THÉORIE DES GROUPES - SÉRIE 13

13 décembre 2019

Groupes libres

Exercice 1. Montrer qu'un groupe F est libre si et seulement si, pour tout homomorphisme surjectif $\phi\colon G \to H$ et tout homomorphisme $\psi\colon F \to H$, il existe un homomorphisme $\alpha\colon F \to G$ tel que $\psi = \phi \circ \alpha$.
Astuce: Utiliser (sans preuve) qu'un sous-groupe d'un groupe libre est libre.

Solution. Supposons que F soit un groupe libre. Alors il existe un ensemble S qui forme une base pour F. Soient $\phi\colon G \to H$ un homomorphisme surjectif et $\psi\colon F \to H$ un homomorphisme. On construit un homomorphisme $\alpha\colon F \to G$ tel que $\psi = \phi \circ \alpha$. Soit $s \in S$. Comme ϕ est surjective, il existe $g_s \in G$ tel que $\phi(g_s) = \psi(s)$. On définit une fonction $a\colon S \to G$ par $a(s) = g_s$. Par la propriété universelle du groupe libre F, la fonction $a\colon S \to G$ s'étend uniquement en un homomorphisme de groupe $\alpha\colon F \to G$. De plus, comme $\phi \circ \alpha(s) = \phi \circ a(s) = \phi(g_s) = \psi(s)$, par unicité de la propriété universelle pour F, on obtient que $\phi \circ \alpha = \psi$.

Supposons maintenant que F satisfait la condition que: pour tout homomorphisme surjectif $\phi\colon G \to H$ et tout homomorphisme $\psi\colon F \to H$, il existe un homomorphisme $\alpha\colon F \to G$ tel que $\psi = \phi \circ \alpha$. Par une proposition du cours, il existe un groupe libre $\mathcal{F}$ et un homomorphisme surjectif $\phi\colon \mathcal{F} \to F$. On pose $\psi = \mathrm{id}_F\colon F \to F$. Par la propriété ci-dessus, il existe un homomorphisme $\alpha\colon F \to \mathcal{F}$ tel que $\phi \circ \alpha = \mathrm{id}_F$. On montre facilement que α est injective (puisque id_F l'est). Donc F est isomorphe à un sous-groupe du groupe libre $\mathcal{F}$ et est donc lui-même libre par l'Astuce.

Exercice 2. Soient G un groupe et $N < G$ un sous-groupe normal tel que le quotient G/N est libre. Montrer qu'il existe un sous-groupe $H < G$ tel que $G = HN$ et $H \cap N = \{e\}$.
Astuce: Utiliser l'Exercice 1.

Solution. On applique l'Exercice 4 au groupe libre $F = G/N$, à l'homomorphisme quotient $\phi = \pi\colon G \to G/N$ et à l'identité $\psi = \mathrm{id}_{G/N}\colon G/N \to G/N$. On trouve donc un homomorphisme $\alpha\colon G/N \to G$ tel que $\pi \circ \alpha = \mathrm{id}_{G/N}$. On pose $H = \mathrm{Im}(\alpha)$. Soient $g \in G$ et $h = \alpha(gN) \in H$. Alors

$$gN = \pi(\alpha(gN)) = \pi(h) = hN$$

et il existe $n \in N$ tel que $g = hn$. Donc on a bien $G = HN$. Finalement, soit $h \in H \cap N$. Comme $h \in H$, il existe $g \in G$ tel que $h = \alpha(gN)$. De plus, comme $h \in N$, alors

$$gN = \pi(\alpha(gN)) = \pi(h) = hN = N$$

et donc $g \in N$. Ainsi $h = \alpha(N) = e$ puisque α est un homomorphisme. Cela montre que $H \cap N = \{e\}$.

Exercice 3. Montrer que le centre d'un groupe libre de rang > 1 est trivial.

Solution. Soit F un groupe libre de rang > 1 et soit S l'ensemble qui forme une base pour F. Soit $x \in Z(F)$ un élément du centre de F. On écrit le mot réduit $x = s_1^{m_1} \cdots s_n^{m_n}$ avec $s_i \in S$ pour tout $1 \leq i \leq n$ et $s_i \neq s_{i+1}$ pour tout $1 \leq i < n$. Supposons par l'absurde que $n > 0$. Comme $x \in Z(F)$, alors

$$(s_{n-1}^{-m_{n-1}} \cdots s_1^{-m_1})x \underset{1}{=} x(s_{n-1}^{-m_{n-1}} \cdots s_1^{-m_1})$$

et, en simplifiant à gauche, on obtient que

$$s_n^{m_n} = s_1^{m_1} \cdots s_n^{m_n} s_{n-1}^{-m_{n-1}} \cdots s_1^{-m_1}.$$

Par unicité de l'écriture, on doit avoir $n = 1$. Donc x est de la forme $x = s_1^{n_1}$. Soit $t \in S$ tel que $t \neq s_1$. Alors, comme $x \in Z(F)$, on a que

$$s_1^{n_1} t = xt = tx = ts_1^{n_1}$$

mais par unicité de l'écriture, on obtient une contradiction. Donc $n = 0$ et $x = e$. On conclut donc que $Z(F) = \{e\}$.

Exercice 4. Soit F un groupe libre. Montrer qu'il existe un automorphisme $\phi\colon F \to F$ tel que

(i) si $\phi(x) = x$, alors $x = e$, et

(ii) $\phi \circ \phi$ est l'identité sur F.

(Comparer avec l'Exercice 10 Série 1.)

Solution. Soit S l'ensemble qui forme une base pour F. On définit une fonction $f\colon S \to F$ par $f(s) = s^{-1}$. Par la propriété universelle de F, il existe un unique homomorphisme $\phi\colon F \to F$ tel que $\phi(s) = f(s) = s^{-1}$ pour tout $s \in S$. On vérifie que ϕ satisfait les conditions (i) et (ii). On remarque que $\phi \circ \phi(s) = \phi \circ f(s) = \phi(s^{-1}) = s$ pour tout $s \in S$ et, par l'unicité dans la propriété universelle de F, on obtient que $\phi \circ \phi = \mathrm{id}_F$. Supposons maintenant que $\phi(x) = x$ pour un certain $x \in F$. On écrit le mot réduit $x = s_1^{\pm 1} \cdots s_n^{\pm 1}$ avec $s_i \in S$ pour tout $1 \leq i \leq n$. Alors $s_1^{\pm 1} \cdots s_n^{\pm 1} = x = \phi(x) = s_1^{\mp 1} \cdots s_n^{\mp 1}$, d'où $s_1^{\pm 1} \cdots s_n^{\pm 1} s_n^{\pm 1} \cdots s_1^{\pm 1} = e$. Si $n > 0$, alors $s_n^{\pm 1} s_n^{\pm 1}$ ne se simplifie pas. Donc on obtient directement $n = 0$ et $x = e$.

Exercice 5.

(a) Montrer le **Lemme du Ping-Pong**:

Soit G un groupe qui agit sur un ensemble X. Soient $g_1, \dots, g_k \in G$ d'ordre infini, pour $k \geq 2$. Supposons qu'il existe des sous-ensembles non-vides et disjoints $X_1, \dots, X_k$ de X tels que $g_i^n X_j \subseteq X_i$ pour tout $i \neq j \in \{1, \dots, k\}$ et tout $n \in \mathbb{Z}^*$. Alors le sous-groupe $H = \langle g_1, \dots, g_k \rangle < G$ est libre avec base $\{g_1, \dots, g_k\}$.

Astuce: Montrer que tout mot réduit $w = g_{i_1}^{n_1} \cdots g_{i_r}^{n_r}$ n'est pas trivial en considérant son action sur un des X_i (bien choisir!). Commencer par le cas où $i_1 = i_r$.

(b) Utiliser le Lemme du Ping-Pong pour montrer que le sous-groupe $\langle A, B \rangle$ de $SL_2(\mathbb{Z})$ est libre, où

$$A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \text{ et } B = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}.$$

Solution.

(a) Soit $w = g_{i_1}^{n_1} \cdots g_{i_r}^{n_r}$ un mot réduit.

Cas 1: Supposons d'abord que $i_1 = i_r$. Comme w est réduit, on peut supposer de plus que $i_j \neq i_{j+1}$ pour tout $1 \leq j \leq r-1$. Soit $k \neq i_1$. Alors

$$wX_k = g_{i_1}^{n_1} \cdots g_{i_r}^{n_r} X_k \underset{k \neq i_r}{\subseteq} g_{i_1}^{n_1} \cdots g_{i_{r-1}}^{n_{r-1}} X_{i_r} \underset{i_r \neq i_{r-1}}{\subseteq} g_{i_1}^{n_1} \cdots g_{i_{r-2}}^{n_{r-2}} X_{i_{r-1}} \subseteq \ldots \subseteq g_{i_1}^{n_1} X_{i_2} \subseteq X_{i_1}.$$

En particulier, w n'agit pas trivialement sur X_k, puisque X_{i_1} et X_k sont disjoints. Donc $w \neq e$.

Cas 2: Supposons maintenant que $i_1 \neq i_r$. Soit $m \in \mathbb{Z}$ tel que $m \neq n_1$ et $m \neq 0$. On pose

$$w' = g_{i_1}^{-m} w g_{i_1}^{m} = g_{i_1}^{-m} g_{i_1}^{n_1} \cdots g_{i_r}^{n_r} g_{i_1}^{m} = g_{i_1}^{n_1 - m} \cdots g_{i_r}^{n_r} g_{i_1}^{m}$$

Alors w' est un mot réduit comme dans le premier cas. Donc $w' \neq e$ et ainsi $w = g_{i_1}^{m} w' g_{i_1}^{-m} \neq e$.

(b) On considère l'action (standard) de $SL_2(\mathbb{Z})$ sur $\mathbb{R}^2$. On remarque tout d'abord que, pour $n \in \mathbb{Z}$, on a

$$A^n = \begin{pmatrix} 1 & 2n \\ 0 & 1 \end{pmatrix} \text{ et } B^n = \begin{pmatrix} 1 & 0 \\ 2n & 1 \end{pmatrix}.$$

En particulier, les matrices A et B sont d'ordre infini. On pose $G = SL_2(\mathbb{Z})$, $g_1 = A$, $g_2 = B$ et $X = \mathbb{R}^2$ dans le Lemme du Ping-Pong et on considère les sous-ensembles

$$X_1 = \{(x, y) \in \mathbb{R}^2 \mid |x| > |y|\} \text{ et } X_2 = \{(x, y) \in \mathbb{R}^2 \mid |x| < |y|\}.$$

Alors X_1 et X_2 sont disjoints. De plus, on a que $A^n X_2 \subseteq X_1$ et $B^n X_1 \subseteq X_2$ pour tout $n \in \mathbb{Z}$. Par le Lemme du Ping-Pong, le sous-groupe $\langle A, B \rangle$ de $SL_2(\mathbb{Z})$ est libre.

Présentations de groupes

Exercice 6. Trouver des présentations pour les groupes suivants:

(a) le groupe libre $\mathcal{F}(X)$ sur un ensemble X,

(b) le groupe cyclique $\mathbb{Z}/n\mathbb{Z}$ pour $n \in \mathbb{N}$,

(c) le groupe symétrique S_3,

(d) le groupe symétrique S_4,

(e) le groupe abélien libre $\mathbb{Z}^3$ de rang 3,

(f) le produit de groupes cycliques $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ pour $n, m \in \mathbb{N}$,

(g) le groupe des quaternions $\mathbf{Q}$ (voir Exercice 8 Série 3).

Solution.

(a) $\mathcal{F}(X) \cong \langle x \in X \mid \emptyset \rangle$.

(b) $\mathbb{Z}/n\mathbb{Z} \cong \langle x \mid x^n \rangle$.

(c) $S_3 \cong \langle x, y \mid x^2, y^3, (xy)^2 \rangle$, où l'isomorphisme identifie (par exemple) $(1\ 2) \leftrightarrow x$, $(1\ 2\ 3) \leftrightarrow y$.

(d) $S_4 \cong \langle x, y \mid x^2, y^3, (xy)^4 \rangle$, où l'isomorphisme identifie (par exemple) $(1\ 2) \leftrightarrow x$, $(2\ 3\ 4) \leftrightarrow y$.

(e) $\mathbb{Z}^3 \cong \langle x, y, z \mid xyx^{-1}y^{-1}, xzx^{-1}z^{-1}, yzy^{-1}z^{-1} \rangle$.

(f) $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \cong \langle x, y \mid x^n, y^m, xyx^{-1}y^{-1} \rangle$.

(g) $\mathbf{Q} \cong \langle i, j \mid i^4, i^2j^2, ijij^{-1} \rangle$, où l'isomorphisme identifie (par exemple) $A \leftrightarrow i$, $B \leftrightarrow j$.

Exercice 7. On considère le groupe G de présentation

$$G = \langle x, y, z \mid x^2 = y^3 = z^3 = xyz \rangle.$$

(a) Montrer que G n'a pas de sous-groupe d'indice 2.

(b) Montrer que $xyz \in Z(G)$ et que $G/\langle xyz \rangle \cong A_4$.

Solution.

(a) Supposons que $H < G$ soit un sous-groupe d'indice $[G : H] = 2$. Alors $G/H \cong \mathbb{Z}/2\mathbb{Z}$ et il existe un homomorphisme de groupes surjectif $f\colon G \to \mathbb{Z}/2\mathbb{Z}$. Or on calcule que

$$0 = 2f(x) = f(x^2) = f(y^3) = 3f(y) = f(y) \text{ et } 0 = 2f(x) = f(x^2) = f(z^3) = 3f(z) = f(z).$$

De plus, on a aussi

$$0 = f(x^2) = f(xyz) = f(x) + f(y) + f(z) = f(x).$$

Ainsi $f(x) = f(y) = f(z) = 0$ et comme x, y, z génère G, alors $f = 0$. Donc f ne peut pas être surjective. Contradiction!

(b) Pour montrer que $xyz \in Z(G)$, il suffit de montrer que xyz commute avec x, y et z respectivement. C'est en effet le cas puisque $xyz = x^2 = y^3 = z^3$. En particulier, cela implique que le sous-groupe $\langle xyz \rangle$ est normal dans G. Le groupe quotient $G/\langle xyz \rangle$ admet la présentation suivante

$$\begin{aligned} G/\langle xyz \rangle &\cong \langle x, y, z \mid x^2 = y^3 = z^3 = xyz = e \rangle \\ &\underset{x=yz}{\cong} \langle y, z \mid y^3 = z^3 = (yz)^2 = e \rangle \end{aligned}$$

On montre que cette dernière présentation est une présentation de A_4. On note

$$G' = \langle y, z \mid y^3 = z^3 = (yz)^2 = e \rangle$$

et on considère l'homomorphisme $\phi\colon G' \to A_4$ tel que $\phi(y) = (1\ 2\ 3)$ et $\phi(z) = (2\ 3\ 4)$. On calcule que

$$\phi(yz) = \phi(y)\phi(z) = (1\ 2\ 3)(2\ 3\ 4) = (1\ 2)(3\ 4).$$

Alors ϕ est bien défini, car

$$\phi(y)^3 = (1\ 2\ 3)^3 = \mathrm{id} = \phi(e) = \phi(y^3),$$

$$\phi(z)^3 = (2\ 3\ 4)^3 = \mathrm{id} = \phi(e) = \phi(z^3),$$

$$\phi(yz)^2 = ((1\ 2)(3\ 4))^2 = \mathrm{id} = \phi(e) = \phi((yz)^2).$$

Comme A_4 est engendré par les éléments $(1\ 2\ 3)$ et $(2\ 3\ 4)$, alors ϕ est surjectif. Donc $|G'| \geq |A_4| = 12$. On montre que $|G'| \leq 12$, ce qui implique que $|G'| = 12$ et que ϕ est un isomorphisme.

On pose $a = yz$ et $b = zy$. Remarquez que $b = zy = y^{-1}yzy = y^{-1}ay$. On a que $a^2 = (yz)^2 = e$ et $b^2 = (y^{-1}ay)^2 = y^{-1}a^2y = e$. De plus,

$$(ab)^2 = yz^{-1}y^{-1}z^{-1}y = y(yz)^{-2}y^2 = ya^{-2}y^2 = y^3 = e.$$

Ainsi on a $ab = (ab)^{-1} = ba$. Donc le sous-groupe $H = \langle a, b\rangle < G'$ est isomorphisme à $Z/2\mathbb{Z} \times Z/2\mathbb{Z}$ et est d'ordre 4. On considère également le sous-groupe $K = \langle y\rangle < G'$ d'ordre 3. On a que $y^{-1}ay = zy = b \in H$ et $y^{-1}by = y^{-1}zy^{-1} = y^{-1}z^{-1}z^{-1}y^{-1} = (zy)^{-1}(yz)^{-1} = ba \in H$. Donc $K < N_{G'}(H)$ et ainsi HK est un sous-groupe de G'. On remarque également que $y, z \in HK$, car $y \in K$ et $z = y^{-1}yz = y^{-1}a \in HK$. Comme G' est généré par y, z, alors $G' = HK$ et donc $|G'| = |HK| \leq |H||K| = 12$. On conclut que $G' \cong A_4$. Donc on a bien $G/\langle xyz\rangle \cong A_4$.