Agrégation interne 2004

Corrigé de la première épreuve

Partie I : parties dédoublables de C=R^2

A.1.(a) Comme x et y sont éléments de $\overline{D}$, on peut écrire :

$$2 = |x - y| \leq |x| + |y| \leq 1 + 1 = 2.$$

Ces deux inégalités sont donc des égalités : la première impose à x et y d'être positivement liés (cas d'égalité de l'inégalité de Minkowski) et la seconde donne $|x| = |y| = 1$. Les complexes x et y sont donc deux éléments diamétralement opposés du cercle unité et admettent 0 pour milieu.

A.1.(b) Supposons que w n'est pas élément de A, i.e. qu'il est élément de B. Il existe alors v dans A tel que $w = \tau(v)$. Comme τ est une isométrie, nous obtenons

$$|v| = |v - 0| = |\tau(w) - \tau(0)| = |w - \tau(0)| > 1$$

ce qui est absurde : le complexe w est donc élément de A.

A.1.(c) $x = \tau(0)$ étant un complexe non nul, nous pouvons poser $u = i\,\dfrac{\tau(0)}{|\tau(0)|}$ et $v = -u$. Comme $|u| = 1$, $[u, v]$ est un diamètre de $\overline{D}$; d'autre part, $|u - \tau(0)| = |v - \tau(0)| = \sqrt{1 + |\tau(0)|^2} > 1$, donc u et v sont éléments de A d'après le (b).

A.1.(d) Les points $x = \tau(u)$ et $y = \tau(v)$ appartiennent à $\overline{D}$ et vérifient $|x - y| = |u - v| = 2$; d'après le (a), 0 est le milieu du segment $[x, y]$. Comme τ est affine, $0 = \dfrac{\tau(u) + \tau(v)}{2} = \tau\left(\dfrac{u + v}{2}\right) = \tau(0)$, ce qui est absurde car $0 \in A$ et $\tau(0) \notin A$.

A.2. Supposons que $\overline{D}$ est $\mathfrak{I}_2$-dédoublable. Il existe alors deux parties A_1 et A_2 et deux isométries g_1 et g_2 vérifiant :

- $\overline{D} = A_1 \amalg A_2$;
- $g_1(\overline{D}) = A_1$ et $g_2(\overline{D}) = A_2$.

Quitte à échanger A_1 et A_2, on peut supposer que $0 \in A_1$. En posant $A = A_1$, $B = A_2$ et $\tau = g_2 \circ q_1^{-1}$, nous sommes dans la situation de la question 1, ce qui est absurde : $\overline{D}$ n'est pas $\mathfrak{I}_2$-dédoublable.

B 1.1.(a) La partie R est non vide (car $\mathcal{B}$ est non vide bornée) et minorée par 0 : elle admet donc une borne inférieure.

B 1.1.(b) Pour n entier naturel non nul, $\rho + 1/n$ n'est pas un minorant de R : il existe donc un élément r de R tel que $r < \rho + 1/n$. Par définition de r, il existe ensuite un élément de **C**, que nous pouvons noter x_n, tel que $\mathcal{B} \subset \overline{D}\left(x_n, \rho + \dfrac{1}{n}\right)$.

B 1.2.(a) Si a_0 est un élément fixé de $\mathcal{B}$, la suite (x_n) est contenue dans $\overline{D}(a_0, \rho + 1)$: cette partie est fermée bornée, donc compacte (**C** est un espace vectoriel normé de dimension finie). On en déduit donc que la suite (x_n) possède une valeur d'adhérence.

B 1.2.(b) Il existe donc une application $\varphi : \mathbf{N}^* \to \mathbf{N}^*$ strictement croissante et $a \in \mathbf{C}$ tels que $x_{\varphi(n)} \xrightarrow[n\to+\infty]{} a$. Pour chaque x de $\mathcal{B}$, nous pouvons alors écrire :

$$\forall\, n \in \mathbf{N}^*,\ |x - x_{\varphi(n)}| \leq \rho + \frac{1}{\varphi(n)}$$

ce qui donne $|x-a| \leq \rho$ en faisant tendre n vers l'infini : nous avons donc démontré que $\mathcal{B}$ est inclus dans $\overline{D}(a,\rho)$.

B 1.2.(c) Supposons qu'il existe deux valeurs distinctes a_1 et a_2 telles que $\mathcal{B}$ soit contenu à la fois dans $\overline{D}(a_1,\rho)$ et $\overline{D}(a_2,\rho)$.On pose alors $x = \dfrac{a_1+a_2}{2}$ et $r = \sqrt{\rho^2 - \dfrac{|a_2-a_1|^2}{4}}$. Nous avons alors :

$$\mathcal{B} \subset \overline{D}(a_1,\rho) \cap \overline{D}(a_2,\rho) \subset \overline{D}(x,r),$$

ce qui traduit que $r \in R$. Comme $r < \rho$, ceci est absurde : l'élément a est bien unique.

B 2.1. Les isométries du plan affine euclidien sont :

- l'application identité ;
- les rotations d'angle non nul ;
- les translations de vecteur non nul ;
- les réflexions ;
- les composées d'une réflexion d'axe D et d'une translation de vecteur non nul colinéaire à D.

B 2.2.(a) Étudions les différents cas :

- si τ_i est l'application identité, $\mathcal{B} = \mathcal{B}_i$: c'est absurde ;
- si τ_i est une translation de vecteur non nul $\vec{u}$, en fixant un point a_0 de $\mathcal{B}$, nous obtenons une suite $(a_0 + n\vec{u})_{n\in\mathbf{N}}$ d'éléments de $\mathcal{B}$: c'est une nouvelle fois absurde car $\mathcal{B}$ est supposée bornée ;
- si τ_i est une réflexion, τ_i est involutive, ce qui donne $\tau_i(\mathcal{B}) = \mathcal{B}_i \subset \mathcal{B}$, puis $\tau_i\left(\tau_i(\mathcal{B})\right) \subset \tau_i(\mathcal{B})$, i.e. $\mathcal{B} \subset \mathcal{B}_i$: c'est absurde.
- enfin, si τ_i est la composée d'une réflexion d'axe D et d'une translation de vecteur $\vec{u}$ non nul colinéaire à D, la suite $(a_0 + 2n\vec{u})_{n\in\mathbf{N}}$ est une nouvelle fois une suite non bornée d'éléments de $\mathcal{B}$.

Il reste donc un unique cas possible : τ_i est une rotation d'angle non nul.

B 2.2.(b) On considère l'unique disque $\overline{D}(a,\rho)$ de rayon minimal contenant $\mathcal{B}$. Comme $\mathcal{B}_i$ est contenu dans $\mathcal{B}$, et donc dans $\overline{D}(a,\rho)$, nous obtenons :

$$\mathcal{B} = \tau_i^{-1}(\mathcal{B}_i) \subset \tau_i^{-1}\left(\overline{D}(a,\rho)\right) = \overline{D}(\tau_i^{-1}(a),\rho)$$

puisque l'image d'un disque de centre a par une isométrie g est un disque de même rayon et de centre $g(a)$. Par unicité de a (question 2.(c)), nous obtenons $\tau_i^{-1}(a) = a$, i.e. $\tau_i(a) = a$. Le seul point fixe d'une rotation d'angle non nul étant son centre, ceci donne bien $\omega_1 = a = \omega_2$.

B 2.2.(c) En partant de l'inclusion $\tau_2(\mathcal{B}) = \mathcal{B}_2 \subset \mathcal{B}$ et en appliquant τ_1, nous obtenons :

$$\tau_1\left(\tau_2(\mathcal{B})\right) \subset \tau_1(\mathcal{B}) = \mathcal{B}_2.$$

Comme τ_1 et τ_2 sont des rotations de même centre, elles commutent : on a donc par symétrie

$$\tau_1(\tau_2(\mathcal{B})) \subset \tau_2(\mathcal{B}) = \mathcal{B}_1,$$

ce qui donne l'inclusion demandée.

Cette inclusion est alors impossible, puisque $\tau_1(\tau_2(\mathcal{B}))$ est non vide ($\mathcal{B}$ est non vide) alors que $\mathcal{B}_1 \cap \mathcal{B}_2$ est vide !

Nous avons donc démontré par l'absurde qu'aucune partie (non vide) bornée de $\mathbf{C}$ n'est $\mathfrak{I}_2$-dédoublable.

Partie II : le paradoxe de Sierpinski-Mazurkiewicz [1914]

1. Supposons qu'il existe un élément y commun à $t(\mathcal{D})$ et $r(\mathcal{D})$. Il existe alors deux polynômes P et Q à coefficients dans $\mathbf{N}$ tels que $P(u) + 1 = y = uQ(u)$. On en déduit que le polynôme $XQ - P - 1$ admet u pour racine : comme il est à coefficients entiers et que u est transcendant, ce polynôme est nul, ce qui donne $XQ = P + 1$, et donc $P(0) = -1$: cette égalité est absurde puisque P est à coefficients dans $\mathbf{N}$.

Nous avons donc montré par l'absurde que $t(\mathcal{D}) \cap r(\mathcal{D}) = \emptyset$.

2. Notons $\mathcal{D}_1 = t(\mathcal{D})$ et $\mathcal{D}_2 = r(\mathcal{D})$. Nous avons :

- $\mathcal{D}_1 \cap \mathcal{D}_2 = \emptyset$;
- soit $x \in \mathcal{D}$ avec $x = P(u)$ où $P \in \mathcal{P}_\mathbf{N}$. Deux cas sont alors possibles :
  - Si X divise P, on peut écrire $P = XQ$ avec $Q \in \mathcal{P}_\mathbf{N}$, ce qui donne $x = r(y)$ avec $y = Q(u) \in \mathcal{D}$: x est élément de $\mathcal{D}_2$.
  - Sinon, $P(0)$ est un entier naturel non nul, donc $P(0) \geq 1$ et on peut écrire $P = 1+Q$ avec $Q \in \mathcal{P}_\mathbf{N}$, ce qui donne $x = t(y)$ avec $y = Q(u) \in \mathcal{D}$: x est élément de $\mathcal{D}_1$.

  Nous avons donc $\mathcal{D} = \mathcal{D}_1 \amalg \mathcal{D}_2$.
- comme r et s sont des isométries (u est de module 1), nous avons démontré que $\mathcal{D}$ était $\mathfrak{I}_2$-dédoublable.

Le paradoxe de Sierpinski-Mazurkiewicz est donc établi : il existe une partie (non bornée) de $\mathbf{C}$ et $\mathfrak{I}_2$-dédoublable.

Partie III : parties dédoublables de R

A.1. Pour $p, q \geq 1$, considérons l'application $\varphi : \begin{array}{ccc} B_S(p) \times B_S(q) & \longrightarrow & G \\ (x,y) & \longmapsto & xy \end{array}$.

L'image de φ est égale à $B_S(p+q)$:

- si $(x,y) \in B_S(p) \times B_S(q)$, on peut écrire $x = s_1 \dots s_k$ et $y = s_{k+1} \dots s_{k+n}$ avec $0 \leq k \leq p$, $0 \leq n \leq q$ et $s_1, \dots, s_{k+n} \in S$, ce qui donne $xy = s_1 \dots s_{k+n} \in B_S(p+q)$;
- si $z \in B_S(p+q)$, z s'écrit $z = s_1 \dots s_k$ avec $0 \leq k \leq p+q$ et $s_1, \dots, s_k \in S$. Si $k \leq p$, on pose $x = z \in B_S(p)$ et $y = 1 \in B_S(q)$; sinon, on pose $x = s_1 \dots s_p \in B_S(p)$ et $y = s_{p+1} \dots s_k \in B_S(q)$. Dans les deux cas, on obtient $z = \varphi((x,y))$.

On en déduit donc que le cardinal de $B_S(p+q)$ est au plus égal à celui de $B_S(p) \times B_S(q)$, ce qui donne l'inégalité demandée.

A.2.(a) L'inégalité précédente donne successivement :

- $\forall\, p, q \geq 1,\ u_{p+q} \leq u_p + u_q$;
- $\forall\, p, q \geq 1,\ u_{pq} \leq q u_p$;
- $\forall\, q \geq 1,\ u_q \leq q u_1$.

Si n et p sont des entiers naturels non nul, effectuons la division euclidienne de n par p : $n = pq + r$ avec $0 \leq r \leq p-1$. Nous avons alors, dans le cas où r est non nul :

$$v_n = \frac{u_{pq+r}}{n} \leq \frac{u_{pq} + u_r}{n} \leq \frac{q u_p + r u_1}{n} \leq \frac{qp}{n}\, v_p + \frac{r}{n}\, v_1 \leq v_p + \frac{p}{n}\, v_1.$$

Si $r = 0$, nous obtenons :

$$v_n = \frac{u_{pq}}{n} \leq \frac{q u_p}{n} \leq \frac{qp}{n}\, v_p \leq v_p \leq v_p + \frac{p}{n}\, v_1$$

en remarquant que $v_1 \geq 0$.

A.2.(b) En choisissant $p = 1$ dans l'inégalité précédente, nous obtenons la majoration :

$$\forall\, n \geq 1,\ v_n \leq v_1 \left(1 + \frac{1}{n}\right) \leq 2\, v_1.$$

La suite $(v_n)_{n \geq 1}$ est donc bornée (elle est positive et majorée). Pour montrer qu'elle converge, il suffit donc de montrer qu'elle possède une unique valeur d'adhérence (propriété des suites dans une partie compacte). Soit donc λ une valeur d'adhérence, limite de la sous-suite $(v_{\varphi(n)})_{n \geq 1}$. Pour tout $p \geq 1$, nous avons alors :

$$\forall\, n \geq 1,\ v_{\varphi(n)} \leq v_p + \frac{p}{\varphi(n)}\, v_1$$

ce qui donne $\lambda \leq v_p$ en faisant tendre n vers l'infini. Ainsi, λ minore la suite $(v_n)_{n \geq 1}$, et ne peut donc être que le plus petit des minorant. On en déduit que la seule valeur d'adhérence de la suite est $v = \inf_{n \geq 1} v_n$, ce qui prouve la convergence de v_n vers v quand n tend vers l'infini.

A.3. Comme $c_S(n) = \mathrm{e}^{v_n}$, la suite $c_S(n)$ converge quand n tend vers l'infini vers $C_S = \mathrm{e}^{v}$ avec $C_S \geq 1$ puisque $v \geq 0$ (les v_n sont positifs car les parties $B_S(n)$ contiennent toutes 1).

A.4. Si G contient un sous-groupe H à croissance exponentielle, il est évident que G est également à croissance exponentielle (pour S, partie finie symétrique de $H \setminus \{1\}$, le calcul de C_S ne dépend pas du groupe dans lequel S est plongé).

A.5. Soit G un groupe abélien et $S = \{s_1, s_2, \ldots, s_p\}$ une partie finie symétrique de $G \setminus \{1\}$. Pour $n \geq 1$, tout élément x de $B_S(n)$ peut s'écrire (en utilisant la commutativité de G) sous la forme

$$x = s_1^{i_1} s_2^{i_2} \ldots s_p^{i_p}$$

avec $i_1, \ldots, i_p \in \mathbf{N}$ et $i_1 + \cdots + i_p \leq n$. L'ensemble $B_S(n)$ est donc contenu dans l'image de l'application

$$\begin{array}{ccc} \{0, 1, \ldots, n\}^p & \longrightarrow & G \\ (i_1, i_2, \ldots, i_p) & \longmapsto & s_1^{i_1} s_2^{i_2} \ldots s_p^{i_p} \end{array}$$

On en déduit que $\gamma_S(n)$ est majoré par $(n+1)^p$, ce qui donne :

$$1 \leq c_s(n) \leq (n+1)^{p/n} = \exp\left(p\,\frac{\ln(n+1)}{n}\right) \xrightarrow[n\to+\infty]{} 1.$$

Un groupe abélien est donc à croissance sous-exponentielle.

B.1. Soit f un élément de $\mathfrak{I}_1$; f est affine, donc il existe des réels u et v tels que $f : x \to ux+v$. Comme f est une isométrie, $|u| = |f(1)-f(0)| = |1-0| = 1$, et donc $u = \pm 1$.

Réciproquement, une application $f : x \to ux+v$ avec $v \in \mathbf{R}$ et $u = \pm 1$ est affine et conserve la distance, puisque $|f(x)-f(y)| = |u(x-y)| = |x-y|$.

B.2. Unicité : supposons que (ε', t) existe. En posant $f = \varepsilon \circ s$, deux cas peuvent être distingués :

- si f est indirecte, $\varepsilon' \in \mathfrak{I}_1^-$, soit $\varepsilon' = -Id$, puis $t = -f$;
- si f est directe, $\varepsilon \in \mathfrak{I}_1^+$, soit $\varepsilon' = -Id$, puis $t = f$.

Ceci prouve donc l'unicité du couple (ε', t).

Existence : nous pouvons poser $\varepsilon' = Id$ ou $\varepsilon' = -Id$ selon que $\varepsilon \circ s$ est directe ou indirecte, puis $t = \varepsilon \circ s \circ \varepsilon'$. On a clairement $t \in \mathfrak{I}_1^+$ et $\varepsilon \circ s = t \circ \varepsilon'$, ce qui prouve l'existence du couple (ε', t).

B.3. Soit $\tau \in B_S(n)$. Nous pouvons donc écrire $\tau = s_1 \circ \ldots \circ s_k$ avec $0 \leq k \leq n$ et $s_1, \ldots, s_k \in S$. Une récurrence immédiate permet de construire une suite $(t_1, \ldots, t_k)$ d'éléments de T_0 et une suite $(\varepsilon_1, \ldots, \varepsilon_k)$ à valeur dans $\{\pm Id\}$ telle que :

$$\forall\, i \in \{1, \ldots, k\},\ s_1 \circ \ldots \circ s_i = t_1 \circ \ldots \circ t_i \circ \varepsilon_i,$$

en appliquant successivement le résultat précédent aux éléments $Id \circ s_1$, $\varepsilon_1 \circ s_2$,..., $\varepsilon_{k-1} \circ s_k$. Nous obtenons $\tau = \sigma \circ \varepsilon$ avec $\sigma = t_1 \circ \ldots \circ t_k \in B_T(n)$ et $\varepsilon = \varepsilon_k \in \{\pm Id\}$.

B.4. L'application

$$\begin{array}{rccc} \varphi : & B_T(n) \times \{\pm Id\} & \longrightarrow & \mathfrak{I}_1 \\ & (\sigma, \varepsilon) & \longmapsto & \sigma \circ \varepsilon \end{array}$$

est injective (si deux éléments (t_1, ε_1) et (t_2, ε_2) ont même image, on obtient $\varepsilon_1 = \varepsilon_2$ car t_1 et t_2 sont des isométries directes, puis $t_1 = t_2$) et l'image de φ contient $B_S(n)$. On en déduit donc :

$$\gamma_S(n) \leq \ \mathrm{Card}\ (\mathrm{Im}(\varphi)) = 2\,\gamma_T(n),$$

ce qui donne $c_S(n) \leq 2^{1/n}\, c_T(n)$ puis $C_S \leq C_T$ par passage à la limite. Comme T est contenu dans le groupe abélien $\mathfrak{I}_1^+$, qui est à croissance sous-exponentielle d'après le A.5, C_T est égal à 1, ce qui achève la preuve : $C_S = 1$ pour toute partie finie non vide de $\mathfrak{I}_1$ et le groupe $\mathfrak{I}_1$ est à croissance sous-exponentielle.

C.1. Notons k le plus petit entier i tel que $s_i \neq s_i'$. Par symétrie, on peut supposer que $s_k = \tau_1$ et $s_k' = \tau_2$. Nous avons alors $s_k \circ \ldots \circ s_n(\mathcal{D}) \subset s_k(D) = \tau_1(\mathcal{D}) = \mathcal{D}_1$ et $s_k' \circ \ldots \circ s_n'(\mathcal{D}) \subset s_k'(D) = \tau_2(\mathcal{D}) = \mathcal{D}_2$. En notant $\sigma = s_1 \circ \ldots s_{k-1} = s_1' \circ \ldots s_{k-1}'$, nous avons alors $\gamma_s(\mathcal{D}) \subset \sigma(\mathcal{D}_1)$ et $\gamma_{s'}(\mathcal{D}) \subset \sigma(\mathcal{D}_2)$. Comme $\mathcal{D}_1$ et $\mathcal{D}_2$ sont disjoints, la bijectivité de σ prouve que $\sigma(\mathcal{D}_1)$ et $\sigma(\mathcal{D}_2)$ sont disjoints : les parties $\gamma_s(\mathcal{D})$ et $\gamma_{s'}(\mathcal{D})$ sont donc disjointes.

C.2. On déduit de la question précédente que l'application $\begin{array}{ccc} \{\tau_1, \tau_2\}^n & \longrightarrow & B_S(n) \\ s & \longmapsto & \gamma_s \end{array}$ est injective. Ceci prouve que le cardinal de $B_S(n)$ est au moins égal à 2^n, i.e. que $c_S(n) \geq 2$. En passant à limite quand n tend vers l'infini, on obtient la minoration : $C_S \geq 2$.

C.3. Nous venons donc de démontrer que l'existence d'une partie de $\mathbf{R}$ $\mathfrak{I}_1$-dédoublable implique l'existence d'une partie finie symétrique S de $\mathfrak{I}_1$ telle que $C_S \geq 2$, ce qui contredit la croissance sous-exponentielle du groupe $\mathfrak{I}_1$: aucune partie de $\mathbf{R}$ n'est $\mathfrak{I}_1$-dédoublable.

D. Considérons la partie $S = \{t, t^{-1}, r, r^{-1}\}$ où r et t sont les éléments de $\mathfrak{I}_2$ définis dans la partie II. En reprenant exactement la preuve de la partie **C.**, on montre que l'application

$$\begin{array}{ccc} \{r,t\}^n & \longrightarrow & B_S(n) \\ (s_1,\ldots,s_n) & \longmapsto & s_1 \circ \ldots \circ s_n \end{array}$$

est injective, ce qui donne ensuite $C_S \geq 2$: $\mathfrak{I}_2$ est à croissance exponentielle.

Partie IV : un groupe “paradoxal”

A.1. En notant N la matrice nilpotente $N = A - I$, les matrices N et I commutent et nous pouvons utiliser la formule du binôme de Newton :

$$\forall\, k \in \mathbf{N},\ A^k = (I+N)^k = \sum_{i=0}^{k} \begin{pmatrix} k \\ i \end{pmatrix} N^i = I + kN = \begin{pmatrix} 1 & 2k \\ 0 & 1 \end{pmatrix}.$$

En remarquant ensuite que $A^{-1} = I - N$, nous obtenons de la même façon :

$$\forall\, k \in \mathbf{N}^*,\ A^{-k} = (I-N)^k = \sum_{i=0}^{k} \begin{pmatrix} k \\ i \end{pmatrix} (-1)^k N^i = I - kN = \begin{pmatrix} 1 & -2k \\ 0 & 1 \end{pmatrix}.$$

Nous avons donc :

$$\forall\, k \in \mathbf{Z},\ A^k = \begin{pmatrix} 1 & 2k \\ 0 & 1 \end{pmatrix} \text{ et } B^k = ({}^tA)^k = {}^t(A^k) = \begin{pmatrix} 1 & 0 \\ 2k & 1 \end{pmatrix}.$$

A.2. Soit $M = A^k$ avec $k \in \mathbf{Z}^*$ et $X_2 = \begin{pmatrix} x \\ y \end{pmatrix} \in E_2$. Alors :

$$MX_2 = \begin{pmatrix} x + 2ky \\ y \end{pmatrix}$$

Quitte à y en $-y$ et k en $-k$, nous pouvons supposer que $y \geq 0$. Comme $-y < x < y$, nous avons $(2k-1)y < x + 2ky < (2k+1)y$. Nous pouvons ensuite distinguer deux cas :

- si $k \geq 1$, $0 \leq y \leq (2k-1)y < x + 2ky$;
- si $k \leq -1$, $x + 2ky < (2k+1)y \leq -y \leq 0$;

Ainsi, dans tous les cas, $|x + 2ky| > |y|$ et $MX_2 \in E_1$.

La seconde propriété est exactement équivalente à la première, en échangeant les rôles de x et y.

B.1. Soit U un élément de Γ. Il existe alors k dans $\mathbf{N}$ et $i_1, j_1, i_2, j_2, \ldots, i_k, j_k$ dans $\mathbf{Z}$ tels que :

- $U = B^{i_1}A^{j_1}B^{i_2}A^{j_2}\ldots B^{i_k}A^{j_k}$;
- si $k \neq 0$, $j_1, i_2, \ldots, j_{k-1}, i_k$ sont non nuls.

Nous sommes alors dans l'un des cas suivants :

- $k=0$: $U=I$ (cas **(0)**) ;
- $k=1$, $i_1=j_1=0$: $U=I$ (cas **(0)**) ;
- $k=1$, $i_1\neq 0$ et $j_1=0$: $U=B^{i_1}=P_0$ (cas **(1)**) ;
- $k=1$, $i_1=0$ et $j_1\neq 0$: $U=A^{j_1}=M_0$ (cas **(2)**) ;
- $k=1$, $i_1\neq 0$ et $j_1\neq 0$: $U=B^{i_1}A^{j_1}=P_0M_0$ (cas **(3)**) ;
- $k\geq 2$, $i_1=0$ et $j_k=0$: $U=(A^{j_1}B^{i_2})(A^{j_2}B^{i_3})\dots(A^{j_{k-1}}B^{i_k})$ (cas **(4)** avec $n=k-1$) ;
- $k\geq 2$, $i_1\neq 0$ et $j_k=0$: $U=B^{i_1}(A^{j_1}B^{i_2})(A^{j_2}B^{i_3})\dots(A^{j_{k-1}}B^{i_k})$ (cas **(5)** avec $r=k-1$) ;
- $k\geq 2$, $i_1=0$ et $j_k\neq 0$: $U=(A^{j_1}B^{i_2})(A^{j_2}B^{i_3})\dots(A^{j_{k-1}}B^{i_k})A^{j_k}$ (cas **(6)** avec $s=k-1$) ;
- $k\geq 2$, $i_1\neq 0$ et $j_k\neq 0$: $U=B^{i_1}(A^{j_1}B^{i_2})(A^{j_2}B^{i_3})\dots(A^{j_{k-1}}B^{i_k})A^{j_k}$ (cas **(7)** avec $t=k-1$) ;

B.2.(a) Si U_3 était égale à I, on aurait $P_0=M_0^{-1}$. Comme $M_0\in\Gamma_1\setminus\{I\}$, son inverse est également dans $\Gamma\setminus\{I\}$, ce qui donne $P_0\in(\Gamma_1\cap\Gamma_2)\setminus\{I\}=\emptyset$! Nous avons donc montré par l'absurde que $U_3\neq I$.

B.2.(b) En choisissant X_2 dans E_2 (cE_2 est non vide), nous avons : $U_6X_2=\Pi_sM_{s+1}X_2=M_1P_1\dots M_sP_sM_{s+1}X_2$. D'après le **A.2.**, $M_{s+1}X_2\in E_1$, puis $P_sM_{s+1}X_2\in E_2$, et ainsi de suite jusqu'à $M_1P_1\dots M_sP_sM_{s+1}X_2\in E_1$. On en déduit donc que $U_6X_2\neq X_2$, puisque $E_1\cap E_2=\emptyset$, ce qui donne $U_6\neq I$.

B.2.(c) La matrice AU_5A^{-1} est de la forme (**6**) : on en déduit donc d'après le **(b)** que $AU_5A^{-1}\neq I$, ce qui donne $U_5\neq I$.

De même, en posant $U_4=M_1P_1\dots M_nP_n$, on peut choisir $M\in\Gamma_1$ tel que $M\notin\{M_1,I\}$. La matrice $M^{-1}U_4M$ est alors de la forme **(6)**, puisque $M^{-1}M_1$ et M sont éléments de $\Gamma_1\setminus\{I\}$. On déduit encore du **(b)** que $M^{-1}U_4M\neq I$, puis que $U_4\neq I$.

B.2.(d) Si $U_7=I$, $M_{t+1}P_0\Pi_t=M_{t+1}IM_{t+1}^{-1}=I$, ce qui est absurde car $M_{t+1}P_0\Pi_t$ est de type **(4)**.

B.3.(a) Comme $\Pi'_n\Pi_n^{-1}$ est égale à l'identité, il n'est pas possible de la décomposer sous l'une des formes **(1)** à **(7)** (seules les formes **(2)** et **(3)** n'ont pas été étudiées à la question **2.**, mais $U_1\neq I$ et $U_2\neq I$ par définition). Comme :

$$\Pi'_n\Pi_n^{-1}=M'_1P'_1\dots M'_n(P'_nP_n^{-1})M_n^{-1}P_{n-1}^{-1}M_{n-1}^{-1}\dots P_1^{-1}M_1^{-1},$$

si $P'_nP_n^{-1}$ n'était pas égale à I, cette matrice serait de type **(6)**. On en déduit donc que $P'_n=P_n$, puis :

$$\Pi'_n\Pi_n^{-1}=M'_1P'_1\dots M'_{n-1}P'_{n-1}(M'_nM_n^{-1})P_{n-1}^{-1}M_{n-1}^{-1}\dots P_1^{-1}M_1^{-1},$$

ce qui donne $M'_n=M_n$ (sinon, la matrice serait de type **(6)**). Par récurrence, on obtient ainsi $P_i=P'_i$ et $M_i=M'_i$ pour tout i, $1\leq i\leq n$.

B.3.(b) D'après la question précédente, l'application :

$$\begin{array}{ccc} (\{A,-A\}\times\{B,-B\})^n & \longrightarrow & B_S(2n) \\ (M_i,P_i)_{1\leq i\leq n} & \longmapsto & (M_1P_1)(M_2P_2)\dots(M_nP_n) \end{array}$$

est injective. On en déduit donc que $2^{2n}\leq\gamma_S(2n)$, puis que $2\leq c_S(2n)$: ainsi, $C_S\geq 2$ et le groupe Γ est à croissance exponentielle.

La question **III.A.4.** permet ensuite d'affirmer que $SL_2(\mathbf{Z})$ est également à croissance exponentielle.

C.1. Si U est du type **(4)** (resp. **(7)**), k étant non nul, U^k est également du type **(4)**(resp. **(7)**) et ne peut donc pas être égal à I.

Si U est du type **(3)**, U^k est de type **(7)** et c'est une nouvelle fois impossible.

Les éléments d'ordre fini de Γ ne peuvent donc pas être de type **(3)**, **(4)** ou **(7)**.

C.2.(a) $V_1 = (M_{s+1}M_1P_1)(M_2P_2)\dots(M_sP_s)$ donc si $M_{s+1}M_1 \neq I$, V_1 est de type **(4)**, ce qui est incompatible avec la propriété $V_1^k = M_{s+1}U^kM_{s+1}^{-1} = I$. On en déduit donc que $M_{s+1}M_1 = I$.

On obtient ensuite $V_2 = (M_2P_2)\dots(M_sP_sP_1)$. Comme $V_2^k = I$, V_2 n'est pas de type **(4)** et donc $P_sP_1 = I$

C.2.(b) Supposons qu'il existe une matrice de type **(6)** d'ordre fini, et choisissons une telle matrice $U = \Pi_s M_{s+1}$ avec s minimal. D'après le **(a)**, cette matrice U est alors semblable à la matrice $V_2 = (M_2P_2)\dots(M_{s-1}P_{s-1})M_s$. Comme V_2 est d'ordre fini, elle n'est pas de type **(6)** (par minimalité de s). On en déduit donc que $s = 1$, i.e. que V_2 est de type **(2)**, ce qui est absurde car le seul élément de Γ_1 d'ordre fini est I.

C.3. Si U était de type **(5)**, avec $U = P_0(M_1P_1)\dots(M_rP_r)$, on pourrait poser :

$$V = AUA^{-1} = (AP_0)(M_1P_1)\dots(M_rP_r)A^{-1}.$$

V serait alors un élément d'ordre fini de type **(6)**, ce qui serait absurde d'après la question précédente.

C.4. U ne peut pas être de type **(3)**, **(4)**, **(5)**, **(6)** ou **(7)**. Comme le seul élément de Γ_1 ou de Γ_2 d'ordre fini est I (Γ_1 et Γ_2 sont isomorphes à $(\mathbf{Z}, +)$ car A et B sont d'ordre infini), seul le type **(1)** reste possible : $U = I$.

D. Chaque élément de Γ admet une écriture "canonique" unique (on peut parler de *forme normale*), de l'une des formes **(0)** à **(7)**. Soient alors les quatre parties disjointes :

- $\mathcal{Q}_1$ est constitué des U de Γ dont la forme normale commence par A ;
- $\mathcal{Q}_2$ est constitué des U de Γ dont la forme normale commence par A^{-1} ;
- $\mathcal{R}_1$ est constitué des U de Γ dont la forme normale commence par B ;
- $\mathcal{R}_2$ est constitué des U de Γ dont la forme normale commence par B^{-1}.

Pour être plus précis, nous pourrions définir $\mathcal{Q}_1$ comme l'ensemble des U relevant de l'un des trois cas suivants :

- U est de type **(2)** avec $M_0 \in \{A^k,\ k \geq 1\}$;
- U est de type **(4)** avec $M_1 \in \{A^k,\ k \geq 1\}$;
- U est de type **(6)** avec $M_1 \in \{A^k,\ k \geq 1\}$.

et donner des définitions symétriques pour $\mathcal{Q}_2$, $\mathcal{R}_1$ et $\mathcal{R}_2$. A et B jouant des rôles symétriques, il suffit de montrer que $\Gamma = \mathcal{Q}_1 \cup \mathcal{Q}_2$. Soit donc $U \in \Gamma$. Étudions les différents cas possibles :

- si la forme normale de U commence par un A, U est élément de $\mathcal{Q}_1$;
- si la forme normale de U ne commence pas par un A, la forme normale de $A^{-1}U$ commencera dans tous les cas par un A^{-1} (on ne pourra pas simplifier le premier A^{-1} puisque la forme normale de U ne commence pas par un A). On en déduit que $U = A\underbrace{(A^{-1}U)}_{\in \mathcal{Q}_2} \in A\mathcal{Q}_2$,

ce qui achève de démontrer que $\mathcal{Q} = \mathcal{Q}_1 \cup \mathcal{Q}_2$, l'inclusion inverse étant évidente.

Remarque : cette partie **IV** donne une construction du groupe libre à deux générateurs. Ce groupe est le groupe "le plus général" engendré par deux éléments a et b, i.e. le groupe engendré par a et b tel qu'il n'existe aucune relation entre a, b, a^{-1} et b^{-1} autres que celles imposées par la structure de groupe (comme par exemple $abb^{-1}aa^{-1}ba^{-1} = aba^{-1}$). De façon rigoureuse, ce groupe est l'unique solution G (à isomorphisme près) du problème universel :

- G est un groupe engendré par les éléments a et b ;
- pour tout groupe H et pour tout couple (x, y) d'éléments de H, il existe un et un seul morphisme de groupe $\varphi : G \to H$ tel que $\varphi(a) = x$ et $\varphi(b) = y$.

Cette définition est à rapprocher de celle de *monoïde libre* sur l'alphabet $\{a, b\}$. On peut également remarquer que le groupe libre G est *librement engendré* par a et b, de la même façon qu'une base engendre librement un espace vectoriel.

Partie IV : ensembles G-paradoxaux

A.1. Il suffit de faire agir Γ sur lui-même par *translation à gauche* : $\forall\, M, N \in \Gamma,\ M \star N = MN$. En reprenant les notations de la partie **IV.D.**, les éléments :

$$m = n = 2,\ \mathcal{Q} = \mathcal{Q}_1 \amalg \mathcal{Q}_2,\ \mathcal{R} = \mathcal{R}_1 \amalg \mathcal{R}_2,\ g_1 = I,\ g_2 = A,\ h_1 = I \text{ et } h_2 = B$$

prouvent que Γ est Γ-paradoxal.

A.2. Considérons l'action naturelle de G sur E :

$$\forall\, (g, x) \in G \times E,\ g \star x = g(x).$$

Soit $\mathcal{P}$ une partie G-dédoublable de E, avec

$$\mathcal{P} = \mathcal{Q} \amalg \mathcal{R},\ g, h \in G,\ g(\mathcal{P}) = \mathcal{Q} \text{ et } h(\mathcal{P}) = \mathcal{R}.$$

En posant $m = n = 1$, $\mathcal{Q}_1 = \mathcal{Q}$, $\mathcal{R}_1 = \mathcal{R}$, $g_1 = g^{-1}$ et $h_1 = h^{-1}$, nous avons $g_1 \star \mathbf{Q}_1 = g^{-1}(\mathcal{Q}) = \mathcal{P}$ et $h_1 \star \mathbf{R}_1 = h^{-1}(\mathcal{Q}) = \mathcal{P}$.
Nous avons ainsi montré que toute partie G-dédoublable de E est G-paradoxale pour l'action canonique de G sur E.

A.3. Soit T une partie de E contenant un et un seul élément de chaque orbite. En reprenant les parties $\mathcal{Q}_1$, $\mathcal{Q}_2$, $\mathcal{R}_1$ et $\mathcal{R}_2$ définies à la question **IV.D.**, posons :

$$\mathcal{Q}_1^E = \{U \star x,\ U \in \mathcal{Q}_1,\ x \in T\} \qquad \mathcal{Q}_2^E = \{U \star x,\ U \in \mathcal{Q}_2,\ x \in T\}$$

$$\mathcal{R}_1^E = \{U \star x,\ U \in \mathcal{R}_1,\ x \in T\} \qquad \mathcal{R}_2^E = \{U \star x,\ U \in \mathcal{R}_2,\ x \in T\}$$

$$\mathcal{Q}^E = \mathcal{Q}_1^E \cup \mathcal{Q}_2^E \qquad \mathcal{R}^E = \mathcal{R}_1^E \cup \mathcal{R}_2^E$$

$$m = 2,\ g_1 = I \text{ et } g_2 = A \qquad n = 2,\ h_1 = I \text{ et } h_2 = B.$$

Nous avons alors :

- les parties $\mathcal{Q}_1$, $\mathcal{Q}_2$, $\mathcal{R}_1$ et $\mathcal{R}_2$ sont deux à deux disjointes : si x appartient à deux de ces quatre parties, il existe $(C_0, C_1, x_0, x_1) \in \Gamma \times \Gamma \times T \times T$ tel que

$$x = C_0 \star x_0 = C_1 \star x_1$$

avec C_0 et C_1 éléments de deux des quatre parties $\mathcal{Q}_1$, $\mathcal{Q}_2$, $\mathcal{R}_1$ et $\mathcal{R}_2$. Comme x_0 et x_1 sont des éléments de $T \cap \mathcal{O}(x)$ qui est un singleton, $x_0 = x_1$. On a ensuite

$$(C_0^{-1}C_1) \star x_1 = C_0^{-1} \star (C_1 \star x_1) = C_0^{-1} \star (C_0 \star x_0) = x_0 = x_1$$

donc $C_0^{-1}C_1 = I$, soit $C_0 = C_1$, qui contredit l'hypothèse puisque les parties $\mathcal{Q}_1$, $\mathcal{Q}_2$, $\mathcal{R}_1$ et $\mathcal{R}_2$ sont disjointes.

- $E = \bigcup_{1 \leq i \leq m} g_i \star \mathcal{Q}_i^E$:

  si $x \in E$, notons x_0 l'unique élément de $T \cap \mathcal{O}(x)$. Il existe alors $U \in \Gamma$ tel que $x = U \star x_0$. Comme $\Gamma = \mathcal{Q}_1 \cup \mathcal{A}Q_2$, deux cas se présentent :

  - si U est élément de $\mathcal{Q}_1$, $x \in Q_1^E$ et donc $x \in I \star \mathcal{Q}_1^E = g_1 \star \mathcal{Q}_1^E$;
  - si U est élément de $A\mathcal{Q}_2$, il existe $V \in \mathcal{Q}_2$ tel que $U = AV$, puis $x = A\star(V\star x_0) \in A\star Q_2^E = g_2\star\mathcal{Q}_1^E$.

- $E = \bigcup_{1 \leq j \leq n} h_j \star \mathcal{R}_j^E$: la preuve est rigoureuse identique à la précédente.

Nous avons donc montré qu'un ensemble non vide E sur lequel le groupe libre à deux générateurs Γ agit *simplement* est Γ-paradoxal.

B.1. Comme le pôle de la fraction est réel, la fonction h_M est définie sur H^2. Nous avons ensuite :

$$\operatorname{Im} h_M(x) = \frac{\operatorname{Im} x}{|cx + d|^2} > 0$$

donc h_M est à valeurs dans H^2. Comme M^{-1} est élément de $SL_2(\mathbf{Z})$, l'application $h_{M^{-1}}$ est également à valeurs dans H^2 et on montre facilement que $h_{M^{-1}} \circ h_M = h_M \circ h_{M^{-1}} = Id_{H^2}$: h_M est donc une bijection de H^2 sur lui-même.

B.2.(a) Si $h_M = Id$, le polynôme $P = (aX + b) - (cX + d)X$ admet une infinité de racines complexes : il est donc nul, ce qui donne $c = b = 0$ et $a = d$. La condition $ad - bc = 1$ impose alors $a = \pm 1$, ce qui conduit à $M = \pm I$. Comme, réciproquement, $h_{-I} = Id$, le noyau du morphisme est $\{\pm I\}$.

B.2.(b) Notons φ la restriction de ce morphisme à Γ. Comme $\Gamma \cap \{\pm I\} = \{I\}$, φ est un morphisme de groupe injectif : c'est donc un isomorphisme de Γ sur son image.

B.3.(a) Comme h_M fixe au moins un point de H^2, le polynôme $cX^2 + (d - a)X - b$ a au moins une racine dans H^2. Nous avons alors deux cas :

- si $c \neq 0$, ce polynôme est de degré 2 et à coefficients réels : son discriminant est donc strictement négatif (sinon, toutes ces racines seraient réelles). On en déduit que $(d - a)^2 + 4bc < 0$, ce qui donne $(a + d)^2 < 4$ en remplaçant bc par $ad - 1$. Ainsi $|a + d| < 2$, soit $|\operatorname{tr} M| < 2$;

- si $c = 0$, ce polynôme est de degré au plus 1 et à coefficients réels : il n'admet des racines non réelles que s'il est nul. On en déduit que $c = d - a = b = 0$, soit $M = \pm I$ (en utilisant $ad - bc = 1$) et $h_M = Id$.

B.3.(b) Si $h_M = Id$, h_M est d'ordre fini. Sinon, on a $\operatorname{tr} M \in \mathbf{Z}$ et $|\operatorname{tr} M| < 2$, donc $\operatorname{tr} M \in \{-1, 0, 1\}$. Comme $\det M = 1$, le polynôme caractéristique χ_M de M ne peut donc prendre que trois valeurs :

- $\chi_M = X^2 - X + 1$: le théorème de Cayley-Hamilton donne alors $M^2 - M + I = 0$, puis

$$M^6 - I = (M - I)(M + I)(M^2 + M + I)(M^2 - M + I) = 0\,;$$

- $\chi_M = X^2 + 1$: on a maintenant $M^2 + I = 0$, puis $M^4 - I = 0$;
- $\chi_M = X^2 + X + 1$: cette fois, on obtient $M^2 + M + I = 0$ puis $M^3 - I = (M - I)(M^2 + M + I) = 0$.

Dans tous les cas, la matrice M est d'ordre fini, ainsi que h_M puisque $M \to h_M$ est un morphisme de groupe.

B.4. D'après la question précédente, si h_M a un point fixe dans H^2, il est d'ordre fini dans $\overline{\Gamma}$; comme $\overline{\Gamma}$ est isomorphe à Γ et que le seul élément d'ordre fini de Γ est I, $h_M = Id$. Ainsi, aucun élément de $\overline{\Gamma} \setminus \{Id\}$ n'a de point fixe dans H^2.

B.5. Considérons l'application : $\begin{array}{ccc} \Gamma \times H^2 & \longrightarrow & H^2 \\ (M, x) & \longmapsto & h_M(x) \end{array}$. Cette application définit clairement une action de Γ sur H^2 et pour tout x, le stabilisateur de x est réduit à $\{I\}$ d'après la propriété démontrée à la question **4.** ; le résultat de la question **A.3.** s'applique donc : H^2 est Γ-paradoxal pour l'action $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \star x = \dfrac{ax + b}{cx + d}$.

C.1. Soit $\gamma \in \Gamma_g$, avec $\gamma = \gamma_U$, et $p = (x, y)$ et $q = (z, t)$ deux éléments de $\mathbf{R}^2$ tels que $p \sim q$. En notant (a, b, c, d) les coefficients entiers de U, nous avons :

$$\gamma(p) - \gamma(q) = (a(x - z) + b(y - t), c(x - z) + d(y - t)) \in \mathbf{Z}^2$$

car $a, x - z, b, y - t, c, x - z, d, y - t \in \mathbf{Z}$; nous avons donc $\gamma(p) \sim \gamma(q)$.

C.2. Soient γ_1 et γ_2 deux éléments de Γ_g. Pour tout $p \in \mathbf{R}^2$:

- $\widehat{\gamma}_1(\widehat{\gamma}_2(p))$ est un élément de Δ ;
- $\gamma_2(p) \sim \widehat{\gamma}_2(p)$ donne (d'après **1.**) : $\gamma_1 \circ \gamma_2(p) \sim \gamma_1(\widehat{\gamma}_2(p)) \sim \widehat{\gamma}_1(\widehat{\gamma}_2(p))$.

Ceci prouve donc que $\widehat{\gamma}_1 \circ \widehat{\gamma}_2 = \widehat{\gamma_1 \circ \gamma_2}$.

Cette égalité démontre ensuite la bijectivité de $\widehat{\gamma}$ pour tout γ, puisque $\widehat{\gamma} \circ \widehat{\gamma^{-1}} = \widehat{\gamma^{-1}} \circ \widehat{\gamma} = \widehat{Id_{\mathbf{R}^2}} = Id_\Delta$.

L'application $\varphi\ :\ \gamma \mapsto \widehat{\gamma}$ est donc un morphisme du groupe $(\Gamma_g, \circ)$ dans le groupe $(\mathfrak{S}_\Delta, \circ)$. Montrons que φ est injective : soit $\gamma \in \operatorname{Ker}(\varphi)$, associé à $U = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$. Pour tout entier $n \geq 2$, nous avons

$$\gamma((1/n, 0)) \sim (1/n, 0),$$

ce qui donne $\dfrac{a - 1}{n} \in \mathbf{Z}$ et $\dfrac{c}{n} \in \mathbf{Z}$. Ainsi, n divise $a - 1$ et c. Comme n est un entier ≥ 2 quelconque, $a = 1$ et c est nul. On montrerait de la même manière que $d = 1$ et $b = 1$, ce qui donne $\gamma = Id_{\mathbf{R}^2}$: le noyau de φ est réduit à $\{Id_{\mathbf{R}^2}\}$.

C.3. Les applications $\begin{array}{ccc} \Gamma & \longrightarrow & \Gamma_g \\ U & \longmapsto & \gamma_U \end{array}$ et $\begin{array}{ccc} \Gamma_g & \longrightarrow & \widehat{\Gamma}_g \\ \gamma & \longmapsto & \widehat{\gamma} \end{array}$ sont bijectives : il suffit donc de montrer que Γ est dénombrable pour démontrer que $\widehat{\Gamma}_g$ l'est. Il suffit pour cela de remarquer :

- que Γ n'est pas fini (A, par exemple, est d'ordre infini) ;
- que Γ est réunion dénombrable d'ensembles finis :

$$\Gamma = \bigcup_{n \in \mathbf{N}} \{U \in SL_2(\mathbf{Z}),\ \exists\, (U_1, U_2, \ldots, U_n) \in \{A, A^{-1}, B, B^{-1}\},\ U = U_1 U_2 \ldots U_n\}.$$

C.4.(a) Chaque $C_0 \cap \mathcal{D}_n$ contient au maximum deux éléments : la réunion de ces parties est une partie dénombrable, qui ne peut donc être égale à C_0 qui n'est pas dénombrable. En effet, si X_0 est le centre de C_0 et si r est son rayon (avec $r > 0$), l'application

$$\begin{array}{ccc}]-\pi,\pi[& \longrightarrow & C_0 \\ \theta & \longmapsto & X_0 + r\begin{pmatrix}\cos(\theta)\\ \sin(\theta)\end{pmatrix} \end{array}$$

est injective, et $]-\pi,\pi[$ est homéomorphe à $\mathbf{R}$, donc non dénombrable.

C.4.(b) Soit $\gamma \in \Gamma_g \setminus \{Id\}$. Si p est invariant par $\widehat{\gamma}$, il existe un élément $q \in \mathbf{Z}^2$ tel que $\gamma(p) = p + q$. Comme γ est différent de Id, on peut voir cette équation comme un système linéaire d'inconnu p et de rang au moins 1. Plus précisément, nous pouvons distinguer deux cas :

- si $\gamma - Id$ est de rang 2, l'équation $\gamma(p) = p + q$ a une et une seule solution $p_{\gamma,q}$ dans $\mathbf{R}^2$;
- si $\gamma - Id$ est de rang 1, l'équation $\gamma(p) = p + q$ a pour solution ou bien l'ensemble vide, ou bien une droite affine $D_{\gamma,q}$.

Comme $\mathbf{Z}^2$ et Γ_g sont dénombrables, il est possible d'énumérer les familles :

$$\Big(p_{\gamma,q}\Big)_{\substack{\gamma\in\Gamma_g,\ q\in\mathbf{Z}^2\\ \mathrm{rg}(\gamma-Id)=2}} \text{ et } \Big(D_{\gamma,q}\Big)_{\substack{\gamma\in\Gamma_g,\ q\in\mathrm{Im}\,(\gamma-Id)\\ \mathrm{rg}(\gamma-Id)=1}}$$

en respectivement

$$(p_n)_{n\in\mathbf{N}} \text{ et } (D_n)_{n\in\mathbf{N}}.$$

Nous avons alors :

$$F = \Big(\Delta \cap \{p_n, n\in\mathbf{N}\}\Big) \cup \Big(\bigcup_{n\in\mathbf{N}} \Delta \cap D_n\Big)$$

puis

$$C_0 \cap F = \Big(C_0 \cap \{p_n, n\in\mathbf{N}\}\Big) \cup \Big(\bigcup_{n\in\mathbf{N}} C_0 \cap D_n\Big).$$

Ceci prouve, avec l'argument de la question précédente, que $C_0 \cap F$ est dénombrable, donc distinct de C_0.

Il est également possible d'utiliser directement le résultat précédent en choisissant, pour chaque point p_n, une droite $\mathcal{D}'_n$ passant par p_n. Nous avons alors :

$$C_0 \cap F \subset \bigcup_{n\in\mathbf{N}} \Big((C_0 \cap \mathcal{D}_n) \cup (C_0 \cap \mathcal{D}'_n)\Big)$$

et cette partie est strictement contenue dans C_0.

C.5. D'après la question précédent, F ne contient aucun cercle, donc, à plus forte raison, aucun disque ouvert de rayon non nul : F est d'intérieur vide.

C.6. Comme F est d'intérieur vide, $F \neq \Delta$ et $\mathcal{P}$ est bien une partie bornée non vide de $\mathbf{R}^2$. Considérons alors l'application :

$$\star : \begin{array}{ccc} \Gamma \times \mathcal{P} & \longrightarrow & \Delta \\ (U,p) & \longmapsto & U \star p = \widehat{\gamma}_U(p) \end{array}$$

Nous avons successivement :

- si $(U,p) \in \Gamma \times \mathcal{P}$, $U \star p \in \mathcal{P}$.
  En effet, dans le cas contraire, il existerait $\widehat{\gamma} \in \widehat{\Gamma}_g \setminus \{Id\}$ tel que $\widehat{\gamma}(\widehat{\gamma}_U(p)) = \widehat{\gamma}_U(p)$, ce qui donnerait $\widehat{\gamma_U^{-1} \circ \gamma \circ \gamma_U}(p) = p$: ceci est impossible car $\gamma_U^{-1} \circ \gamma \circ \gamma_U \neq Id$ et $p \notin F$.
- l'application $\star$ est une action de Γ sur $\mathcal{P}$:
  - pour tout $(U,V) \in \Gamma^2$ et pour tout $p \in F$,
  $$U \star (V \star p) = \widehat{\gamma}_U\,(\widehat{\gamma}_V\,(p)) = \widehat{\gamma_U \circ \gamma_V}(p) = \widehat{\gamma}_{UV}(p) = (UV) \star p\,;$$
  - $\forall\, p \in \mathcal{P}$, $Id \star p = \widehat{p} = p$.
- si $p \in \mathcal{H}$, l'unique $U \in \Gamma$ tel que $U \star p = p$ est $U = I$ (par définition de F).

Comme Γ agit simplement sur $\mathcal{P}$, on peut appliquer le résultat du **A.3.** : $\mathcal{P}$ est un ensemble Γ-paradoxal.