeq}$ pour la relation de divisibilité à droite : $a \mathrel{\widetilde{\preccurlyeq}} b$ est vraie s'il existe x vérifiant $xa = b$. Alors, $a \preccurlyeq b$ implique $\widetilde{a} \mathrel{\widetilde{\preccurlyeq}} \widetilde{b}$, et les relations qui précèdent impliquent

$$a \mathrel{\widetilde{\preccurlyeq}} \widetilde{c}, \quad b \preccurlyeq \widetilde{c} \quad \text{et} \quad \forall x \in B_\infty^+ \, ((x \mathrel{\widetilde{\preccurlyeq}} \widetilde{a}) \,\&\, (x \mathrel{\widetilde{\preccurlyeq}} \widetilde{b}) \Rightarrow x \mathrel{\widetilde{\preccurlyeq}} \widetilde{c}),$$

le point étant que l'application $\widetilde{\ }$ est surjective sur B_n^+. Mais alors, par définition, $\widetilde{c}$ est ppcm à droite de a et b.

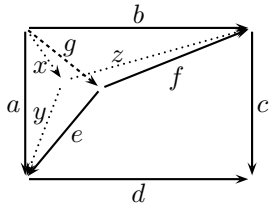
L'argument pour les ppcm à gauche est similaire. □

Exercice 52 (**calcul pgcd**).— (i) Soient a, b quelconques dans B_∞^+. Soit $ad = bc$ le ppcm à droite de a et b, puis $ed = fc$ le ppcm à gauche de c et d. Montrer qu'il existe g vérifiant $a = ge$ et $b = gf$, et que g est le pgcd à gauche de a et b.

(ii) En déduire un algorithme fondé sur la procédure de retournement de III.3.2.4 pour calculer le pgcd dans B_∞^+. □

Solution. (i) On a $ad = bc$, donc $ad = bc$ est un multiple commun à gauche de c et de d. D'autre part, $ed = fc$ est le ppcm à gauche de c et de d. Par définition du ppcm à droite, ad est un multiple à gauche de cd : il existe g vérifiant $ad = ged$. Par simplifiabilité à droite, on déduit $a = ge$. D'autre part, on a $bc = ad = ged = gfc$, d'où $b = gf$.

Par construction, g est un diviseur à gauche commun à a et b. D'autre part, supposons $x \preccurlyeq a$ et $x \preccurlyeq b$, soit $a = xy$ et $b = xz$. On déduit $xyd = ad = bc = xzc$. L'élément yd, qui est aussi zc, est un multiple commun à gauche à c et d, donc $yd = zc$ est un multiple à gauche de $ed = fc$. Par conséquent, x est un diviseur à gauche de g, et g est le pgcd à gauche de a et b.



(ii) Faisons appel à la procédure de retournement à gauche symétrique au retournement à droite. Alors $\overline{u}v$ se retourne à droite en $v'\overline{u'}$ si, et seulement si, $\widetilde{v}\,\overline{\widetilde{u}}$ se retourne à gauche en $\overline{\widetilde{u'}}\widetilde{v'}$, et les deux procédures sont entièrement symétriques l'une de l'autre.

Alors, a et b étant deux éléments quelconques de B_∞^+, par construction, un premier retournement à droite de $\overline{a}b$ aboutit à $d\overline{c}$. Puis un retournement à gauche de $d\overline{c}$ aboutit à $\overline{e}d$. Finalement, un retournement à gauche de $a\overline{e}$ aboutit à g. □

Exercice 53 (centre).— (i) Appelons *quasi-central* un élément a de B_n^+ vérifiant $\forall b \in B_n^+ \exists c \in B_n^+ (ba = ac)$. Montrer que tout élément Δ_n^m est quasi-central.

(ii) Inversement, montrer que, si a est quasi-central dans B_n^+ et que l'on a $\sigma_i \preccurlyeq a$, alors on a aussi $\sigma_j \preccurlyeq a$ pour $|i - j| = 1$.

(iii) En déduire que, si a est quasi-central, il est multiple à droite de Δ_n, puis que a est une puissance de Δ_n.

(iv) En déduire que, pour $n \geqslant 3$, le centre de B_n^+ est le sous-monoïde engendré par Δ_n^2, puis, en utilisant l'exercice 47, que le centre de B_n est le sous-groupe engendré par Δ_n^2. □

Solution. (i) On a déjà observé que, pour toute tresse b dans B_n^+ et tout entier m, on a $b\Delta_n^m = \Delta_n^m \phi_n^m(b)$, donc Δ_n^m est quasi-central.

(ii) Supposons a quasi-central et $\sigma_i \preccurlyeq a$. Soit $j := i \pm 1$. Par définition, il existe c vérifiant $\sigma_j \sigma_i a = ac$. Puisque ac est multiple

à droite de σ_i et de $\sigma_j\sigma_i$, il est multiple à droite de leur ppcm à droite, qui est $\sigma_j\sigma_i\sigma_j$. On a donc $\sigma_i\sigma_j\sigma_j \preccurlyeq \sigma_j\sigma_i a$, donc $\sigma_j \preccurlyeq a$.

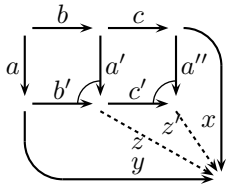
(iii) Supposons a quasi-central avec $a \neq 1$. Il existe au moins un entier i vérifiant $\sigma_i \preccurlyeq a$. Par (ii), on déduit de proche en proche $\sigma_j \preccurlyeq a$ pour tout j dans $\{1, ..., n-1\}$. Donc a doit être multiple à droite du ppcm à droite de $\sigma_1, ..., \sigma_{n-1}$, qui est Δ_n. Écrivons $a = \Delta_n a'$. Alors a' est quasi-central. En effet, soit b quelconque. Il existe c vérifiant $\phi_n(b)\Delta_n a' = \Delta_n a' c$, soit $\Delta_n b a' = \Delta_n a' c$, donc $ba' = a'c$. Une induction sur ℓ montre alors que, si a est quasi-central de longueur ℓ, alors il existe m tel que a est Δ_n^m.

(iv) Un élément central est quasi-central. Il ne reste donc qu'à regarder quelles puissances de Δ_n sont centrales dans B_n^+. Pour $n \geqslant 3$, on a $\sigma_1\Delta_n = \Delta_n\sigma_{n-1} \neq \Delta_n\sigma_1$, donc Δ_n n'est pas central. En revanche, on a déjà vu que Δ_n^2 est central, et le centre de B_n^+ est donc $\{\Delta_n^{2m} \mid m \geqslant 0\}$. Ensuite, suivant l'exercice MOZCentre, un élément g de B_n est central si, et seulement si, il s'écrit $\Delta_n^{2m}a$ avec a central dans B_n^+. On déduit donc que le centre du groupe B_n est $\{\Delta_n^{2m} \mid m \in \mathbb{Z}\}$. □

Exercice 54 (**ppcm itéré**).— Donner une démonstration directe du résultat général : « Si a, b, c sont des éléments d'un monoïde M simplifiable à gauche, et si l'on a $ab' = ba' = \mathsf{ppcm}(a, b)$ et $a'c' = ca'' = \mathsf{ppcm}(a', c)$, alors $\mathsf{ppcm}(a, bc)$ existe et on a $\mathsf{ppcm}(a, bc) = ab'c' = bca''$ ». □

Solution. On lit d'abord $ab'c' = ba'c' = bca''$, d'où $a(b'c') = (bc)a''$.

Supposons $ay = (bc)x$. Puisque ba' est ppcm à droite de a et b, il existe z vérifiant $ay = bcx = ba'z$, d'où $a'z = cx$ en simplifiant b à gauche. Puisque $a'c'$ est ppcm à droite de a' et c, il existe z' vérifiant $a'z = a'c'z'$, d'où $ay = ba'z = ba'c'z'$, et $ab'c' \preccurlyeq ay$. Donc $ab'c'$ est ppcm à droite de a et bc.



□

Exercice 55 (**forme normale**).— Déterminer la forme normale de σ_1^k, de Δ_n^k, de $\sigma_1\sigma_2$, et de $\sigma_1^2\sigma_2^2$. □

Solution. La forme normale de σ_1^k est $(\sigma_1, ..., \sigma_1)$, avec k termes, car c'est une décomposition de σ_1^k et elle est normale.

De même, la forme normale de Δ_n^k, est $(\Delta_n, ..., \Delta_n)$, avec k termes : c'est une décomposition de Δ_n^k et elle est normale.

La forme normale de $\sigma_1\sigma_2$ est $(\sigma_1\sigma_2)$, car $\sigma_1\sigma_2$ est simple.

Enfin, la forme normale de $\sigma_1^2\sigma_2^2$ est $(\sigma_1, \sigma_1\sigma_2, \sigma_2)$, de longueur 3, car $(\sigma_1, \sigma_1\sigma_2, \sigma_2)$ est une décomposition de $\sigma_1^2\sigma_2^2$, les tresses σ_1, $\sigma_1\sigma_2$ et σ_2 sont simples, on a $T(\sigma_1^2\sigma_2^2) = \sigma_1$, et $T(\sigma_1\sigma_2^2) = \sigma_1\sigma_2$. □

Exercice 56 (**algorithme**).— Écrire le pseudocode du calcul de la forme normale sur B_n^+ tel que basé sur la définition inductive directe. □

Solution. On note CONCAT(S, T) la concaténation de deux suites finies S et T. Par ailleurs, on définit RETOURNEMENT(w) comme le résultat du retournement (à droite) du mot w. De la sorte, si on a $u \preccurlyeq v$, disons $v \equiv^+ uu'$, on a RETOURNEMENT$(\overline{u}v) \equiv^+ u'$: le retournement détermine le quotient à gauche. Voici alors une proposition :

Algorithme : FORME NORMALE SUR B_n^+

Entrée : un mot w de $\mathcal{BW}_n^+$
Sortie : la forme normale de $[w]^+$

---

1 : POSER $S := ()$
2 : **tant que** $w \neq \varepsilon$ **faire**
3 : POSER $a := T(w)$ $(=$ PGCD$(a, \Delta_n))$
4 : POSER $S :=$ CONCAT$(S, (a))$
5 : POSER $w :=$ RETOURNEMENT$(\overline{a}w)$
6 : RENVOYER S

On notera que la boucle est **tant que**, mais la condition $a \neq \varepsilon$ garantit que le nombre d'itérations est borné par $|w|$. □

Exercice 57 (**normalité**).— Montrer que (s_1, s_2) est normale si, et seulement si, $s_1\sigma_i$ n'est simple pour aucun diviseur à gauche σ_i de s_2. □

Solution. Par 2.2.6, (s_1, s_2) est normale si, et seulement si, $\mathsf{pgcd}(\partial_n s_1, s_2,)$ est trivial, ce qui équivaut au fait que, pour tout diviseur à gauche σ_i de s_2, on a $\sigma_i \not\preccurlyeq \partial_n s_1$, équivalent à $s_1\sigma_i \not\preccurlyeq s_1\partial_n s_1$, donc à $s_1\sigma_i \not\preccurlyeq \Delta_n$. Comme s_1 est simple, $s_1\sigma_i \not\preccurlyeq \Delta_n$ équivaut à la non-simplicité de $s_1\sigma_i$. □

Exercice 58 (**multiplication par** Δ_n^e).— Montrer que, si la forme Δ_n-normale d'une tresse g est $(\Delta_n^m \mid s_1, ..., s_d)$, alors, pour tout entier relatif e, celle de $\Delta_n^e g$ est $(\Delta_n^{m+e} \mid s_1, ..., s_d)$. □

Solution. La suite $(\Delta_n^{p+e} \mid s_1, ..., s_d)$ satisfait les conditions pour être une suite Δ-normale dès que $(\Delta_n^p \mid s_1, ..., s_d)$ le fait, et elle fournit une décomposition de $\Delta_n^e g$ dès que $(\Delta_n^p \mid s_1, ..., s_d)$ fournit de décomposition de g. Par unicité de la forme Δ_n-normale, il en résulte que $(\Delta_n^{p+e} \mid s_1, ..., s_d)$ est la forme Δ_n-normale de $\Delta_e g$. □

Exercice 59 (**algorithme**).— Écrire le pseudocode d'un algorithme déterminant la forme Δ_n-normale d'une tresse de B_n en introduisant les deux procédures de multiplication de division à gauche par un simple. □

Solution. Pour s, t simples, notons $\mathsf{DécNormale}(t, s)$ l'unique couple normal (s', t') vérifiant $ts = s't'$, déterminé par $s' := T(ts)$ et $ts = s't'$. Voici alors une proposition :

Algorithme : FORME Δ_n-NORMALE DANS B_n

Entrée : un mot signé w dans $\mathcal{BW}_n$
Sortie : la forme Δ_n-normale $(m \mid S)$ de la tresse $[w]$

```
1 : POSER (m | S) := (0 | )
2 : pour p décroissant de |w| à 1 faire
3 :     si Positif(w(p)) alors
4 :         S := MultGaucheΔ(m, S, w(p))
5 :     sinon
6 :         S := DivGaucheΔ(m, S, w(p))
7 : SUPPRIMER LA DERNÈRE LETTRE DE w
8 : tant que DernierTerme(S) = 1 faire
9 :     SUPPRIMER DernierTerme(S)
10 : RENVOYER S
```

Fonction MultGaucheΔ$((m, S)$: suite Δ_n-normale, t : tresse simple)

```
1 :     POSER t' := φ_n^m(t)
2 :     POSER S' := ()
3 :     pour k croissant de 1 à |S| faire
4 :         POSER (s, t) := DécNormale(t, S(k))
5 :         POSER S' := CONCAT((s), S')
6 :     POSER S' := CONCAT(S', (t))
7 :     si S'(1) ≠ Δ_n alors
8 :         RENVOYER (m | S')
9 :     sinon
10 :        RENVOYER (m+1 | Suite(S'))
```

Fonction DivGaucheΔ$((m, S)$: suite Δ_n-normale, t : tresse simple)

```
1 :     POSER r := Δ_n t^{-1}
2 :     POSER r' := φ_n^m(s)
3 :     POSER S' := ()
4 :     pour k croissant de 1 à |S| faire
5 :         POSER (s, t) := DécNormale(t, S(k))
6 :         POSER S' := CONCAT((s), S')
7 :     POSER S' := CONCAT(S', (t))
8 :     si S'(1) ≠ Δ_n alors
9 :         RENVOYER (m | S')
10 :    sinon
11 :        RENVOYER (m+1 | Suite(S'))
```

□

Exercices du chapitre V

Exercice 60 (**permutation**).— Montrer que des homéomorphismes de $\mathbb{D}_n$ isotopes induisent nécessairement la même permutation des points marqués. □

Solution. Pour tout homéomorphisme ϕ de $\mathbb{D}_n$, soit $\mathsf{perm}(\phi)$ la permutation des points marquées associée, déterminée par $\phi(P_k) = P_{\mathsf{perm}(\phi)(k)}$ pour tout k. Par définition, ϕ dépend continûment de la classe d'isotopie de ϕ, donc, par composition, il en est de même de l'application $\phi \mapsto \mathsf{perm}(\phi)$, à valeurs dans le groupe symétrique $\mathfrak{S}_n$. Ce dernier est un espace discret (à $n!$ éléments), donc la valeur de $\mathsf{perm}(\phi)$ est constante sur chaque classe d'isotopie. □

Exercice 61 (**trichotomie**).— (i) En admettant la propriété d'acyclicité, démontrer que, pour toute tresse g, les propriétés « g est σ_i-positive », « g est σ_i-neutre », et « g est σ_i-négative » sont mutuellement exclusives.

(ii) En admettant la propriété d'acyclicité, démontrer que, pour toute tresse g, les propriétés « g est σ-positive », « g est triviale », et « g est σ-négative » sont mutuellement exclusives.

(iii) Montrer qu'une tresse ne peut être σ_i-positive que pour une valeur de i au plus. □

Solution. (i) Soit g une tresse quelconque, et supposons g simultanément σ_i-positive et σ_i-négative. Par définition, il existe un représentant σ_i-positif w de g, et un représentant σ_i-négatif w' de g. Les mots w et $\overline{w'}$ sont alors σ_i-positifs, et il en est de même du produit $w\overline{w'}$. Donc, par définition, la tresse $[w\overline{w'}]$ est σ-positive. Or cette tresse est gg^{-1}, donc est triviale. Par la propriété d'acyclicité, une tresse σ-positive n'est pas triviale. L'hypothèse est donc contractoire.

L'argument est le même pour« g est σ_i-positive », « g est σ_i-neutre » : supposant $g = [w] = [w']$ avec w σ_i-positif et w' σ_i-neutre, le mot $w\overline{w'}$ est σ_i-positif et représente 1, d'où la même contradiction.

Supposant maintenant $g = [w] = [w']$ avec w σ_i-négatif et w' σ_i-neutre, le mot $\overline{w}w'$ est σ_i-positif et représente $g^{-1}g = 1$, contradiction.

(ii) On raisonne de façon analogue. Supposons g simultanément σ-positive et σ-négative. Par définition, il existe un représentant σ_i-positif w de g, et un représentant σ_j-négatif w' de g. Si on a $i \leqslant j$, le mot w' est soit σ_i-neutre, soit σ_i-négatif, et $w\overline{w'}$ est σ_i-positif. Or, il représente $gg^{-1} = 1$, exposant à la même contradiction qu'en (i). Si on a $i > j$, le mot w est σ_j-négatif, et $\overline{w}w'$ est σ_j-positif. Or, il représente $gg^{-1} = 1$, exposant toujours à la même contradiction qu'en (i).

Les cas mettant en jeu « g est triviale » sont conséquences directes de la propriété d'acyclicité.

(iii) Soient w un mot σ_i-positif et w' un mot σ_j-positif, avec $i < j$. Supposons $g = [w] = [w']$. Alors w' est σ_i-neutre. Donc $w\overline{w'}$ est un mot σ_i-positif, et $[w\overline{w'}]$ est une tresse σ_i-positive, donc σ-positive. Or on a $[w\overline{w'}] = gg^{-1} = 1$, contredisant la propriété d'acyclicité. □

Exercice 62 (image).— Montrer que $\widehat{\sigma_1}$ envoie tout mot réduit se terminant par x_1 sur un mot réduit se terminant par x_1^{-1}. □

Solution. Considérons un mot réduit se terminant par x_1, disons vx_1. On trouve

$$\widehat{\sigma_1}(vx_1) = \mathsf{red}(\widehat{\sigma_1}(v)x_1x_2x_1^{-1}).$$

Supposons que $\widehat{\sigma_1}(vx_1)$ ne finit pas par x_1^{-1}. Cela signifie que, dans la réduction ci-dessus, la lettre x_1^{-1} finale disparaît par réduction avec une lettre x_1 qui, ne pouvant être celle qui précède x_2, provient nécessairement de $\widehat{\sigma_1}(v)$. Par définition de $\widehat{\sigma_1}$, une lettre x_1 dans $\widehat{\sigma_1}(v)$ provient ou bien d'une lettre $x_1^{\pm 1}$ dans v, ou bien d'une lettre x_2.

Supposons que la lettre x_1 mise en jeu vient d'une lettre x_1^e, $e = \pm 1$, dans v, soit $v = v_1x_1^ev_2$. On trouve alors

$$\widehat{\sigma_1}(vx_1) = \mathsf{red}(\widehat{\sigma_1}(v_1)\, x_1\, \underline{x_2^ex_1^{-1}\widehat{\sigma_1}(v_2)x_1x_2}\, x_1^{-1}),$$

où le facteur souligné se réduit au mot vide. On a donc $\widehat{\sigma_1}(v_2) = x_1x_2^{-1-e}x_1^{-1}$, ce qui, par définition de $\widehat{\sigma_1}$, requiert $v_2 = x_1^{-2}$

pour $e=1$, et $v_2 = 1$ pour $e=-1$. Alors le mot vx_1 est ou bien $v_1x_1x_1^{-2}x_1$, ou bien $v_1x_1^{-1}x_1$, et aucun n'est réduit. Ce cas est donc impossible.

Supposons maintenant que la lettre x_1 mise en jeu vient d'une lettre x_2 dans v, soit $v = v_1x_2v_2$. On trouve alors

$$\widehat{\sigma_1}(vx_1) = \mathsf{red}(\widehat{\sigma_1}(v_1)\, x_1\, \underline{\widehat{\sigma_1}(v_2)x_1x_2}\, x_1),$$

où le facteur souligné se réduit au mot vide. On a donc $\widehat{\sigma_1}(v_2) = x_2^{-1}x_1^{-1}$, qui implique $v_2 = x_2^{-1}x_1^{-1}$. Alors on a $vx_1 = v_1x_2x_2^{-1}x_1^{-1}x_1$, qui n'est pas réduit. Ce cas est donc également impossible et, de là, l'hypothèse que $\widehat{\sigma_1}(vx_1)$ ne finit pas par x_1^{-1} est donc contractoire. □

Exercice 63 (**groupe fondamental**).— Montrer que, si $\mathcal{X}$ est un sous-espace de $\mathbb{R}^n$ tel que, pour tout P dans $\mathcal{X}$, le segment $[0,P]$ est inclus dans $\mathcal{X}$ (espace « étoilé »), alors le groupe fondamental de $\mathcal{X}$ est trivial. □

Solution. On montre que tout lacet dans $\mathcal{X}$ peut être déformé continûment sur la lacet trivial. En effet, soit γ un lacet dans $\mathcal{X}$, et γ_s l'image de γ par l'homothétie de centre O de rapport s pour $s \in [0,1]$. L'hypothèse que $\mathcal{X}$ est étoilé garantit que γ_s est inclus dans $\mathcal{X}$. Alors, la famille $(\gamma_s)_{s\in[0,1]}$ est une homotopie joignant γ au lacet trivial. □

Exercices du chapitre VI

Exercice 64 (**réduction**).— Vérifier algébriquement que toute poignée correcte est équivalente à sa réduite. □

Solution. Par définition, une σ_i-poignée correcte est un mot de la forme $v = \sigma_i^e u \sigma_i^{-e}$ avec $e = \pm 1$, u σ_i-neutre et les lettres σ_{i+1} et σ_{i+1}^{-1} pas toutes les deux présentes dans u. Faisant apparaître les (éventuelles) lettres $\sigma_{i+1}^{\pm 1}$ dans u, on peut écrire

$$v = \sigma_i^e\, u_0\, \sigma_{i+1}^d\, u_1\, \cdots\, u_{r-1}\, \sigma_{i+1}^d\, u_r\, \sigma_i^{-e},$$

avec $d = \pm 1$ et $u_0, ..., u_r$ σ_{i+1}-neutres. La réduite de v est alors

$$v' = u_0\, \sigma_{i+1}\sigma_i\sigma_{i+1}^{-1}\, u_1\, \cdots\, u_{r-1}\, \sigma_{i+1}\sigma_i\sigma_{i+1}^{-1}\, u_r\, \sigma_i^{-1}\sigma_i.$$

Supposons $e=-1$ et $d=1$, soit

$$v = \sigma_i^{-1}\, u_0\, \sigma_{i+1}\, u_1 \cdots u_{r-1}\, \sigma_{i+1}\, u_r\, \sigma_i.$$

Le principe est de faire migrer la lettre σ_i^{-1} de la gauche vers la droite. Les seuls générateurs apparaissant dans u_0 étant $\sigma_j^{\pm 1}$ avec $j \geqslant i+2$, on a $\sigma_i^{-1} u_0 \equiv u_0 \sigma_i^{-1}$, et donc

$$v \equiv u_0\, \sigma_i^{-1}\, \sigma_{i+1}\, u_1 \cdots u_{r-1}\, \sigma_{i+1}\, u_r\, \sigma_i.$$

On a alors $\sigma_i^{-1}\, \sigma_{i+1} \equiv \sigma_{i+1}\sigma_i\sigma_{i+1}^{-1}\, \sigma_i^{-1}$, donc

$$v \equiv u_0\, \sigma_{i+1}\sigma_i\sigma_{i+1}^{-1}\, \sigma_i^{-1}\, u_1 \cdots u_{r-1}\, \sigma_{i+1}\, u_r\, \sigma_i.$$

Répétant de même avec $\sigma_i^{-1} u_1$, on a $\sigma_i^{-1} u_1 \equiv u_1 \sigma_i^{-1}$, et donc

$$v \equiv u_0\, \sigma_{i+1}\sigma_i\sigma_{i+1}^{-1}\, u_1\, \sigma_i^{-1} \cdots u_{r-1}\, \sigma_{i+1}\, u_r\, \sigma_i.$$

On continue à faire migrer la lettre σ_i^{-1} de gauche à droite par commutation avec les mots u_k et par $\sigma_i^{-1} \cdot \sigma_{i+1} \equiv \sigma_{i+1}\sigma_i\sigma_{i+1}^{-1} \cdot \sigma_i^{-1}$, et on parvient finalement à

$$v \equiv u_0\, \sigma_{i+1}\sigma_i\sigma_{i+1}^{-1}\, u_1 \cdots u_{r-1}\, \sigma_{i+1}\sigma_i\sigma_{i+1}^{-1}\, u_r\, \sigma_i^{-1}\, \sigma_i,$$

et par une réduction libre $\sigma_i^{-1}\, \sigma_i \equiv \varepsilon$, à

$$v \equiv u_0\, \sigma_{i+1}\sigma_i\sigma_{i+1}^{-1}\, u_1 \cdots u_{r-1}\, \sigma_{i+1}\sigma_i\sigma_{i+1}^{-1}\, u_r = v'.$$

Le cas $e=1$ et $d=-1$ se traite de même, en utilisant $\sigma_i \cdot \sigma_{i+1}^{-1} \equiv \sigma_{i+1}^{-1}\sigma_i^{-1}\sigma_{i+1} \cdot \sigma_i$ à la place de $\sigma_i^{-1} \cdot \sigma_{i+1} \equiv \sigma_{i+1}\sigma_i\sigma_{i+1}^{-1} \cdot \sigma_i^{-1}$.

Les deux autres cas correspondent à faire migrer la lettre finale $\sigma_i^{\pm 1}$ de la droite vers la gauche, en faisant appel, pour $e=d=-1$, à $\sigma_{i+1}^{-1} \cdot \sigma_i \equiv \sigma_i \cdot \sigma_{i+1}\, \sigma_i^{-1}\, \sigma_{i+1}^{-1}$, et, pour $e=d=1$, à $\sigma_{i+1} \cdot \sigma_i^{-1} \equiv \sigma_i^{-1} \cdot \sigma_{i+1}^{-1}\, \sigma_i\, \sigma_{i+1}$ respectivement. □

Exercice 65 (**injectivité**).— Supposons que F est une fonction sur B_n telle que $F(g) \neq F(1)$ implique $F(\mathsf{dec}(g)) \neq F(1)$ et $F(g^{-1}) \neq F(1)$. Montrer que, si on a $F(g) \neq F(1)$ pour toute tresse σ_1-positive g, on a $F(g) \neq F(1)$ pour toute tresse non triviale. □

Solution. Soit g une tresse non triviale. Alors g est soit σ-positive, soit σ-négative. Supposons g σ-positive. Il existe i tel que g est σ_i-positive. Pour $i=1$, on a $F(g) \neq F(1)$ par hypothèse. Pour $i \geqslant 2$, il existe g' σ_1-positive vérifiant $g = \mathsf{dec}^{i-1}(g')$. Par hypothèse, on a $F(g') \neq F(1)$, qui implique $F(g) = F(\mathsf{dec}^{i-1}(g') \neq F(1)$.

Supposons maintenant g σ-négative. Il existe i tel que g est σ_i-négative. Pour $i = 1$, la tresse g^{-1} est σ_1-positive. On a $F(g^{-1}) \neq F(1)$ par hypothèse, qui implique $F(g) \neq F(1)$. Pour $i \geqslant 2$, il existe g' σ_1-positive vérifiant $g = \mathsf{dec}^{i-1}(g'^{-1}) = (\mathsf{dec}^{i-1}(g'))^{-1}$. Par hypothèse, on a $F(g') \neq F(1)$, donc $F(g) = F((\mathsf{dec}^{i-1}(g'))^{-1})$, et par conséquent $F(g) \neq F(1)$. □

Exercice 66 (**biordonnabilité**).— Supposons $n \geqslant 3$. Montrer qu'aucun ordre total sur B_n ne peut être compatible avec le produit à gauche et à droite. □

Solution. Supposons que $\prec$ est un ordre total compatible avec le produit à gauche et à droite. Supposons $\sigma_1 \prec \sigma_2$. Par compatibilité avec le produit à gauche, on déduit $\Delta_3^{-1}\sigma_1 \prec \Delta_3^{-1}\sigma_2$, puis, par compatibilité avec le produit à droite, $\Delta_3^{-1}\sigma_1\Delta_3 \prec \Delta_3^{-1}\sigma_2\Delta_3$, ce qui est dire $\sigma_2 \prec \sigma_1$, contredisant l'hypothèse. Symétriquement, $\sigma_2 \prec \sigma_1$ impliquerait $\sigma_1 \prec \sigma_2$. C'est donc que l'existence d'un ordre compatible avec le produit à gauche et à droite est intenable. □

Exercice 67 (**ordonnabilité à droite**).— Montrer que la relation $a^{-1} < b^{-1}$ est un ordre total sur les tresses compatible avec le produit à droite. □

Solution. otons $a \prec b$ la relation $a^{-1} < b^{-1}$. Alors $\prec$ est un ordre total sur B_∞. Supposons $a \prec b$, et soit c quelconque. Par hypothèse, ab^{-1}, soit $(a^{-1})^{-1}b^{-1}$, est une tresse σ-positive. Par conséquent, $acc^{-1}b^{-1}$, soit $((ac)^{-1})^{-1}(bc)^{-1}$, est σ-positive. De là, on déduit $(ac)^{-1} < (bc)^{-1}$, donc $ac \prec bc$: la relation $\prec$ est compatible avec le produit à droite. □

Exercice 68 (**non-conradien**).— Soit $a := \sigma_2^{-1}\sigma_1$ et $b := \sigma_2^{-2}\sigma_1$. Montrer qu'on a $a > 1$ et $b > 1$, et qu'il n'existe aucun entier p vérifiant $a < ba^p$. □

Solution. Les mots $a = \sigma_2^{-1}\sigma_1$ et $b = \sigma_2^{-2}\sigma_1$ sont σ_1-positifs, témoignant de $a > 1$ et $b > 1$. Nous allons démontrer que, pour

tout $p \geqslant 0$ que le mot $a^{-1}ba^p$ a un représentant σ_1-negatif, témoignant de $a^{-1}ba^p < 1$, et, de façon équivalente, de $ba^p < a$. On n'a donc $a < ba^p$ pour aucun entier p.

Pour $p = 0$, on trouve

$$a^{-1}b = \sigma_1^{-1}\sigma_2\sigma_2^{-2}\sigma_1 = \sigma_1^{-1}\sigma_2^{-1}\sigma_1 = \sigma_2\sigma_1^{-1}\sigma_2^{-1},$$

explicitement σ_1-négatif. Pour $p = 1$, on trouve

$$\begin{aligned} a^{-1}ba = \sigma_1^{-1}\sigma_2\sigma_2^{-2}\sigma_1\sigma_2^{-1}\sigma_1 = \sigma_1^{-1}\sigma_2^{-1}\sigma_1\sigma_2^{-1}\sigma_1 \\ = \sigma_2\sigma_1^{-1}\sigma_2^{-2}\sigma_1 = \sigma_2^2\sigma_1^{-2}\sigma_2^{-1}, \end{aligned}$$

à nouveau explicitement σ_1-négatif. Finalement, on établit

$$a^{-1}ba^p = \sigma_2^2(\sigma_1^{-1}\sigma_2)^{p-1}\sigma_1^{-2}\sigma_2^{-1}$$

par induction sur $p \geqslant 1$. La formule est vérifiée pour $p = 1$. Pour $p \geqslant 2$, utilisant l'hypothèse d'induction et l'égalité $\sigma_1^{-1}\sigma_2^{-2}\sigma_1 = \sigma_2\sigma_1^{-2}\sigma_2^{-1}$, on trouve

$$\begin{aligned} a^{-1}ba^p &= (\sigma_2^2(\sigma_1^{-1}\sigma_2)^{p-2}\sigma_1^{-2}\sigma_2^{-1})(\sigma_2^{-1}\sigma_1) \\ &= \sigma_2^2(\sigma_1^{-1}\sigma_2)^{p-2}\sigma_1^{-1}\sigma_2\sigma_1^{-2}\sigma_2^{-1} = \sigma_2^2(\sigma_1^{-1}\sigma_2)^{p-1}\sigma_1^{-2}\sigma_2^{-1}, \end{aligned}$$

à nouveau une expression σ_1-négative. □

Exercice 69 (ordre flippé).— (i) Montrer que l'ordre $<$ est compatible avec le décalage sur B_∞.

(ii) Pour a, b dans B_n, on déclare $a \mathrel{\widetilde{<}}_n b$ quand on a $\phi_n(a) < \phi_n(b)$, où ϕ_n est l'automorphisme qui échange σ_i et σ_{n-i} pour tout i. Montrer que $\mathrel{\widetilde{<}}_n$ est un ordre total sur B_n, compatible avec le produit à gauche, et que l'ordre $\mathrel{\widetilde{<}}_n$ sur B_n est la restriction de l'ordre $\mathrel{\widetilde{<}}_{n+1}$ sur B_{n+1}. Quel est le plus petit élément de B_n^+ suivant $\mathrel{\widetilde{<}}$? □

Solution. (i) On rappelle que dec est l'endomorphisme injectif de B_∞ qui envoie σ_i sur σ_{i+1} pour tout i (*cf.* exercices 40 et 46). La propriété « c est σ_i-positif » est équivalente à « $\mathsf{dec}(c)$ est σ_{i+1}-positif », donc « c est σ-positif » est équivalente à « $\mathsf{dec}(c)$ est σ-positif. De là, $a < b$ est équivalente à $\mathsf{dec}(a) < \mathsf{dec}(b)$.

(ii) La relation $\mathrel{\widetilde{<}}$ est un ordre total sur B_n. Supposons $a \mathrel{\widetilde{<}} b$ et soit c quelconque : on a $\phi_n(a) < \phi_n(b)$, d'où $\phi_n(c)\phi_n(a) < \phi_n(c)\phi_n(b)$, qui est $\phi_n(ca) < \phi_n(cb)$, *alias* $ca \mathrel{\widetilde{<}} cb$: l'ordre $\mathrel{\widetilde{<}}$ est compatible avec le produit à gauche.

Supposons $a, b \in B_n$ et $a \widetilde{<}_n b$. Par définition, on a $\phi_n(a) < \phi_n(b)$. Par (i) on déduit $\mathsf{dec}(\phi_n(a)) < \mathsf{dec}(\phi_n(b))$. Or, on a par construction $\mathsf{dec}(\phi_n(a)) = \phi_{n+1}(a)$ et $\mathsf{dec}(\phi_n(b)) = \phi_{n+1}(b)$, d'où $\phi_{n+1}(a) < \phi_{n+1}(b)$, soit encore $a \widetilde{<}_{n+1} b$. Inversement, supposons $a \widetilde{<}_{n+1} b$. Si on n'avait pas $a \widetilde{<}_n b$, on aurait nécessairement $a = b$ ou $b \widetilde{<}_n a$, qui excluerait $a \widetilde{<}_{n+1} b$. On a donc $a \widetilde{<}_n b \Leftrightarrow a \widetilde{<}_{n+1} b$, et l'ordre $\widetilde{<}_n$ est la restriction de $\widetilde{<}_{n+1}$ à B_n. Il en résulte qu'il existe un ordre total $\widetilde{<}$ bien défini sur B_∞ dont $\widetilde{<}_n$ est la restriction à B_n. Par construction, on a

$$1 \widetilde{<} \sigma_1 \widetilde{<} \sigma_1^2 \widetilde{<} \sigma_1^3 \widetilde{<} \cdots \widetilde{<} \sigma_2 \widetilde{<} \sigma_3 \widetilde{<} \cdots$$

Soit $g \in B_\infty^+ \setminus B_2^+$: toute expression de g contient un générateur σ_i avec $i \geqslant 2$, témoignant de la relation $\sigma_1 < g$: le plus petit élément non trivial de B_∞^+ est σ_1. □

Exercices du chapitre VII

Exercice 70 (formules de Dynnikov).— Partant de la suite $(0, 1, 0, 1, ..., 0, 1)$, vérifier que les formules de 1.3.7 donnent pour σ_1 les valeurs $(1, 0, 0, 2, 0, 1, ..., 0, 1)$ lues sur la figure VII.3. Quelles sont les valeurs pour σ_1^{-1} ? □

Solution. Soit S la suite des coordonnées de σ_1 dans B_n. Appliquant les formules de 1.3.7, S est égal à $F^+(0, 1, 0, 1)$, suivi par $n-3$ fois $(0, 1)$. Le paramètre « t_1 » est $t_1 := 0-1^- -0+1^+ := 1$. On trouve alors

$$F_1^+(0, 1, 0, 1) := 0 + 1^+ + 1^+ - 1^+ := 1$$
$$F_2^+(0, 1, 0, 1) := 1 - 1^+ := 0$$
$$F_3^+(0, 1, 0, 1) := 0 + 1^- + 1^- + 1^- := 0$$
$$F_4^+(0, 1, 0, 1) := 1 + 1^+ := 2,$$

d'où $S = (1, 0, 0, 2, 0, 1, ..., 0, 1)$.

De même, soit S' la suite des coordonnées de σ_1^{-1} dans B_n. Cette fois, S' est égal à $F^-(0, 1, 0, 1)$, suivi par $n-3$ fois $(0, 1)$. Le para-

mètre « t_2 » est $t_2 := 0 + 1^- - 0 - 1^+ := -1$. On trouve alors

$$F_1^-(0,1,0,1) := 0 - 1^+ - 1^+ - 1^+ := -1$$
$$F_2^-(0,1,0,1) := 1 + (-1)^- := 0$$
$$F_3^-(0,1,0,1) := 0 - 1^- + 0^- - (-1)^- := 0$$
$$F_4^-(0,1,0,1) := 1 - (-1)^- := 2,$$

d'où $S' = (-1, 0, 0, 2, 0, 1, ..., 0, 1)$.

Plus généralement, on pourra vérifier que, pour k positif, on a

$$\rho_D(\sigma_1^k) := (1, -k{+}1, 0, k{+}1, 0, 1, ..., 0, 1)$$
$$\rho_D(\sigma_1^{-k}) := (-1, -k{+}1, 0, k{+}1, 0, 1, ..., 0, 1).$$ □

Exercice 71 (σ**-négatif**).— Montrer que la première coordonnée impaire non nulle d'une tresse σ-négative est un entier strictement négatif. □

Solution. Soit w un mot σ_1-négatif, $w = w_0\sigma_1^{-1}w_1\sigma_1^{-1}\cdots\sigma_1^{-1}w_p$ où $\sigma_1^{\pm 1}$ est absente des mots w_k. On suit les deux premières coordonnées de $(0, 1, ..., 0, 1)_\bullet w$ au fur et à mesure que les lettres sont ajoutées, en partant du début. On part avec $(0, 1)$. Aussi longtemps que σ_1^{-1} n'est pas rencontrée, on reste avec $(0, 1)$. Lorsque la première lettre σ_1^{-1} est atteinte, la première coordonnée devient $F_1^-(0, 1, x_2, y_2)$, soit, par définition, $0 - 1^+ - z^+$ pour un certain entier z (en l'occurrence $-x_2$), donc un entier strictement négatif. Ensuite, la traversée des mots w_k ne change pas la première coordonnée, tandis que celle des lettres σ_1^{-1} ne peut que la diminuer puisque, par définition, on lui soustrait des entiers non négatifs. Donc le résultat est établi pour une tresse σ_1-négative.

Soit maintenant w un mot de tresse σ_i^{-1}-négatif avec $i \geqslant 2$. Alors w est $\mathsf{dec}^{i-1}(w')$ où w' est σ_1-négatif w'. Par construction, la suite des coordonnées de w est celle de w' précédée de $(0, 1, ..., 0, 1)$ avec $2i - 2$ termes. Les $i - 1$ premières coordonnées impaires de w sont donc nulles, tandis que la $i^{\text{ième}}$ est la première de w', qui est strictement négative comme montré ci-dessus. □

Exercices du chapitre VIII

Exercice 72 (famille génératrice).— (i) Montrer que $\{\sigma_1, ..., \sigma_{n-1}\}$ est famille génératrice minimale de B_n, au sens où aucune sous-famille propre n'est génératrice.

(ii) Montrer que, pour tout $n \geqslant 3$, la famille $\{\sigma_1, \sigma_1 \cdots \sigma_{n-1}\}$ engendre B_n. □

Solution. (i) Soit G le sous-groupe de B_n engendré par $\{\sigma_1, ..., \sigma_{i-1}\} \cup \{\sigma_{i+1}, ..., \sigma_n\}$. On veut démontrer que σ_i n'est pas élément de G. Soit g quelconque dans G. Par induction sur la longueur d'un représentant de g, on montre que $\mathsf{perm}(g)$ est de la forme ff', où f appartient à $\mathfrak{S}_{\{1,...,i\}}$ et f' appartient à $\mathfrak{S}_{\{i+1,...,n\}}$: en d'autres termes, $\mathsf{perm}(g)$ laisse les ensembles $\{1, ..., i\}$ et $\{i+1, ..., n\}$ globalement invariants. Il en résulte que σ_i n'appartient pas à G, car $\mathsf{perm}(\sigma_i)$, qui est la transposition s_i, ne laisse pas $\{1, ..., i\}$ et $\{i+1, ..., n\}$ invariant car elle envoie i sur $i+1$.

(ii) Pour $2 \leqslant i \leqslant n$, on

Par III.1.3.3, on a $\sigma_2 \cdot \sigma_1 \cdots \sigma_n = \sigma_1 \cdots \sigma_n \cdot \sigma_1$, donc le conjugué de σ_1 par $\sigma_1 \cdots \sigma_{n-1}$ est σ_2 :

$$\sigma_2 = (\sigma_1 \cdots \sigma_n)\, \sigma_1\, (\sigma_1 \cdots \sigma_n)^{-1},$$

et, de même, pour $2 \leqslant i \leqslant n$,

$$\sigma_i = (\sigma_1 \cdots \sigma_n)^{i-1}\, \sigma_1\, (\sigma_1 \cdots \sigma_n)^{-i+1}.$$

Le sous-groupe de B_n engendré par σ_1 et $\sigma_1 \cdots \sigma_{n-1}$ contient donc $\sigma_1, \sigma_2, ..., \sigma_{n-1}$, c'est donc l'intégralité de B_n. □

Exercice 73.— Démontrer le résultat : « En termes des générateurs $a_{i,j}$, le groupe B_n est présenté par les relations $a_{i,j}a_{i',j'} = a_{i',j'}a_{i,j}$ si les intervalles $[i, j]$ et $[i', j']$ sont disjoints ou emboîtés, et $a_{i,j}a_{j,k} = a_{j,k}a_{i,k} = a_{i,k}a_{i,j}$ pour $1 \leqslant i < j < k \leqslant n$. » □

Solution. It est aisé de vérifier à partir de la définition des générateurs $a_{i,j}$ en termes des $\sigma_i^{\pm 1}$ que les relations indiquées sont satisfaites. Si les intervalles $[i, j]$ et $[i', j']$ sont disjoints, chacun des $\sigma_p^{\pm 1}$ figurant dans $a_{i,j}$ commute avec chacun des $\sigma_q^{\pm 1}$ figurant dans $a_{i',j'}$, donc $a_{i,j}$ et $a_{i',j'}$ commutent. Si l'intervalle $[i', j']$ est

emboîté dans $[i', j']$, chacun des $\sigma_q^{\pm 1}$ figurant dans $a_{i',j'}$ commute avec $a_{i,j}$: avec la notation de III.1.3.3, on a $a_{i,j} = \sigma_{i,j}\sigma_{i,j-1}^{-1}$, et, pour $i < k < j$, par (III.1.9) et (III.1.10), on a

$$\sigma_k \cdot a_{i,j} = \sigma_k \cdot \sigma_{i,j}\sigma_{i,j-1}^{-1} = \sigma_{i,j} \cdot \sigma_{k-1} \cdot \sigma_{i,j-1}^{-1} = \sigma_{i,j}\sigma_{i,j-1}^{-1} \cdot \sigma_k = a_{i,j} \cdot \sigma_k.$$

Donc $a_{i,j}$ commute avec $a_{i',j'}$. Soit maintenant $i < j < k$. Chacun des générateurs $\sigma_p^{\pm 1}$ figurant dans $\sigma_{i,j-1}^{-1}$ commute avec chacun des générateurs $\sigma_q^{\pm 1}$ figurant dans $a_{j,k}$. On peut donc écrire, introduisant un terme trivial $\sigma_{i,j}^{-1}\sigma_{i,j}$,

$$\begin{aligned} a_{i,j}a_{j,k} &= \sigma_{i,j}\sigma_{i,j-1}^{-1}a_{j,k} \\ &= \sigma_{i,j}a_{j,k}\sigma_{i,j-1}^{-1} \\ &= \sigma_{i,j}a_{j,k}\sigma_{i,j}^{-1}\sigma_{i,j}\sigma_{i,j-1}^{-1}, \\ &= (\sigma_{i,j}a_{j,k}\sigma_{i,j}^{-1}) \cdot (\sigma_{i,j}\sigma_{i,j-1}^{-1}) = a_{i,k}a_{i,j} \end{aligned}$$

en regroupant les termes. La vérification pour $a_{i,j}a_{j,k} = a_{j,k}a_{i,k}$ est analogue.

D'un autre côté, les relations ci-dessus impliquent les relations d'Artin. En effet, un cas particulier d'intervalle disjoint est $[i, i+1]$ et $[j, j+1]$ avec $j \geqslant i+2$, auquel cas on obtient

$$\sigma_i\sigma_j = a_{i,i+1}a_{j,j+1} = a_{j,j+1}a_{i,i+1} = \sigma_j\sigma_i.$$

Et, par ailleurs, on a $a_{i,i+1}a_{i+1,i+2} = a_{i+1,i+2}a_{i,i+1}$, ce qui se traduit en $\sigma_i\sigma_{i+1} = \sigma_{i+1}\sigma_{i+1}\sigma_i^{-1}\sigma_i^{-1}$, impliquant la relation $\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_{i+1}\sigma_i$. □

Exercice 74 (conjugaison par Δ_n^*).— Montrer que la conjugaison par Δ_n^* est l'automorphisme de B_n^{+*} qui envoie $a_{i,j}$ sur $a_{i+1,j+1}$ pour $j < n$, et $a_{i,n}$ sur $a_{1,i+1}$. Quel est son ordre ? À quelle transformation géométrique correspond-il dans la correspondance de la figure VIII.2 ? □

Solution. Soit ϕ_n^* la conjugaison par Δ_n^* définie par $\phi_n^*(g) := \Delta_n^* g \Delta_n^{*-1}$. Par définition, on a $\Delta_n^* = \sigma_1 \cdots \sigma_{n-1}$, et, comme vu dans l'exercice 72, on a $\phi_n^*(\sigma_i) = \sigma_{i+1}$ pour $1 \leqslant i < n$. En reportant dans la définition des générateurs $a_{i,j}$, on voit que, pour $j < n$, on a $\phi_n^*(a_{i,j}) = a_{i+1,j+1}$. En outre, on a

$$\phi_n^*(\sigma_{n-1}) := \Delta_n^*\sigma_{n-1}\Delta_n^{*-1} = \sigma_1 \cdots \sigma_{n-1}\sigma_{n-1}\sigma_{n-1}^{-1} \cdots \sigma_1^{-1} = a_{1,n},$$

soit $\phi_n^*(a_{n-1,n}) = a_{1,n}$.

On déduit, pour $1 \leqslant i < n$,

$$\begin{aligned}\phi_n^*(a_{i,n}) &= \phi_n^*(\sigma_i \cdots \sigma_{n-2}\sigma_{n-1}\sigma_{n-2}^{-1} \cdots \sigma_i^{-1}) \\ &= \sigma_{i+1} \cdots \sigma_{n-1} a_{1,n} \sigma_{n-1}^{-1} \cdots \sigma_{i+1}^{-1}. \qquad (*)\end{aligned}$$

On fait une récurrence descendante sur $i < n$. Pour $i := n-2$, l'égalité $(*)$ est

$$\phi_n^*(a_{n-1,n}) = \sigma_{n-1} a_{1,n} \sigma_{n-1}^{-1} = a_{n-1,n} a_{1,n} a_{n-1,n}^{-1} :$$

or les relations entre les $a_{i,j}$ (1.1.3, *cf.* exercice 73) impliquent $a_{n-1,n}a_{1,n} = a_{1,n-1}a_{n-1,n}$, donc $\phi_n^*(a_{n-2,n}) = a_{1,n-1}$. Pour $i := n-3$, l'égalité $(*)$ est

$$\phi_n^*(a_{n-1,n}) = \sigma_{n-2} a_{1,n-1} \sigma_{n-2}^{-1} = a_{n-2,n-1} a_{1,n-1} a_{n-2,n-1}^{-1} :$$

par les relations entre les $a_{i,j}$, on a $a_{n-2,n-1}a_{1,n-1} = a_{1,n-2}a_{n-2,n-1}$, donc $\phi_n^*(a_{n-3,n}) = a_{1,n-2}$. Et ainsi de suite...

Il en résulte que, pour tout i, on a

$$\begin{aligned}(\phi_n^*)^n(\sigma_i) &= (\phi_n^*)^{i+1}(\sigma_{n-1}) = (\phi_n^*)^i(a_{1,n}) \\ &= (\phi_n^*)^{i-1}(a_{1,2}) = (\phi_n^*)^{i-1}(\sigma_1) = \sigma_i :\end{aligned}$$

l'automorphisme ϕ_n^* est d'ordre n. Il correspond à une rotation d'angle $2\pi/n$ dans le sens des aiguilles d'une montre dans la représentation de la figure VIII.2. Par contraste, l'automorphisme ϕ_n qui est la congugaison par Δ_n est d'ordre 2, et correspond à une symétrie. □

Exercice 75.— Vérifier le résultat « Pour tous i, n, la matrice $\Sigma_{i,n}$ est inversible dans $\mathsf{Mat}_n(\mathbb{Z}[t,t^{-1}])$, et l'application ρ_{B} qui, pour tout i, envoie σ_i sur $\Sigma_{i,n}$ induit une représentation linéaire de B_n dans $\mathsf{GL}(\mathbb{Z}[t,t^{-1}])$ ». □

Solution. L'inverse de $\Sigma_{2,2}$ est $\begin{pmatrix} 0 & 1 \\ t^{-1} & 1-t^{-1} \end{pmatrix}$. L'invariance de ρ_{B} par rapport aux relations de commutation est immédiate. Vue l'action du décalage, il suffit de comparer $\rho_{\mathsf{B}}(\sigma_1\sigma_2\sigma_1)$ et $\rho_{\mathsf{B}}(\sigma_2\sigma_1\sigma_2)$. Or toutes deux sont égales à $\begin{pmatrix} 1-t & t-t^2 & t^2 \\ 1-t & t & 0 \\ 1 & 0 & 0 \end{pmatrix}$. □