TD4 : groupes résolubles et nilpotents, croissance des groupes

Exercices $\star$: à préparer à la maison avant le TD, seront corrigés en début de TD.
Exercices $\star\star$: seront traités en classe en priorité.
Exercices $\star\star\star$: plus difficiles.

Si G est un groupe, on note $C^0(G) := G$ et $C^{n+1}(G) := [G, C^n(G)]$, à savoir le sous-groupe de G engendré par les commutateurs $ghg^{-1}h^{-1}$, avec $g \in G$ et $h \in C^n(G)$. On dit que G est nilpotent s'il existe $N \geq 0$ tel que $C^N(G) = \{e\}$. Dans ce cas, l'entier $N \geq 0$ minimal tel que $C^N(G) = \{e\}$ est appelé classe de nilpotence de G.

Exercice 1 : $\star$
Soit G un groupe.

a) Donner une définition des groupes nilpotents en termes de suite de composition.

b) Montrer qu'un groupe nilpotent est résoluble.

c) Que dire de la réciproque ?

d) Montrer que le centre d'un groupe nilpotent est non trivial.

e) Montrer que si G est nilpotent et H est un sous-groupe de G, alors H est nilpotent.

f) On suppose désormais dans la suite que H est un sous-groupe distingué de G. Montrer que si G est nilpotent, G/H est nilpotent.

g) On suppose H et G/H nilpotents. Le groupe G est-il nilpotent ?

h) Les groupes $\mathfrak{S}_3$ et $\mathfrak{S}_4$ sont-ils résolubles ? nilpotents ?

i) Soit p un nombre premier. Montrer que tout p-groupe est nilpotent (on pourra montrer que le centre d'un tel groupe est non-trivial, en utilisant la partition du groupe en classes de conjugaison).

j) (***) Soient p, q, r trois nombres premiers. Montrer que tout groupe d'ordre pqr est résoluble. Un tel groupe est-il nilpotent ?

k) On suppose G fini. Montrer que si G est nilpotent, alors tout sous-groupe maximal de G est distingué (la réciproque est vraie, mais plus difficile).

Solution de l'exercice 1.

a) Montrons que G est nilpotent si et seulement s'il existe une suite de sous-groupes de G

$$G = G_0 \supset G_1 \supset \cdots \supset G_{n+1} = \{e\}$$

telle que pour tout i, $G_i \lhd G$ et G_i/G_{i+1} est central dans G/G_{i+1}.
Si G est nilpotent, il suffit de prendre $G_i := G^i(G)$ pour tout i.
Réciproquement, on voit que la condition "G_i/G_{i+1} central dans G/G_{i+1}" équivaut à l'inclusion $[G, G_i] \subset G_{i+1}$, donc une récurrence simple assure que l'on a pour tout i, $C^i(G) \subset G_i$, donc $C^{n+1}(G) = \{e\}$, donc G est nilpotent.

b) On montre facilement par récurrence que pour tout $n \in \mathbb{N}$, on a $D^n(G) \subset C^n(G)$. Cela assure l'implication demandée.

c) La réciproque est fausse : le groupe $G = \mathfrak{S}_3$ est résoluble puisque sont groupe dérivé est le groupe abélien $\mathfrak{A}_3 \cong \mathbb{Z}/3\mathbb{Z}$, donc $D^2(G) = \{\mathrm{id}\}$ (G est extension d'un groupe abélien par un autre groupe abélien). En revanche, G n'est pas nilpotent puisque $C^1(G) = \mathfrak{A}_3$ n'est pas central dans G (le 3-cycle (123) ne commute pas avec (12) par exemple), donc $C^2(G) = [\mathfrak{S}_3, \mathfrak{A}_3]$ est un sous-groupe non trivial de $\mathfrak{A}_3 \cong \mathbb{Z}/3$, donc $C^2(G) = \mathfrak{A}_3 = C^1(G)$, donc $C^n(G) = \mathfrak{A}_3$ pour tout $n \geq 1$.

d) Soit G un groupe nilpotent. Il existe un entier $n \geq 0$ maximal tel que $C^n(G) \neq \{e\}$. Alors $C^{n+1}(G) = \{e\}$, donc $[G, C^n(G)] = \{e\}$, ce qui signifie que le sous-groupe non trivial $C^n(G)$ est contenu dans le centre de G. Donc $Z(G) \neq \{e\}$.

e) Une récurrence simple assure que pour tout $n \geq 0$, $C^n(H) \subset C^n(G)$, d'où le résultat.

f) La projection canonique $\pi : G \to G/H$ est un morphisme de groupes, donc une récurrence assure que $\pi(C^n(G)) \subset C^n(G/H)$ pour tout n. Or π est surjectif, donc une nouvelle récurrence assure que $\pi(C^n(G)) = C^n(G/H)$ (un commutateur dans G/H se relève en un commutateur dans G...). Cette égalité assure le résultat.

g) Non. Si $G = \mathfrak{S}_3$, $H = \mathfrak{A}_3$ et $G/H = \{\pm 1\}$, alors H et G/H sont abéliens donc nilpotents, alors que G n'est pas nilpotent par la question c).

En revanche, on a le résultat plus faible suivant : si $H \subset G$ est un sous-groupe central, alors G/H nilpotent implique G nilpotent. En effet, la question précédente assure que si $C^n(G/H) = \{e\}$, alors $C^n(G) \subset H$, donc $C^{n+1}(G) = [G, C^n(G)] \subset [G, H] \subset [G, Z(G)] = \{e\}$, donc G est nilpotent.

h) On voit facilement que ces groupes sont résolubles : pour $\mathfrak{S}_3$, le sous-groupe dérivé est abélien, donc il est bien résoluble. Pour $\mathfrak{S}_4$, le sous-groupe dérivé est $\mathfrak{A}_4$, qui admet un sous-groupe V_4 distingué isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (le sous-groupe des bitranspositions) tel que le quotient $\mathfrak{A}_4/V_4$ soit d'ordre 3, donc abélien, ce qui assure que $\mathfrak{S}_4$ est résoluble. Pour $\mathfrak{S}_3$, voir la question c). Et $\mathfrak{S}_3$ est isomorphe à un sous-groupe de $\mathfrak{S}_4$, donc la question e) assure que $\mathfrak{S}_4$ n'est pas nilpotent.

i) Soit G un groupe de cardinal p^n. On montre par récurrence sur n que G est nilpotent. Si $n = 1$, c'est évident car un groupe d'ordre p est commutatif. On suppose $n \geq 2$. Alors on considère la partition de G en classes de conjugaison : on note $g \sim g'$ si g et g' sont conjugués dans G. Alors $G = \coprod_{g \in G/\sim} C(g)$, où $C(g)$ désigne la classe de conjugaison de g dans G. Or $C(g)$ est réduite à un élément si et seulement si $g \in Z(G)$. Donc on déduit de la réunion précédente la formule

$$|G| = |Z(G)| + \sum_{g \in (G \setminus Z(G))/\sim} |C(g)|\,.$$

Or pour tout $g \in G \setminus Z(G)$, l'application $G \to C(g)$ définie par $h \mapsto hgh^{-1}$ induit une bijection $G/Z_G(g) \xrightarrow{\sim} C(g)$, où $Z_G(g)$ est le sous-groupe de G formé des éléments qui commutent avec g. En particulier, $Z_G(g)$ est un sous-groupe strict de G, donc $|G/Z_G(g)|$ est une puissance positive de p. Par conséquent, la formule $|G| = |Z(G)| + \sum_{g \in (G \setminus Z(G))/\sim} |C(g)|$ assure que $|G|$ est divisible par p, donc le centre $Z(G)$ de G n'est pas réduit à $\{e\}$, donc $G/Z(G)$ est de cardinal p^i avec $0 \leq i < n$. Par hypothèse de récurrence, $G/Z(G)$ est nilpotent, donc la remarque dans la réponse à la question g) assure que G est nilpotent.

j) — On suppose d'abord que $p = q = r$. Alors G est nilpotent par la question i), donc G est résoluble.

— On suppose maintenant $p = q \neq r$. Les théorèmes de Sylow assurent que $n_p = 1$ ou r et $n_r = 1$, p ou p^2. Supposons que $n_r = p^2$. Alors G contient exactement $p^2(r-1) = p^2 r - p^2 = |G| - p^2$ éléments d'ordre r, et un p-Sylow de G est de cardinal p^2, ce qui assure que G admet un unique p-Sylow, i.e. $n_p = 1$. Si l'on supose que $n_r = p$, alors nécessairement $n_p \neq r$ (sinon on aurait $p | r-1$ et $r | p-1$, ce qui est absurde), donc $n_p = 1$. Finalement, dans tous les cas, on a soit $n_r = 1$, soit $n_p = 1$. On a donc dans G un sous-groupe distingué d'ordre r ou d'ordre p^2, donc abélien, tel que le groupe quotient soit d'ordre p^2 ou r, donc abélien également. Cela assure que G est résoluble. En outre, G n'est pas nécessairement nilpotent (cf par exemple $G = \mathfrak{S}_3 \times \mathbb{Z}/2\mathbb{Z}$).

— On suppose maintenant que $p < q < r$. Alors $n_r = 1$ ou $n_r = pq$, et $n_q = 1$, r ou pr. Supposons que $n_r \neq 1$ et $n_q \neq 1$. Alors G admet exactement $pq(r-1)$ élément d'ordre r, et au moins $r(q-1)$ éléments d'ordre q. Donc on a

$$|G| \geq pq(r-1) + r(q-1) = pqr + (q-1)r - pq \geq pqr + pr - pq = |G| + p(r-q) > |G|\,,$$

ce qui est contradictoire. Donc $n_1 = 1$ ou $n_q = 1$, donc G admet un sous-groupe distingué d'ordre premier (donc abélien), tel que le quotient soit un groupe dont le cardinal est produit

de deux nombres premiers distincts. En particulier, ce quotient est résoluble (voir TD2, exercice 9, a)), donc G est résoluble. En revanche, G n'est pas toujours nilpotent, voir par exemple $G = \mathfrak{S}_3 \times \mathbb{Z}/5\mathbb{Z}$.

k) On suppose G nilpotent. Soit $M \subset G$ un sous-groupe maximal. Il existe un entier $n \geq 1$ minimal tel que $C^n(G) \subset M$. Par minimalité de n, il existe $g \in C^{n-1}(G) \setminus M$. Alors on a $[g, M] \subset [C^{n-1}(G), G] \subset C^n(G) \subset M$, ce qui assure que $gMg^{-1} \subset M$, donc $g \in N_G(M) \setminus M$. Donc $N_G(M)$ est un sous-groupe de G contenant strictement M. Par maximalité de M, cela implique que $N_G(M) = G$, donc M est distingué dans G.

Exercice 2 : ⋆⋆

Soit G un sous-groupe de $\mathrm{GL}_n(\mathbb{C})$. On note $T_n(\mathbb{C})$ le sous-groupe de $\mathrm{GL}_n(\mathbb{C})$ formé des matrices triangulaires supérieures.

a) Montrer que si G est connexe, alors $D(G)$ l'est aussi.

b) Montrer que si G est abélien, alors G est conjugué à un sous-groupe de $T_n(\mathbb{C})$.

c) On suppose G résoluble connexe. Montrer que G est conjugué à un sous-groupe de $T_n(\mathbb{C})$.

Solution de l'exercice 2.

a) Par définition, $D(G) = \bigcup_{n\in\mathbb{N}^*} G_n$, où G_n désigne l'ensemble des éléments de G qui s'écrivement comme produits de n commutateurs dans G. Montrons que pour tout n, G_n est connexe : l'application $c_n : G^{2n} \to G$ définie par $c_n(g_1, \ldots, g_{2n}) := [g_1, g_2] \ldots [g_{2n-1}, g_{2n}]$ est continue, et son image est exactement G_n. Cela assure que G_n est connexe car G^{2n} l'est. Or pour tout $n \geq 1$, G_n contient l'élément neutre de G, donc $D(G)$ admet un recouvrement par des parties connexes de G ayant toutes un point de G en commun, donc $D(G)$ est connexe.

b) Tout élément de $\mathrm{GL}_n(\mathbb{C})$ est trigonalisable, donc tout élément de G est trigonalisable. Or G est abélien, donc les éléments de G sont cotrigonalisables, i.e. il existe $P \in \mathrm{GL}_n(\mathbb{C})$ telle que $PGP^{-1} \subset T_n(\mathbb{C})$.

c) Soit G un groupe résoluble. On note V le $\mathbb{C}$-espace vectoriel $\mathbb{C}^n$. Montrons que si $n > 1$, V admet un sous-espace vectoriel strict non nul stable par tous les éléments de G. Pour ce faire, on raisonne par l'absurde, i.e. on suppose qu'aucun sous-espace vectoriel strict non nul de V n'est stable par G, et on va montrer que $n = 1$. On raisonne alors par récurrence sur la "classe de résolubilité" du groupe G, i.e. sur l'entier minimal $r \geq 1$ tel que $D^r(G) = \{I_n\}$.
   — Si $r = 1$, alors G est abélien, donc la question b) assure que V admet une droite stable par G, donc l'hypothèse implique que $n = 1$.
   — On suppose $r > 1$. Alors $H := D^{r-1}(G)$ est un sous-groupe commutatif distingué dans G, non trivial. La question b) assure que quitte à conjuguer, on peut supposer que H est un sous-groupe de $T_n(\mathbb{C})$. On définit

$$W := \{v \in V : v \text{ est vecteur propre de tout élément de } H\}.$$

   On sait que W contient une droite, donc $W \neq \{0\}$. Montrons que W est stable par G. Soit $w \in W$ et $g \in G$. Alors pour tout $h \in H$, on a $h(g(w)) = g(g^{-1}hg(w))$, et $g^{-1}hg \in H$ puisque H est distingué, donc $g^{-1}hg(w)$ est proportionnel à w, donc $h(g(w))$ est proportionnel à $g(w)$, donc $g(w) \in W$. Donc W est bien stable par G. Par hypothèse, on a donc $W = V$. Cela signifie que V admet une base de vecteurs propres pour tous les éléments de H, i.e. que quitte à conjuguer, on peut supposer que $H \subset D_n(\mathbb{C})$, où $D_n(\mathbb{C})$ désigne l'ensemble des matrices diagonales de $\mathrm{GL}_n(\mathbb{C})$.
   Montrons maintenant que $H \subset Z(G)$: pour tout $h \in H$ et tout $g \in G$, h et ghg^{-1} ont les mêmes valeurs propres. Or il n'existe qu'un nombre fini de matrices diagonales à valeurs propres fixées. Donc cela assure que l'application $c_h : G \to H$ définie par $c_h(g) := ghg^{-1}$ est d'image finie. Or cette application est continue et G est connexe, donc $c_h(G) = \{h\}$. Cela assure que h est dans le centre de G, donc $H \subset Z(G)$.
   Soit $h \in H \setminus \{I_n\}$. Soit U un espace propre de h. Puisque h commute avec tous les éléments de G, on voit que U est stable par G. Or U est non trivial, donc l'hypothèse initiale assure

que $U = V$. Donc h est une homothétie (matrice scalaire). Or $h \in D(G) \subset \mathrm{SL}_n(\mathbb{C})$, donc $\det(h) = 1$, donc H est fini. Or la question a) assure que H est connexe, donc $H = \{I_n\}$, ce qui est contradictoire avec le fait que $H = D^{r-1}(G) \neq \{I_n\}$.

On a donc montré que si $n \geq 2$ (ce qui est le cas si G n'est pas abélien), V admet un sous-espace vectoriel W strict non nul stable par G. On note W' un supplémentaire de W. La décomposition $V = W \oplus W'$ assure alors que quitte à conjuguer, G est contenu dans le sous-groupe des matrices "triangulaires supérieures par blocs", avec des blocs de taille $\dim(W)$ et $\dim(W')$: tout élément $g \in G$ s'écrit $g = \begin{pmatrix} g_W & * \\ 0 & g_{W'} \end{pmatrix}$. Donc l'image de G par le morphisme $g \mapsto g_W$ est un sous-groupe résoluble connexe de $\mathrm{GL}_{\dim(W)}(\mathbb{C})$, donc par récurrence, comme $\dim(W) < n$, quitte à conjuguer encore, on peut supposer que les matrices g_W sont triangulaires supérieures pour tout $g \in G$. De même, quitte à choisir une bonne base de V/W, on peut supposer que les matrices $g_{W'}$ sont triangulaires supérieures pour tout $g \in G$. Alors il est clair que G est un sous-groupe de $T_n(\mathbb{C})$.

Exercice 3 : $\star\star$

Soit G un groupe de type fini. On définit le sous-groupe de Frattini de G (noté $\phi(G)$) comme l'intersection des sous-groupes maximaux de G.

a) Montrer que $\mathbb{Q}$ ne possède pas de sous-groupe maximal.

b) Montrer que G admet au moins un sous-groupe maximal. La preuve est-elle plus simple si G est fini ?

c) Montrer que $\phi(G)$ est distingué dans G et même qu'il est stable par tout automorphisme de G (on dit qu'il est caractéristique). On note $\pi : G \to G/\phi(G)$ la projection canonique.

d) Soit $S \subset G$ une partie de G. Montrer que S engendre G si et seulement si $\pi(S)$ engendre $G/\phi(G)$.

e) Montrer que $\phi(G)$ est exactement l'ensemble des éléments $g \in G$ tels que pour toute partie $S \subset G$, on a : $\langle S, g\rangle = G \implies \langle S\rangle = G$.

f) (***) Montrer que si G est fini, alors $\phi(G)$ est nilpotent.

g) On suppose G fini. Montrer que si G est nilpotent, alors $D(G) \subset \phi(G)$ (la réciproque est vraie, mais plus difficile).

h) On suppose que G est un p-groupe.

   i) Montrer que tout sous-groupe maximal de G contient $D(G)$ et le sous-groupe G^p engendré par les puissances p-ièmes dans G.

   ii) Montrer que $G/\phi(G)$ est le plus grand quotient abélien de G d'exposant p.

   iii) Que peut-on en déduire sur le nombre minimal de générateurs de G ?

   iv) Montrer que $\phi(G) = D(G).G^p$.

Solution de l'exercice 3.

a) Soit H un sous-groupe strict de $\mathbb{Q}/\mathbb{Z}$. Il existe donc $x \in \mathbb{Q}/\mathbb{Z}$ tel que $x \notin H$. Notons $H' := \langle H, x\rangle$. C'est un sous-groupe de $\mathbb{Q}/\mathbb{Z}$ contenant strictement H. Or $x \in \mathbb{Q}/\mathbb{Z}$ est d'ordre fini n. On considère l'élément $\frac{x}{n} \in \mathbb{Q}/\mathbb{Z}$: si $\frac{x}{n} \in H'$, alors il existe $m \in \mathbb{Z}$ et $h \in H$ tel que $\frac{x}{n} = h + mx$. Donc $x = nh + 0 = nh$, donc $x \in H$, ce qui est contradictoire. Donc $\frac{x}{n} \notin H'$, donc $H' \neq \mathbb{Q}/\mathbb{Z}$, donc H n'est pas maximal dans $\mathbb{Q}/\mathbb{Z}$. Cela assure que $\mathbb{Q}/\mathbb{Z}$ n'admet pas de sous-groupe maximal.

b) On suppose $G \neq \{e\}$ et on écrit $G = \langle a_1, \ldots, a_n\rangle$. On considère l'ensemble $\mathcal{E}$ des sous-groupes stricts de G. C'est un ensemble non vide, muni de la relation d'ordre donnée par l'inclusion. Montrons que toute partie non vide totalement ordonnée $\mathcal{F}$ de $\mathcal{E}$ admet un majorant dans $\mathcal{E}$. Soit $\mathcal{F}$ une telle partie. On définit alors

$$M := \langle H; H \in \mathcal{F}\rangle = \bigcup_{H \in \mathcal{F}} H\,.$$

Il est clair que M est un sous-groupe de G contenant chacun des $H \in \mathcal{F}$. Montrons que $M \neq G$. Si on avait $M = G$, alors pour tout i, $a_i \in M$, donc pour tout i, il existe $H_i \in \mathcal{F}$ tel que $a_i \in H_i$. Or $\mathcal{F}$ est totalement ordonné, donc il existe $H \in \mathcal{F}$ tel que $a_i \in H$ pour tout $1 \leq i \leq n$. Alors $H = G$ puisque les a_i engendrent G. Ceci est une contradiction car $H \in \mathcal{F}$ est un sous-groupe strict de G. Cela assure donc que $M \neq G$, i.e. que $M \in \mathcal{E}$.

On peut alors appliquer le lemme de Zorn pour déduire que l'ensemble $\mathcal{E}$ admet un élément maximal, ce qui revient à dire que G admet un sous-groupe maximal.

Si le groupe G est fini, l'ensemble des sous-groupes de G est fini également, on peut se passer du lemme de Zorn en considérant un sous-groupe strict de G de cardinal maximum.

c) Soit $\varphi \in \mathrm{Aut}(G)$. Alors pour tout sous-groupe maximal $H \subset G$, $\varphi(H)$ est un sous-groupe maximal de G, et l'application $H \mapsto \varphi(H)$ est une permutation de l'ensemble des sous-groupes maximaux de G. Par conséquent, on a

$$\varphi(\phi(G)) = \bigcap_{H \subset G \text{ maximal}} \varphi(H) = \bigcap_{H \subset G \text{ maximal}} H = \phi(G)\,,$$

donc $\phi(G)$ est un sous-groupe caractéristique de G.

d) Le sens direct est clair puisque π est surjective. Montrons le sens réciproque : on suppose que $H = \langle S \rangle$ n'est pas égal à G. Alors H est contenu dans un sous-groupe maximal M de G. Comme H contient $\phi(G)$, $\pi(H)$ s'identifie à $H/\phi(G)$, qui est un sous-groupe strict de $G/\phi(G)$. Cela assure que $\langle \pi(S) \rangle \subset H/\phi(G)$ est un sous-groupe strict de $G/\phi(G)$, donc $\pi(S)$ n'engendre pas $G/\phi(G)$.

e) La question précédente assure que si $g \in \phi(G)$, alors pour tout $S \subset G$, on a $\langle S, g \rangle = G \implies \langle S \rangle = G$. Soit maintenant $g \in G \setminus \phi(G)$. Alors il existe un sous-groupe maximal H de G tel que $g \notin H$. On considère alors $S := H \subset G$. il est clair que $\langle S \rangle = H \neq G$ alors que $\langle S, g \rangle = G$ par maximalité de H. D'où la description de $\phi(G)$ recherchée.

f) Soit P un p-Sylow de $\phi(G)$. Comme $\phi(G)$ est distingué dans G, on en déduit que $G = \phi(G)N_G(P)$. La question d) assure alors que $G = N_G(P)$, donc P est distingué dans G, donc dans $\phi(G)$. Donc tout sous-groupe de Sylow de $\phi(G)$ est distingué dans $\phi(G)$, ce qui assure que $\phi(G)$ est produit de ses groupes de Sylow, donc $\phi(G)$ est nilpotent (voir exercice 1).

g) On suppose G nilpotent. Alors l'exercice 1 assure que pour tout sous-groupe maximal H de G, H est distingué, donc G/H est un groupe simple nilpotent, donc G/H est cyclique d'ordre premier, donc abélien, donc $D(G) \subset H$. Donc $D(G) \subset \phi(G)$.

h) i) Soit H un sous-groupe maximal de G. La preuve de la question précédente assure que H est distingué dans G et G/H est cyclique d'ordre p, ce qui assure que H contient $D(G)$ et G^p.

ii) La question précédente assure que $G/\phi(G)$ est un groupe abélien d'exposant p. Soit maintenant H un sous-groupe distingué de G tel que G/H soit abélien d'exposant p. Notons $\pi_H : G \to G/H$ la projection. On a donc un isomorphisme $G/H \cong (\mathbb{Z}/p\mathbb{Z})^r$. On considère alors les r-projections $\pi_i : (\mathbb{Z}/p\mathbb{Z})^r \to \mathbb{Z}/p\mathbb{Z}$: il est clair que $H = \bigcap_{i=1}^n H_i$, où $H_i := \mathrm{Ker}(\pi_i \circ \pi_H : G \to \mathbb{Z}/p\mathbb{Z})$, et que les H_i sont des sous-groupes maximaux de G (car d'indice p). Donc $H \subset \phi(G)$, ce qui assure l'existence d'un morphisme surjectif $\pi' : G/\phi(G) \to G/H$ tel que $\pi' \circ \pi = \pi_H$. Donc $G/\phi(G)$ est bien le plus grand quotient abélien d'exposant p de G.

iii) Soit $g_1, \ldots, g_m$ une famille génératrice de G. Alors $\pi(g_1), \ldots, \pi(g_m)$ engendrent $G/\phi(G)$, donc $m \geq \dim_{\mathbb{F}_p}(G/\phi(G))$. Or $G/\phi(G)$ admet une partie génératrice minimale de cardinal $\dim_{\mathbb{F}_p}(G/\phi(G))$, et en choisissant des relevés de ces générateurs dans G, on obtient une famille génératrice (voir question d)) de G de cardinal $\dim_{\mathbb{F}_p}(G/\phi(G))$. Cela assure que le nombre minimal de générateurs de G est égal à $\dim_{\mathbb{F}_p}(G/\phi(G))$.

iv) La question h)i) assure que $D(G).G^p \subset \phi(G)$. Or $G/D(G).G^p$ est clairement un groupe abélien d'exposant p, donc la question h)ii) assure que $\phi(G) \subset D(G).G^p$, ce qui conclut.

Exercice 4 : ⋆⋆

Soit G un groupe de type fini. Pour toute partie génératrice finie A de G, pour tout $m \in \mathbb{N}$, on note $B_{G,A}(m)$ l'ensemble des éléments de G qui s'écrivent comme produits d'au plus m éléments de $A \cup A^{-1}$. On pose $\beta_{G,A}(m) := |B_{G,A}(m)|$. Si β et β' sont deux fonctions $\mathbb{N} \to \mathbb{R}^+$, on notera $\beta \preceq \beta'$ s'il existe $c > 0$ et $a \in \mathbb{N}^*$ tels que pour tout n, $\beta(n) \leq c\beta'(an)$, et $\beta \sim \beta'$ si $\beta \preceq \beta'$ et $\beta' \preceq \beta$.

a) Montrer que $B_{G,A}(m)$ est une boule dans l'espace métrique (G, d), où d est une distance que l'on précisera.

b) Soient A et A' deux parties génératrices finies de G. Montrer que $\beta_{G,A} \sim \beta_{G,A'}$. On notera donc abusivement $\beta_G = \beta_{G,A}$.

c) Calculer β_G si G est un groupe fini, si $G = \mathbb{Z}$, si $G = \mathbb{Z}^n$, si G est le groupe libre à n générateurs (i.e. le groupe des mots finis sur un alphabet de n lettres, avec leurs inverses, pour la loi de concaténation des mots).

d) Montrer que $\beta_G(n) \preceq e^n$.

e) Si G' est un groupe de type fini, calculer $\beta_{G\times G'}$.

f) Montrer que si $H \subset G$ est un sous-groupe de type fini, alors $\beta_H \preceq \beta_G$, et si H est d'indice fini, alors $\beta_H \sim \beta_G$.

g) Soit H un quotient de G. Comparer β_H et β_G.

h) Montrer que si $G = \mathrm{SL}_2(\mathbb{Z})$, alors G est de type fini et $\beta_G(n) \sim e^n$.

i) Montrer que si G est nilpotent de classe 2, alors il existe $d \geq 0$ tel que $\beta_G(n) \preceq n^d$.

j) Montrer que si G est nilpotent, alors il existe $d \geq 0$ tel que $\beta_G(n) \preceq n^d$.

k) Montrer que le groupe $G = \mathbb{Z}^2 \rtimes_A \mathbb{Z}$, où le produit semi-direct est défini via la matrice $A := \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$, est un groupe résoluble tel que $\beta_G(n) \sim e^n$.

Solution de l'exercice 4.

a) Soient $g, h \in G$. On définit $d(g, h)$ comme le nombre minimal de termes dans une écriture de gh^{-1} comme produit d'éléments de $A \cup A^{-1}$. Il est clair que cela définit une application $d : G \times G \to \mathbb{N}$ telle que
— pour tous $g, h \in G$, $d(g, h) = d(h, g)$ (car l'ensemble $A \cup A^{-1}$ est stable par inverse).
— pour tous $g, h \in G$, $d(g, h) = 0$ si et seulement si $g = h$.
— pour tous $g, h, k \in G$, $d(g, k) \leq d(g, h) + d(h, k)$.
Donc (G, d) est un espace métrique, et $B_{G,A}(m)$ est la boule fermée de centre e et de rayon m pour cette distance d.

b) Il suffit de le montrer pour $A' = A \cup \{\alpha\}$ avec $\alpha \in G$. Il est clair que pour tout $m \geq 0$, on a $B_{G,A}(m) \subset B_{G,A'}(m)$, donc $\beta_{G,A} \preceq \beta_{G,A'}$. Or $\alpha \in G$ s'écrit $\alpha = a_1 \dots a_r$ avec $a_i \in A$ pour tout i. Soit $g \in B_{G,A'}(m)$. Alors $g = a'_1 \dots a'_k$ s'écrit comme un produit de $k \leq m$ éléments de A'. Pour tout $1 \leq i \leq k$, soit $a'_i \in A$, soit $a'_i = \alpha$ et a'_i est produit de r éléments de A. Cela assure que g est produit d'au plus kr éléments de A. Donc $B_{G,A'}(m) \subset B_{G,A}(km)$, donc $\beta_{G,A'} \preceq \beta_{G,A}$. Donc finalement $\beta_{G,A} \sim \beta_{G,A'}$.

c) — Si G est un groupe fini, alors on peut prendre $A = G$ et on voit que $\beta_{G,A}(m) = |G|$ pour tout $m \geq 1$, donc $\beta_G \sim 1$.
— Si $G = \mathbb{Z}$, on peut prendre $A = \{1\}$, et on voit que $B_{G,A}(m) = \{-m, -(m-1), \dots, 0 \dots, m-1, m\}$, donc $\beta_{G,A}(m) = 2m + 1$, donc $\beta_G(m) \sim m$.
— Si $G = \mathbb{Z}^n$, on peut prendre $A = \{-1, 0, 1\}^n$, et on voit que $B_{G,A}(m) = \mathbb{Z}^n \cap [-m; m]^n$, donc $\beta_{G,A}(m) = (2m + 1)^n$, donc $\beta_G(m) \sim m^n$.
— Si G est le groupe libre à $n \geq 2$ générateurs, notés $a_1, \dots, a_n$, on peut considérer $A = \{a_1, \dots, a_n\}$, où ϵ est l'élément neutre (mot vide). Alors on a $\beta_{G,A}(m) \geq n^m$ en considérant uniquement les mots de m lettres parmi $a_1, \dots, a_n$, et on a $\beta_{G,A}(m) \leq (2n + 1)^m$ de façon évidente. Donc $\beta_G(m) \sim n^m \sim e^m$.

d) En considérant le nombre de mots possibles de longueur m sur un alphabet à $2|A| + 1$ lettres, il est clair que $\beta_{G,A}(m) \leq (2|A| + 1)^m$, donc $\beta_G(m) \preceq e^m$.

e) On choisit une partie génératrice finie A (resp. A') de G (resp. G') stable par inverse et contenant l'élément neutre. Alors $A\times A'$ est une partie génératrice de $G\times G'$, et on a une bijection naturelle $B_{G,A}(m)\times B_{G',A'}(m)\cong B_{G\times G',A\times A'}(m)$, ce qui assure que $\beta_{G\times G'}\sim\beta_G\beta_{G'}$.

f) Il existe une partie génératrice finie A de H. On choisit une partie génératrice finie $B=A\cup A'$ de G. Il est alors clair que $B_{H,A}(m)\subset B_{G,B}(m)$, ce qui assure que $\beta_H\preceq\beta_G$.

On suppose maintenant que H est d'indice fini dans G. On munit G de la distance d_G définie par une partie génératrice finie (fixée) de G. Il est clair que l'action de G sur lui-même par translation est une action par isométries. On note $E\subset G$ un ensemble (fini) de représentants de G modulo H. On note $R:=\max\{d_G(e,x):x\in E\}$. Alors $E\subset B_G(R)$ et $G=\bigcup_{h\in H}B_G(h,R)$, i.e. $G=H.B_G(R)$.

On définit alors l'ensemble fini $S:=B_G(2R+1)\cap H$.

On va montrer que S engendre H et comparer $\beta_{H,S}(m)$ à $\beta_G(m)$.

Soit $h\in H$. On peut trouver $g_0,\dots,g_m\in G$ tels que $g_0=e$, $g_m=h$ et $d_G(g_i,g_{i+1})=1$, avec m minimal, i.e. $m=d_G(e,h)$.

Comme $G=\bigcup_{h\in H}B_G(h,R)$, pour tout i, il existe $h_i\in H$ tel que $g_i\in B_G(h_i,R)$, et on peut supposer $h_0=e$ et $h_m=h$.

On a alors $d(h_i,h_{i+1})\leq 2R+1$, ce qui assure que $s_i:=h_i^{-1}h_{i+1}\in S$. On en déduit via une récurrence simple que

$$h=h_m=h_{m-1}h_{m-1}^{-1}h_m=h_{m-1}s_m=s_1\dots s_m\,.$$

Cela montre en particulier que $H=\langle S\rangle$, et que $d_{H,S}(e,h)\leq m=d_G(e,h)$

Soit alors $m\in\mathbb{N}$ et $g\in B_G(m)$. On sait qu'il existe alors $h\in H$ tel que $d_G(g,h)\leq R$. Alors $d_G(e,h)\leq R+m$ par inégalité triangulaire. On a montré en outre que $d_{H,S}(e,h)\leq d_G(e,h)$, donc $d_{H,S}(e,h)\leq R+m$. Cela assure que

$$B_G(m)\subset\bigcup_{h\in B_{H,S}(R+m)}B_G(h,R)\,.$$

En calculant les cardinaux, on en déduit que

$$\beta_G(m)\leq|B_G(R)|\beta_{H,S}(R+m)\,,$$

ce qui assure que $\beta_G\preceq\beta_H$, d'où finalement

$$\beta_H\sim\beta_G\,.$$

g) Si A est une partie génératrice finie de G, et si $\pi:G\to H$ est la projection canonique, alors $\pi(A)$ est une partie génératrice finie de H. Il est alors clair que $\pi:B_{G,A}(m)\to B_{H,\pi(A)}(m)$ est une application surjective, ce qui assure que $\beta_H\preceq\beta_G$.

h) C'est un résultat classique que $\mathrm{SL}_2(\mathbb{Z})$ est de type fini. On considère le sous-groupe H de $\mathrm{SL}_2(\mathbb{Z})$ engendré par les matrices $A=\begin{pmatrix}1&2\\0&1\end{pmatrix}$ et $B=\begin{pmatrix}1&0\\2&1\end{pmatrix}$. Soient alors $r\geq 1$ et $k_1,l_1,\dots,k_r,l_r\in\mathbb{Z}$ des entiers tous non nuls.

Montrons que $A^{k_1}B^{l_1}\dots A^{k_r}B^{l_r}\neq I_2$.

Pour cela, on définit par récurrence $M_0=I_2$, $M_{2i+1}=M_{2i}A^{k_i}$ et $M_{2i+2}=M_{2i+1}B^{r_i}$, et on note $M_{2i}=\begin{pmatrix}m(2i)&*\\*&*\end{pmatrix}$ et $M_{2i+1}=\begin{pmatrix}*&m(2i+1)\\*&*\end{pmatrix}$. Une récurrence simple assure que $|m(i)|\geq i+1$ pour tout i. Cela assure immédiatement que le produit $A^{k_1}B^{l_1}\dots A^{k_r}B^{l_r}\neq I_2$.

Par conséquent, H est isomorphe au groupe libre à deux générateurs A et B (il faut pour cela également regarder des produits de la forme précédente avec $k_1=0$ ou $l_r=0$). Donc $\beta_H(m)\sim e^m$ par la question c). Cela assure que $\beta_G(m)\sim e^m$ grâce aux questions d) et f).

i) Si G est abélien de type fini et de rang r, alors $\beta_G(m) \sim m^r$ grâce au théorème de classification des groupes abéliens de type fini et au cas de $\mathbb{Z}^r$.

On suppose maintenant G nilpotent de classe 2. Alors $Z := D(G)$ est un sous-groupe central de G, et c'est un groupe abélien de type fini. Donc $\beta_Z(m) \sim m^r$. Fixons une partie génératrice $A = \{g_1, \dots, g_n\}$ de G (stable par inverse et contenant e) de G. Soit alors $g \in B_G(m)$. L'élément g s'écrit comme un produit d'au plus m éléments de A. On cherche à regrouper ces éléments pour écrire g sous la forme $g = g_1^{k_1} \dots g_n^{k_n} d$, avec $d \in Z$. Pour ce faire, on constate que $g_i g_j = g_j g_i [g_i^{-1}, g_j^{-1}]$, donc tout échange de deux générateurs produit un commutateur "à droite", i.e. un élément de Z. Comme Z est central, on peut écrire cet élément "à la fin" de l'écriture de g comme produit. De cette façon, une récurrence simple assure que l'on peut écrire $g = g_1^{k_1} \dots g_n^{k_n} d$, avec $0 \leq k_i \leq m$ et $d \in Z$ produit d'au plus m^2 commutateurs de la forme $[g_i, g_j]$. Donc en prenant pour partie génératrice de Z un partie finie contenant les $[g_i, g_j]$, on en déduit que $\beta_G(m) \leq m^n \beta_Z(m^2)$. Comme β_Z est polynômiale (cas des groupes abéliens de type fini), il existe $r \geq 0$ tel que $\beta_Z(m) \sim m^r$, donc on en déduit qu'il existe $d \geq 0$ tel que $\beta_G(m) \preceq n^d$.

j) Si G est abélien de type fini et de rang r, alors $\beta_G(m) \sim m^r$ grâce au théorème de classification des groupes abéliens de type fini et au cas de $\mathbb{Z}^r$.

On suppose G nilpotent de classe $c \geq 2$. On considère le sous-groupe $H = D(G)$ de G. Il est clair que H est de type fini, nilpotent de classe $\leq c-1$. Par récurrence, on peut supposer que $\beta_H(m) \preceq m^r$. On prend une partie génératrice finie $A = \{g_1, \dots g_n\}$ (stable par inverse et contenant e) de G. Soit alors $g \in B_G(m)$. L'élément g s'écrit comme un produit d'au plus m éléments de A. On cherche à regrouper ces éléments pour écrire g sous la forme $g = g_1^{k_1} \dots g_n^{k_n} d$, avec $d \in H$. Pour ce faire, on constate que $g_i g_j = g_j g_i [g_i^{-1}, g_j^{-1}]$, donc tout échange de deux générateurs produit un commutateur "à droite". On est ensuite amené à échanger ce commutateur avec un autre générateur g_k, ce qui produit un élément de la forme $[g_k^{-1}, [g_i^{-1}, g_j^{-1}]] \in C^2(G)$. On poursuit de cette façon jusqu'à obtenir une écriture de g de la forme $g = g_1^{k_1} \dots g_n^{k_n} d$ avec $d \in H$: on voit que d est produit d'au plus m^2 éléments $[g_i, g_j]$, d'au plus m^3 éléments $[g_i, [g_j, g_k]]$, etc... finalement, on peut écrire $g = g_1^{k_1} \dots g_n^{k_n} d$ avec $d \in H$ produit d'au plus $m^2 + \dots + m^c \leq m^{c+1}$ commutateurs de la forme précédente (commutateurs des g_i). Or tous ces commutateurs sont des mots de longueur bornée k sur un ensemble fini de générateurs de $D(G)$, ce qui assure que $\beta_G(m) = \mathcal{O}(m^n \beta_H(km^{c+1}))$, donc $\beta_G(m) \preceq m^{n+r(c+1)}$. Cela assure donc le résultat.

k) Il est clair que A admet deux valeurs propres réelles λ et λ^{-1}, avec $\lambda > 2$.

Montrons d'abord qu'il existe un vecteur $v \in \mathbb{Z}^2$ tel que pour tout $n \in \mathbb{N}$, les vecteurs $\sum_{i=0}^n \epsilon_i A^i v$ sont deux-à-deux distincts si $(\epsilon_0, \dots, \epsilon_n)$ décrivent $\{0,1\}^{n+1}$. La matrice transposée de A admet aussi λ pour valeur propre. Donc il existe une forme linéaire $f : \mathbb{R}^2 \to \mathbb{R}$ telle que ${}^t A f = \lambda f$. Il suffit alors de prendre $v \in \mathbb{Z}^2 \setminus \mathrm{Ker}(f)$ (la vérification est laissée au lecteur).

On voit v comme un élément de G, et on note $t = (0,0,1) \in G$. On fixe un ensemble S de générateurs de G contenant v et t. En particulier, pour tout $\underline{\epsilon} \in \{0,1\}^{n+1}$, les éléments $g_{\underline{\epsilon}} := v^{\epsilon_0} (tvt^{-1})^{\epsilon_1} \dots (t^n v t^{-n})^{\epsilon_n}$ sont des éléments deux-à-deux distincts de G. Donc l'application $\underline{\epsilon} \mapsto g_{\underline{\epsilon}}$ définit une injection de $\{0,1\}^{n+1}$ dans G telle que pour tout $\underline{\epsilon}$, $d_{G,S}(e, g_{\underline{\epsilon}}) \leq 3n+1$. On en déduit donc que pour tout n, $\beta_{G,S}(3n+1) \geq 2^{n+1}$, ce qui implique que $\beta_{G,S}(n) \sim e^n$ grâce à la question d).

Exercice 5 : $\star\star\star$

On note Σ^* l'ensemble des mots (finis) sur l'alphabet $\Sigma = \{0;1\}$, i.e. $\Sigma^* := \bigcup_{n \in \mathbb{N}} \Sigma^n$. On note G le groupe $\mathfrak{S}(\Sigma^*)$. On note $a \in G$ l'élément défini par $a(1m) := 0m$ et $a(0m) := 1m$ pour tout $m \in \Sigma^*$.

a) Montrer que les formules suivantes définissent des éléments b, c et d de G : $b(0m) = 0a(m)$, $c(0m) = 0a(m)$, $d(0m) = 0m$, $b(1m) = 1c(m)$, $c(1m) = 1d(m)$ et $d(1m) = 1b(m)$. On note $\Gamma := \langle a, b, c, d \rangle \subset G$.

b) Montrer que $a^2 = b^2 = c^2 = d^2 = \mathrm{id}$ et que $bc = cb = d$, $cd = dc = b$, $bd = db = c$.

c) Montrer que tout élément de Γ s'écrit comme produit des éléments a, b, c, d, avec un terme du produit sur deux égal à a.

d) Pour tout $n \geq 1$, on note $\Gamma_n := \{\gamma \in \Gamma : \gamma_{|\Sigma^n} = \mathrm{id}\}$. Montrer que Γ_n est un sous-groupe distingué strict d'indice fini de Γ.

e) On définit $\varphi_1 : \Gamma_1 \to G \times G$ par $\varphi_1(\gamma) := (\gamma_0, \gamma_1)$, où $\gamma_\epsilon(w)$ est le mot tel que $\gamma(\epsilon w) = \epsilon\gamma_\epsilon(w)$. Montrer que φ_1 est un morphisme de groupes injectif.

f) Montrer que les morphismes $\varphi^\epsilon : \Gamma_1 \to \Gamma$ définis par $\gamma \mapsto \gamma_\epsilon$ sont surjectifs. En déduire que Γ est infini.

g) Montrer que $\varphi_1(\Gamma_1)$ est un sous-groupe d'indice fini de $\Gamma \times \Gamma$.

h) Montrer que Γ n'est pas à croissance polynomiale, i.e. pour tout $d \geq 0$, $n^d \prec \beta_\Gamma(n)$.

i) Montrer que pour tout $\gamma \in \Gamma_1$, $l(\gamma_0) + l(\gamma_1) \leq l(\gamma) + 1$, où $l(g)$ désigne le nombre minimal de symboles a, b, c, d nécessaires pour écrire g.

j) Pour tout $n \geq 1$, généraliser les contructions précédentes pour obtenir un morphisme injectif $\varphi_n : \Gamma_n \to \Gamma^{\Sigma_n}$ tel que $\varphi_n(\Gamma_n)$ est un sous-groupe d'indice fini de Γ^{X_n}.

k) Montrer que pour tout $\gamma \in \Gamma_3$, si on note $\varphi_3(\gamma) = (\gamma_\epsilon)_{\epsilon \in \Sigma_3}$, alors

$$\sum_{\epsilon \in \Sigma_3} l(\gamma_\epsilon) \leq \frac{5}{6} l(\gamma) + 8\,.$$

l) Montrer que Γ n'est pas à croissance exponentielle, i.e. $\beta_\Gamma(n) \prec e^n$. On dit que Γ est à croissance intermédiaire.

Solution de l'exercice 5.

a) Une récurrence simple sur la longueur des mots de Σ^* assure que les formules indiquées définissent des applications $b, c, d : \Sigma^* \to \Sigma^*$. On vérifie maintenant que ce sont des bijections. Pour cela, on montre que $b^2 = c^2 = d^2 = \mathrm{id}$. On raisonne par récurrence sur la longueur des mots de Σ^*. Il est clair que $b^2(\varepsilon) = c^2(\varepsilon) = d^2(\varepsilon) = \varepsilon$, où ε désigne le mot vide. Soit $m \in \Sigma^*$ un mot de longueur $n \geq 0$. Alors $b^2(0m) = b(0a(m)) = 0a^2(m) = 0m$, $c^2(0m) = c(0a(m)) = 0a^2(m) = 0m$, $d^2(0m) = d(0m) = 0m$. Et on a, par récurrence sur n, $b^2(1m) = b(1c(m)) = 1c^2(m) = 1m$, $c^2(1m) = c(1d(m)) = 1d^2(m) = 1m$ et $d^2(1m) = d(1b(m)) = 1b^2(m) = 1m$. Donc $b^2 = c^2 = d^2 = \mathrm{id}$. Donc $b, c, d \in G$.

b) On a déjà vu que $a^2 = b^2 = c^2 = d^2 = \mathrm{id}$. Montrons les autres relations par récurrence sur la longueur d'un mot $m \in \Sigma^*$. On a en effet

$$bc(0m) = b(0a(m)) = 0a^2(m) = 0m\,,\ cb(0m) = c(0a(m)) = 0a^2(m) = 0m\,,\ d(0m) = 0m\,,$$

et

$$bc(1m) = b(1d(m)) = 1cd(m) = 1b(m)\,,\ cb(1m) = c(1c(m)) = 1dc(m) = 1b(m)\,,\ d(1m) = 1b(m)\,.$$

De même,

$$cd(0m) = c(0m) = 0a(m)\,,\ dc(0m) = d(0a(m)) = 0a(m)\,,\ b(0m) = 0a(m)\,,$$

et

$$cd(1m) = c(1b(m)) = 1db(m) = 1c(m)\,,\ dc(1m) = d(1d(m)) = 1bd(m) = 1c(m)\,,\ b(1m) = 1c(m)\,.$$

Enfin,

$$bd(0m) = b(0m) = 0a(m)\,,\ db(0m) = d(0a(m)) = 0a(m)\,,\ c(0m) = 0a(m)\,,$$

et

$$bd(1m) = b(1b(m)) = 1cb(m) = 1d(m)\,,\ db(1m) = d(1c(m)) = 1bc(m) = 1d(m)\,,\ c(1m) = 1d(m)\,.$$

On conclut donc que $bc = cb = d$, $cd = dc = b$ et $cd = db = c$.

c) C'est une conséquence simple de la question b), via une récurrence (on peut diminuer la longueur d'une écriture d'un élément de Γ comme produit de a, b, c, d dès que deux éléments consécutifs dans ce produit sont distincts de a).

d) On considère l'application $\psi_n : \Gamma \to \mathrm{Aut}(\Sigma^n)$ définie par $\gamma \mapsto \gamma_{|\Sigma^n}$: celle-ci est bien définie car tout élément de Γ envoie Σ^n dans Σ^n car c'est le cas des générateurs de Γ. En outre, ψ_n est un morphisme de groupes, et $\mathrm{Aut}(\Sigma^n)$ est un groupe fini de cardinal $(2^n)!$. Donc $\Gamma_n = \mathrm{Ker}(\psi_n)$ est un sous-groupe distingué de Γ d'indice divisant $(2^n)!$. Et c'est un sous-groupe strict car $a \notin \Gamma_n$.

e) Vérifions que φ_1 est un morphisme de groupes : soient $\gamma, \gamma' \in \Gamma_1$.
Alors $\varphi_1(\gamma \circ \gamma') = ((\gamma \circ \gamma')_0, (\gamma \circ \gamma')_1)$. Et par définition, on a pour tout $m \in \Sigma^*$ et $x \in \{0;1\}$,

$$(\gamma \circ \gamma')(xm) = \gamma(\gamma'(xm)) = \gamma(x\gamma'_x(m)) = x\gamma_x(\gamma'_x(m))\,,$$

ce qui assure que $(\gamma \circ \gamma')_x(m) = (\gamma_x \circ \gamma'_x)(m)$, donc φ_1 est un morphisme de groupes.
Montrons son injectivité : soit $\gamma \in \mathrm{Ker}(\varphi_1)$. Alors pour tout $m \in \Sigma^*$ et $x \in \{0;1\}$, $\gamma(xm) = x\gamma_x(m) = xm$, donc $\gamma = \mathrm{id}$. Donc φ_1 est injectif.

f) On calcule $\varphi_1(b) = (a, c)$, $\varphi_1(c) = (a, d)$ et $\varphi_1(d) = (\mathrm{id}, b)$, puis $\varphi_1(aba) = (c, a)$, $\varphi_1(aca) = (d, a)$ et $\varphi_1(ada) = (b, \mathrm{id})$. Cela assure immédiatement que φ^0 et φ^1 sont surjectifs. Comme Γ_1 est un sous-groupe strict de Γ, cela assure que Γ est infini.

g) On note B le plus petit sous-groupe distingué de Γ contenant b. Alors on vérifie que $\langle a, d\rangle$ se surjecte sur Γ/B via la projection $\Gamma \to \Gamma/B$. Or il est clair que $\langle a, d\rangle \cong D_4$, donc $[\Gamma : B]$ divise 8.
Pour $\gamma \in \Gamma$, la question précédente assure qu'il existe $g, g' \in \Gamma_1$ tels que $\varphi^0(g) = \varphi^1(g') = \gamma$. Alors un calcul simple assure que $\varphi_1(gadag^{-1}) = (\gamma b \gamma^{-1}, \mathrm{id})$ et $\varphi_1(g'dg'^{-1}) = (\mathrm{id}, \gamma b \gamma^{-1})$. Donc $B \times \{\mathrm{id}\}$ et $\{\mathrm{id}\} \times B$ sont contenus dans $\varphi_1(\Gamma_1)$. Donc $B \times B \subset \varphi_1(\Gamma_1)$. Donc $[\Gamma \times \Gamma : \varphi_1(\Gamma_1)]$ divise $[\Gamma \times \Gamma : B \times B] = [\Gamma : B]^2 = 64$, donc $\varphi_1(\Gamma_1)$ est un sous-groupe d'indice fini (divisant 64) de $\Gamma \times \Gamma$.

h) Les questions d) et g) assurent que Γ et $\Gamma \times \Gamma$ admettent des sous-groupes d'indice fini isomorphes (à Γ_1), donc l'exercice 4, question f) assure que $\beta_\Gamma \sim \beta_{\Gamma\times\Gamma} \sim {\beta_\Gamma}^2$. Supposons alors qu'il existe $k \in \mathbb{N}^*$ (que l'on peut supposer minimal) tel que $\beta_\Gamma(m) \preceq m^k$. Alors on aurait $\beta_\Gamma(m)^2 \sim \beta_\Gamma(m) \preceq m^k$, donc $\beta_\Gamma(m) \preceq m^{\frac{k}{2}}$, donc par minimalité, on aurait $k = 1$ et $\beta_\Gamma(m) \sim m$ (car Γ est infini). Alors $\beta_\Gamma(m) \sim {\beta_\Gamma}^2(m) \sim m^2$, ce qui est contradictoire. Donc Γ n'est pas à croissance polynomiale.

i) Soit $\gamma \in \Gamma_1$. La question c) assure que γ s'écrit sous l'une des quatre formes suivantes (et on peut supposer cette écriture minimale) :

$$\gamma = a * a * \cdots * a * a\,,$$

$$\gamma = a * a * \cdots * a*\,,$$

$$\gamma = *a * \cdots * a * a$$

ou

$$\gamma = *a * \cdots * a*\,,$$

où les symboles $*$ désignent des éléments de l'ensemble $\{b, c, d\}$.
Alors les morphismes φ^ϵ appliqués à ces décompositions s'écrivent explicitement via les règles suivantes (que l'on démontre par récurrence sur la longueur de γ) :

(I) $\varphi^0(\gamma) = \gamma_0$ s'obtient en remplaçant les a par id et en remplaçant chaque symbole $*$ suivant la règle : si $*$ vient après un nombre impair de symboles a, alors $* = b$ est remplacé par a, $* = c$ par a et $* = d$ par id ; si $*$ vient après un nombre pair de symboles a, alors $* = b$ est remplacé par c, $* = c$ par d et $* = d$ par b.

(II) $\varphi^1(\gamma) = \gamma_1$ s'obtient en remplaçant les a par id et en remplaçant chaque symbole $*$ suivant la règle : si $*$ vient après un nombre pair de symboles a, alors $* = b$ est remplacé par a, $* = c$ par a et $* = d$ par id ; si $*$ vient après un nombre impair de symboles a, alors $* = b$ est remplacé par c, $* = c$ par d et $* = d$ par b.

En appliquant ces règles, on voit facilement que dans chacun des quatre types de décomposition mentionnés, on a toujours

$$l(\gamma_0) + l(\gamma_1) \leq l(\gamma) + 1\,.$$

j) Il suffit de considérer l'application $\varphi_n : \Gamma_n \to \Gamma^{\Sigma_n}$ définie de la façon suivante : pour tout $\gamma \in \Gamma_n$, pour tout $\epsilon \in \Sigma^n$, pour tout $m \in \Sigma^*$, $\gamma(\epsilon m)$ est un mot de la forme $\epsilon\gamma_\epsilon(m)$, et on pose alors $\varphi_n(\gamma) = (\gamma_\epsilon)_{\epsilon\in\Sigma^n}$. On adapte alors la preuve de la question g) pour montrer que $\varphi_n(\Gamma_n)$ est d'indice fini dans Γ^{Σ^n}.

k) Il s'agit de raffiner l'argument de la question i). Étant donné $\gamma \in \Gamma_3$, le calcul de $\varphi_3(\gamma) = (\gamma_\epsilon)$ se fait en appliquant, à une écriture minimale de γ, trois fois les règles (I) et (II) énoncées dans la réponse à la question i). À chaque application de l'une de ces règles, on constate que la longueur de γ est diminuée de $l_d(\gamma) - 1$, où $l_d(\gamma)$ est le nombre de symboles d dans l'écriture de γ considérée ; et en outre, chaque lettre c de γ produit une lettre d après application de la règle (I) ou (II), laquelle lettre sera supprimée à l'application suivante d'une des deux règles. Et chaque lettre b de γ fournit une lettre c après la première application d'une des deux règles, laquelle lettre c fournit une lettre d à la deuxième application, laquelle lettre d disparaît à la troisième application. Or l'une des lettre b, c, d apparaît strictement plus que $\frac{l(\gamma)}{6} - 1$ fois dans l'écriture de γ, donc la conjonction de la question i) avec les remarques précédentes aboutit à l'estimation souhaitée :

$$\sum_{\epsilon\in\Sigma_3} l(\gamma_\epsilon) \leq \frac{5}{6} l(\gamma) + 8\,.$$

l) On a donc montré que pour tout $\gamma \in \Gamma_3$, on a

$$\sum_{\epsilon\in\Sigma_3} l(\gamma_\epsilon) \leq \frac{5}{6} l(\gamma) + 8\,.$$

Cela implique que

$$\beta_{\Gamma_3}(m) \leq \sum_{\substack{(n_1,\ldots,n_8)\in\mathbb{N}^8 \\ \sum_i n_i \leq \frac{5}{6}m+8}} \beta_\Gamma(n_1)\ldots\beta_\Gamma(n_8)\,.$$

On pose alors $\lambda := \lim_{n\to+\infty} \sqrt[n]{\beta_\Gamma(n)}$ (on vérifiera que cette limite existe). Supposant $\lambda > 1$, l'inégalité précédente implique après quelques calculs que $\lambda \leq \lambda^{\frac{5}{6}}$, ce qui est contradictoire. Donc $\lambda \leq 1$, ce qui assure que $\beta_\Gamma(n) \prec e^n$.