

CORRIGÉ PARTIEL DE LA FICHE 6

**Exercice 12 (Groupes résiduellement finis)** — Un groupe  $G$  est dit résiduellement fini si, pour tout élément  $x \neq e$  de  $G$ , il existe un sous-groupe distingué  $N$  de  $G$  d'indice fini tel que  $x \notin N$ . Il revient au même de dire que, pour tout  $x \neq e$  dans  $G$ , il existe un groupe fini  $H$  et un homomorphisme  $\varphi : G \rightarrow H$  tels que  $\varphi(x) \neq e$ .

1. Il est clair que les groupes finis sont résiduellement finis. Il est également clair que tout sous-groupe d'un groupe résiduellement fini est encore résiduellement fini.

Quel que soit  $n \geq 1$ , le groupe  $\mathbb{Z}^n$  est résiduellement fini : étant donné  $z = (z_1, \dots, z_n) \neq 0$  dans  $\mathbb{Z}^n$ , il existe un indice  $i$  tel que  $z_i \neq 0$  ; ayant choisi un nombre premier  $p$  ne divisant pas  $z_i$ , l'image de  $z$  par l'homomorphisme  $\varphi : \mathbb{Z}^n \rightarrow \mathbb{Z}/p\mathbb{Z}$ ,  $(x_1, \dots, x_n) \mapsto x_i \pmod{p}$  est non triviale.

On montre par un argument similaire que le groupe  $GL_n(\mathbb{Z})$  est résiduellement fini : étant donné  $g \neq e$  dans  $GL_n(\mathbb{Z})$ , il existe un nombre premier  $p$  tel que l'image de  $g$  par l'homomorphisme canonique  $GL_n(\mathbb{Z}) \rightarrow GL_n(\mathbb{Z}/p\mathbb{Z})$  soit non triviale.

2. Le groupe (additif)  $\mathbb{Q}$  ne possède pas de sous-groupe d'indice fini non trivial : en effet, si  $N$  est d'indice fini  $n$  dans  $\mathbb{Q}$ , alors  $r = n(r/n)$  appartient à  $N$  quel que soit  $r \in \mathbb{Q}$ . Le groupe  $\mathbb{Q}$  n'est donc pas résiduellement fini.

3. Soit  $u \in G * H$  un mot de longueur au plus  $n$ . Étant donné  $g, g' \in G$ ,
- soit l'écriture sous forme normale de  $u$  est  $u = x_1 \dots x_n$  avec  $x_1 \in H$ , auquel cas  $\text{lg}(gu) = \text{lg}(g'u) = n + 1$  et  $g' \cdot (g \cdot u) = g' \cdot u = u$  ;
  - soit  $\text{lg}(u), \text{lg}(gu) \leq n$ , et alors  $g' \cdot (g \cdot u) = g'(g \cdot u) = (gg')u = (gg') \cdot u$ .

Ceci définit donc une action par permutations du groupe  $G$  sur  $\Omega_n$ , i.e. un homomorphisme de groupes  $G \rightarrow \mathfrak{S}(\Omega_n)$ . Procédant de même avec  $H$ , on en déduit un homomorphisme de groupes  $G * H \rightarrow \mathfrak{S}(\Omega_n)$  satisfaisant à la condition imposée.

4. Si  $G$  et  $H$  sont finis, l'ensemble  $\Omega_n$  est fini pour tout  $n \geq 0$ .

Soit  $x \neq e$  un élément de  $G * H$  et soit  $\ell$  la longueur de son écriture sous forme normale. Pour tout  $n \geq \ell$ ,  $x \cdot e = x \in \Omega_n$  et donc l'image de  $x$  dans  $\mathfrak{S}(\Omega_n)$  est non triviale ; comme le groupe  $\mathfrak{S}(\Omega_n)$  est fini, on en déduit que  $G * H$  est résiduellement fini.

5. Supposons que  $G$  et  $H$  soient deux groupes résiduellement finis et considérons un élément  $x \neq e$  dans  $G * H$ , que l'on écrit sous forme normale :  $x = x_1 \dots x_N$  avec  $(x_{2p+1} \in G - \{e\}$  et  $x_{2p} \in H - \{e\})$  ou  $(x_{2p+1} \in H - \{e\}$  et  $x_{2p} \in G - \{e\})$  pour tout  $p$ . Pour fixer les notations, on va supposer que l'on est dans le premier cas de figure.

Comme  $G$  et  $H$  sont résiduellement fini, il existe des groupes finis  $\Gamma_1, \dots, \Gamma_N$  et des homomorphismes

$$\varphi_{2p+1} : G \rightarrow \Gamma_{2p+1}, \quad \psi_{2p} : H \rightarrow \Gamma_{2p}$$

tels que  $\varphi_i(x_i) \neq e$  pour tout  $i$ . Posant  $\Gamma' = \prod_p \Gamma_{2p+1}$  et  $\Gamma'' = \prod_p \Gamma_{2p}$ , on en déduit deux homomorphismes

$$\varphi : G \rightarrow \Gamma' \quad \text{et} \quad \psi : H \rightarrow \Gamma''$$

tels que  $\varphi(x_{2p+1}) \neq e$  et  $\psi(x_{2p}) \neq e$  pour tout  $p$ . L'homomorphisme

$$\varphi * \psi : G * H \rightarrow \Gamma' * \Gamma''$$

envoie  $x$  sur le mot  $\varphi(x_1)\psi(x_2)\dots$ , lequel est sous forme normale par construction ; en particulier,  $(\varphi * \psi)(x) \neq e$ .

En vertu de la question précédente, le groupe  $\Gamma' * \Gamma''$  est résiduellement fini car  $\Gamma'$  et  $\Gamma''$  sont finis. Il existe par suite un groupe fini  $\Gamma$  et un homomorphisme  $\lambda : \Gamma' * \Gamma'' \rightarrow \Gamma$  tel que  $(\lambda \circ (\varphi * \psi))(x) \neq e$ , ce qui montre que le groupe  $\Gamma' * \Gamma''$  est résiduellement fini.

D'après ce que l'on vient de dire, tout produit libre d'un nombre fini de groupes résiduellement finis est résiduellement fini. Ceci est plus généralement vrai pour le produit libre d'une famille arbitraire  $(G_i)_{i \in I}$  de groupes résiduellement finis : pour tout élément  $x \neq e$  de  $G = *_{i \in I} G_i$ , il existe un sous-ensemble fini  $J$  de  $I$  tel que  $x$  appartienne au produit libre des  $(G_j)_{j \in J}$  et son image par l'homomorphisme

$$f : *_{i \in I} G_i \rightarrow *_{j \in J} G_j, \quad f|_{G_i} = \begin{cases} \text{id}_{G_i} & \text{si } i \in J \\ e & \text{sinon} \end{cases}$$

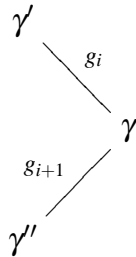
est non triviale.

Finalement, en vertu de l'isomorphisme  $L(X) \simeq *_{x \in X} \mathbb{Z}$  pour tout ensemble  $X$ , on déduit de ce qui précède et de la question 1 que tout groupe libre est résiduellement fini

**Exercice 16** ( $\text{PSL}_2(\mathbb{Z})$ ) — Les cinq premières questions portent sur un groupe quelconque  $G$  muni de deux sous-groupes  $A$  et  $B$  tels que  $A \cap B = \{e\}$ .

1. Désignons par  $\Gamma_0$  (resp.  $\Gamma_1$ ) l'ensemble des sommets (resp. des arêtes) du graphe  $\Gamma$ . On dispose par construction d'une application surjective  $f : G \rightarrow \Gamma_1$  associant à  $g$  l'arête reliant les sommets  $gA$  et  $gB$ . Si deux éléments  $g, h \in G$  détermine la même arête  $f(g) = f(h)$  dans  $\Gamma$ , alors  $gA = hA$  et  $gB = hB$ , d'où  $h^{-1}g \in A \cap B$  et  $h = g$ . L'application  $f$  est donc bijective.

2. Soit  $c$  un chemin dans  $\Gamma$  d'arêtes successives  $g_1, g_2, \dots, g_n$  et considérons deux arêtes successives  $g_i$  et  $g_{i+1}$  :



Vu la définition de  $\Gamma$ , on a

$$\gamma' = g_i A, \quad \gamma = g_i B = g_{i+1} B \quad \text{et} \quad \gamma'' = g_{i+1} A$$

ou

$$\gamma' = g_i B, \quad \gamma = g_i A = g_{i+1} A \quad \text{et} \quad \gamma'' = g_{i+1} B.$$

Dans le premier cas de figure,  $g_{i+1} = g_i b$  avec  $b \in B$  uniquement déterminé ; dans le second cas de figure,  $g_{i+1} = g_i a$  avec  $a \in A$  uniquement déterminé. On en déduit qu'il existe un unique élément  $x_i \in A \cup B$  tel que  $g_{i+1} = g_i x_i$ .

**3, 4 et 5.** Soit  $\mathcal{C}_N$  l'ensemble des chemins de longueur  $N$  dans  $\Gamma$  n'empruntant pas deux fois de suite la même arête et soit  $\mathcal{E}_N$  l'ensemble des suites  $(x_1, \dots, x_N)$  d'éléments de  $(A - \{e\}) \cup (B - \{e\})$  n'ayant pas deux termes successifs dans  $A$  ou dans  $B$ .

Soit  $c = (g_1, \dots, g_{N+1})$  un chemin dans  $\Gamma$ . Les conditions  $x_i = e$  et  $g_{i+1} = g_i x_i$  étant équivalentes,  $e$  apparaît parmi les  $x_i$  si et seulement si  $c$  emprunte deux fois de suite la même arête.



3. Si  $\Gamma$  est connexe, tout sommet  $gA$  peut être relié au sommet  $A$  par un chemin et il existe donc  $(h, x_1, \dots, x_N) \in G \times \mathcal{E}^N$  d'origine  $A$  et d'aboutissement  $gA$ ; on a alors  $h \in A$  et  $hx_1 \dots x_N A = gA$ , donc  $g$  appartient au sous-groupe de  $G$  engendré par  $A$  et  $B$ . Réciproquement, si  $G$  est engendré par  $A$  et  $B$ , alors tout élément  $g$  s'écrit sous la forme  $g = x_1 \dots x_N$  avec  $x_1 \in A$ ,  $x_2 \in B - \{e\}$ ,  $x_3 \in A - \{e\}$ , ... (cette écriture n'est *a priori* pas unique); le chemin  $c$  dans  $\Gamma$  tel que  $\sigma(c) = (e, x_1, \dots, x_N)$  relie alors les arêtes  $A \xrightarrow{e} B$  et  $gA \xrightarrow{g} gB$  et donc  $\Gamma$  est connexe.

4. On l'a vu en passant.

5. On rappelle que le graphe  $\Gamma$  est un arbre si et seulement si deux sommets distincts sont reliés par un unique chemin n'empruntant pas deux fois de suite la même arête, ou encore s'il n'existe pas de circuit injectif.

Supposons qu'il existe  $N \geq 2$  et un élément  $(x_1, \dots, x_N)$  de  $\mathcal{E}_N$  tel que  $x_1 \dots x_N = e$  dans  $G$ ; pour fixer les idées, on suppose  $x_1 \in A$ . Si  $N$  est pair, le chemin  $c = \sigma^{-1}(e; x_1, \dots, x_N)$  relie les sommets  $B$  et  $x_1 \dots x_N A = A$ . Si  $N$  est impair, le chemin  $\sigma^{-1}(x_1; x_2, \dots, x_N) \in \mathcal{E}_{N-1}$  relie les sommets  $A$  et  $B$ . Comme, dans chaque cas, le chemin  $\sigma^{-1}(e)$  de longueur 0 relie  $A$  et  $B$ ,  $\Gamma$  n'est pas un arbre.

Considérons réciproquement un circuit injectif  $c = (g_1, \dots, g_N)$  contenu dans  $\Gamma$ . On a  $N \geq 3$  et, quitte à permuter cycliquement les  $g_i$ , on peut supposer que le sommet commun aux arêtes  $g_1$  et  $g_N$  est de la forme  $gA$ , auquel cas  $g_1 = g$ . On a  $gx_1 \dots x_{N-1} A = g_N A = gA$ , donc  $x_1 \dots x_{N-1} \in A$ ; comme  $N - 1 \geq 2$ , ceci est impossible si  $G$  est le produit libre de  $A$  et  $B$ .

En conclusion, nous avons démontré que  $G$  est le produit libre des sous-groupes  $A$  et  $B$  si et seulement si  $\Gamma$  est un arbre.

6. On fait agir le groupe  $G = \text{SL}_2(\mathbb{Z})$  sur le demi-plan supérieur  $\mathfrak{H}$  par homographies :

$$gz = \begin{pmatrix} p & q \\ r & s \end{pmatrix} z = \frac{pz + q}{rz + s},$$

ce qui a bien un sens puisque  $\text{Im}(gz) = \frac{\text{Im}(z)}{|rz+s|^2}$ . Le sous-groupe  $\{\pm \text{Id}\}$  opérant trivialement, on en déduit une action de  $G = \text{PSL}_2(\mathbb{Z})$ . Un calcul immédiat montre que le stabilisateur de  $i$  (resp.  $j$ ) dans  $\text{SL}_2(\mathbb{Z})$  est le sous-groupe  $\langle \alpha \rangle$  (resp.  $\langle \beta \rangle$ ), de sorte que  $G/A$  (resp.  $G/B$ ) s'identifie à l'orbite de  $i$  (resp. de  $j$ ).

7. Étant donné  $g \in G$ , le chemin continu  $\gamma_g : [0, 1] \rightarrow \mathfrak{H}$ ,  $t \mapsto g \left( e^{(\frac{1}{2} + \frac{t}{6})i\pi} \right)$  relie  $g(i)$  et  $g(j)$  dans  $\mathfrak{H}$ . Observons que l'on a défini  $\gamma_g$  de telle sorte que  $\gamma_g = g\gamma_e$  pour tout  $g \in G$ .

8. Soit  $|\Gamma|$  la réalisation géométrique du graphe  $\Gamma$ , obtenue en munissant  $G$  de la topologie discrète et en quotientant l'espace topologique  $[0, 1] \times G$  par la relation d'équivalence

$$(t, g) \sim (s, h) \iff (t = s = 0 \text{ et } gA = hA) \text{ ou } (t = s = 1 \text{ et } gB = hB).$$

Il s'agit d'un espace topologique connexe en vertu de la question 3.

L'application continue  $[0, 1] \times G \rightarrow \mathfrak{H}$ ,  $(t, g) \mapsto \gamma_g(t)$  passe au quotient en vertu de la question 6 et donne donc naissance à une application continue  $u : |\Gamma| \rightarrow \mathfrak{H}$  d'image  $T$ . Comme  $|\Gamma|$  est connexe, il en est de même de  $T$ .

**9.** Commençons par démontrer le fait suivant : étant donnés  $z \in \{e^{i\vartheta}, \pi/2 \leq \vartheta \leq 2\pi/3\}$  et  $g \in G$ , le point  $g(z)$  appartient au domaine

$$\left\{ z' \in \mathfrak{H} \mid \frac{-1}{2} \leq \operatorname{Re}(z') \leq 0 \text{ et } |z'| \geq 1 \right\}$$

si et seulement si  $z = i$  et  $g \in A$  ou  $z = j$  et  $g \in B$ .

Choisissons une matrice  $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \operatorname{SL}_2(\mathbb{Z})$  représentant  $g$ . Quitte à remplacer  $z$  par  $gz$  et  $g$  par  $g^{-1}$ , on peut supposer  $\operatorname{Im}(g(z)) \geq \operatorname{Im}(z)$  et donc  $|rz + s|^2 \leq 1$ .

- Si  $r = 0$ , alors  $g(z) = z \pm q$  et donc  $q = 0$ ,  $g = e$ .
- Supposons  $r \neq 0$ . Comme  $|z + \lambda| > 1/2$  pour tout  $\lambda \in \mathbb{Q}$ ,  $|r|^2 \leq |z + s/r|^{-2} < 4$  et donc  $r = \pm 1$ . Quitte à remplacer la matrice considérée par son opposée, on peut supposer  $r = 1$ . La condition  $|z + s| \leq 1$  implique  $s = 0$  ou ( $z = j$  et  $s = 0, 1$ ).
- Si  $s = 0$ , alors  $q = -1$  puisque  $ps - qr = 1$  et  $r = 1$ . On a ainsi  $g(z) = p - \frac{1}{z}$ , ce qui est impossible.
- Il reste à examiner le cas  $z = j$  et  $r = s = 1$ . On a  $g(z) = g(j) = 1 + q - \frac{1}{1+j} = 1 + q + j$ , donc  $q = -1$ ,  $g(j) = j$  et finalement  $g \in B$  en vertu de la question 6.

Notre assertion est démontrée.

Une première conséquence de cette observation est l'injectivité de l'application  $\varphi : T \rightarrow \mathfrak{H}$ . En effet, si  $(t_1, g_1)$  et  $(t_2, g_2)$  sont deux points de  $[0, 1] \times G$  tels que  $\gamma_{g_1}(t_1) = \gamma_{g_2}(t_2)$ , alors  $g_1\gamma_e(t_1) = g_2\gamma_e(t_2)$  et  $g_2^{-1}g_1\gamma_e(t_1) = \gamma_e(t_2)$ ; comme  $\gamma_e(t_1), \gamma_e(t_2) \in \{e^{i\vartheta}; \pi/2 \leq \vartheta \leq 2\pi/3\}$ , il découle de ce que l'on vient de dire que l'on a

$$(\gamma_e(t_1) = \gamma_e(t_2) = i \text{ et } g_2A = g_1A) \text{ ou } (\gamma_e(t_1) = \gamma_e(t_2) = j \text{ et } g_2B = g_1B),$$

ce qui signifie précisément que les points  $(g_1, t_1)$  et  $(g_2, t_2)$  ont la même image dans  $|\Gamma|$ .

Toute application continue d'un espace topologique localement compact dans un espace topologique séparé étant propre, nous concluons de ce qui précède que l'application  $\varphi$  est un homéomorphisme de  $|\Gamma|$  sur  $T$ .

Il découle également de l'observation initiale que  $i$  est l'unique élément de  $T$  de partie réelle nulle. Soit en effet  $z$  est un point de  $\mathfrak{H}$  vérifiant  $\operatorname{Re}(z) = 0$ . Comme  $\operatorname{Im}(az) = \operatorname{Im}(z)^{-1}$ , on peut supposer  $|z| = \operatorname{Im}(z) \geq 1$ . Il existe par hypothèse un élément  $z'$  de  $\{e^{i\vartheta}, \pi/2 \leq \vartheta \leq 2\pi/3\}$  et  $g \in G$  tels que  $z = g(z')$ ; on a alors  $z' = i$  et  $g \in A$ , d'où  $z = g(i) = i$ .

Considérons un point  $t$  dans  $T \cap \{z \in \mathfrak{H}, \operatorname{Re}(z) < 0\}$  et soit  $c : [0, 1] \rightarrow T$  un chemin reliant  $t$  à  $i$ . On note  $t_0$  le plus petit élément de  $]0, 1[$  tel que  $c(t_0) = i$ . Il y a dans  $\Gamma$  exactement deux arêtes contenant le sommet  $A$  : l'une, correspondant à l'élément  $e$ , relie  $A$  et  $B$ ; l'autre, correspondant à l'élément  $a$ , relie  $A$  et  $aB$ . Comme  $\gamma_a([0, 1]) = \{e^{i\vartheta}, \pi/3 \leq \vartheta < \pi/2\}$  est entièrement contenu dans  $\{z \in \mathfrak{H}; \operatorname{Re}(z) > 0\}$ , on en déduit que  $\varphi^{-1} \circ c([0, t_0[)$  doit rencontrer l'intérieur de l'arête de  $|\Gamma|$  reliant les sommets  $B$  et  $A$ . De manière équivalente,  $c([0, t_0[)$  contient un point de la forme  $e^{i\vartheta}$  avec  $\pi/2 < \vartheta < 2\pi/3$  et  $t$  peut par conséquent être relié au point  $j$  par un chemin dans  $T \cap \{z \in \mathfrak{H}; \operatorname{Re}(z) < 0\}$ . Nous avons ainsi démontré la connexité par arcs de  $T \cap \{z \in \mathfrak{H}; \operatorname{Re}(z) < 0\}$ . Le cas de  $T \cap \{z \in \mathfrak{H}; \operatorname{Re}(z) > 0\}$  s'en déduit immédiatement puisque  $a$  échange ces deux sous-espaces.

Écrivant  $T - \{i\}$  sous la forme  $T \cap \{z \in \mathfrak{H}; \operatorname{Re}(z) < 0\} \cup T \cap \{z \in \mathfrak{H}; \operatorname{Re}(z) > 0\}$ , il est clair que  $T - \{i\}$  n'est pas connexe.

**10.** Considérons un cycle  $(g_1, \dots, g_n)$  dans  $\Gamma$ . La concaténation des chemins  $\gamma_{g_1}, \dots, \gamma_{g_n}$  fournit un lacet non constant  $c$  dans  $T$  passant par  $g_1(i)$ . Par suite,  $g_1^{-1}c - \{i\}$  est entièrement

contenu dans l'une des deux composantes connexes de  $T - \{i\}$  et finalement, vu la description de  $T$  au voisinage de  $i$  que l'on a donnée à la question précédente, il existe un indice  $\ell$  tel que  $g_{\ell+1} = g_\ell$ . Nous avons ainsi démontré que le graphe  $\Gamma$  ne contient pas de cycle injectif, ce qui signifie précisément qu'il s'agit d'un arbre.

**11.** La conclusion découle directement des questions 5 et 10 :

$$\mathrm{PSL}_2 = A * B \simeq \mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/3\mathbb{Z}.$$

---