Agrégation interne 2004 de Mathématiques

solution proposée par Dany-Jack Mercier

IUFM de Guadeloupe, Morne Ferret,
BP399, Pointe-à-Pitre cedex 97159,
dany-jack.mercier@univ-ag.fr

NB : Le sujet de l'épreuve n'est pas joint à ce document. Il pourra être téléchargé sur le site http ://perso.wanadoo.fr/megamaths/

[0] [ag58] v1.00

Je noterai $d(x,y) = |x-y|$ la distance euclidienne entre deux points de $\mathbb{C}$. De façon générale, je noterai $|E|$ le cardinal d'un ensemble E.

Partie I : Parties dédoublables de $\mathbb{C} = \mathbb{R}^2$

I.A.1.a. On suppose que x et y appartiennent à $\overline{D}$ et vérifient $d(x,y) = 2$. Si 0 n'appartenait pas au segment $[xy]$, on aurait

$$d(x,y) < d(x,0) + d(0,y) \leq 1 + 1 = 2,$$

soit $d(x,y) < 2$, ce qui est absurde. Donc $0 \in [xy]$ et

$$d(x,0) + d(0,y) = d(x,y) = 2.$$

La somme des deux nombres positifs $d(x,0)$ et $d(0,y)$ chacun inférieur à 1, sera égale à 2 si et seulement si $d(x,0) = d(0,y) = 1$. Le point 0 appartient donc au segment $[xy]$ et se trouve à égale distance de ses extrémités : c'est le milieu de $[xy]$.

Remarque : $[xy]$ est finalement un diamètre du cercle $\partial\overline{D}$, frontière du disque $\overline{D}$.

I.A.1.b. Soit $w \in \overline{D}$. La contaposée de

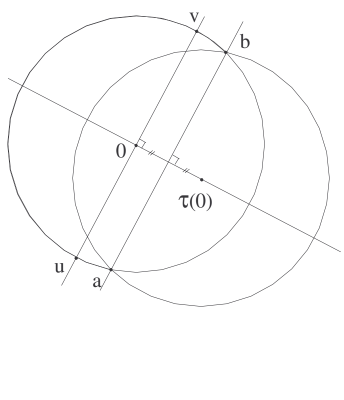
$$|w - \tau(0)| > 1 \Rightarrow w \in A$$

s'écrit

$$w \in B \Rightarrow |w - \tau(0)| \leq 1. \quad (*)$$

Si $w \in B = \tau(A)$, il existe $z \in A$ tel que $w = \tau(z)$.
Puisque $z \in A \subset \overline{D}$ et puisque τ conserve les distances (c'est une isométrie), on obtient bien $d(w, \tau(0)) = d(\tau(z), \tau(0)) = d(z, 0) \leq 1$, et $(*)$ est prouvée.

I.A.1.c. Puisque 0 appartient à A, $\tau(0)$ appartient à B. On a $\tau(0) \neq 0$, sinon 0 appartiendrait à $A \cap B$, ce qui est impossible par hypothèse. Donc $\tau(0) \neq 0$ et les deux cercles $\partial\overline{D}$ et $\mathcal{C}(\tau(0), 1)$ (de centre $\tau(0)$ et de rayon 1) se coupent en deux points a et b tels que (ab) soit la médiatrice de $[0\tau(0)]$.



La parallèle à (ab) passant par 0 coupe $\partial\overline{D}$ en u et v, et le Théorème de Pythagore permet d'écrire

$$d(\tau(0), u)^2 = d(\tau(0), 0)^2 + d(0,u)^2 > d(0,u)^2$$

d'où $d(\tau(0), u) > 1$, et par conséquent $u \in A$ d'après **I.A.1.b**. De la même manière, $v \in A$, et le diamètre $[uv]$ de $\overline{D}$ possède ses deux extrémités dans A.

I.A.1.d. L'image du diamètre $[uv]$ de $\overline{D}$ par l'isométrie τ est un segment $[\tau(u)\,\tau(v)]$ de même longueur 2 et d'extrémités dans B (puisque $\tau(A) = B$). La question **I.A.1.a** montre alors que 0 est le milieu de $[\tau(u)\,\tau(v)]$. Mais τ est une bijection affine, donc conserve les milieux des segments. Elle transforme donc le milieu 0 de $[uv]$ en celui de $[\tau(u)\,\tau(v)]$, c'est-à-dire $\tau(0) = 0$. C'est l'absurdité cherchée ($\tau(0) = 0$ entraîne $0 \in A \cap B$, impossible par hypothèse).

I.A.2. Si $\overline{D}$ était $\mathfrak{I}_2$-dédoublable, il exiterait une partition $\overline{D} = A \cup B$ de $\overline{D}$ ainsi que deux isométries g_1, g_2, telles que $g_1(\overline{D}) = A$ et $g_2(\overline{D}) = B$. On peut toujours supposer que 0 appartient à A quitte à permuter les notations A et B. L'application $\tau = g_2 \circ g_1^{-1}$ appartient à $\mathfrak{I}_2$ et vérifie $\tau(A) = B$. On retrouve les hypothèses de **I.A.1**, et l'on sait que ces hypothèses mènent à une absurdité. En conclusion, $\overline{D}$ n'est pas $\mathfrak{I}_2$-dédoublable.

I.B.1.1.a. L'ensemble R est inclus dans $\mathbb{R}$, minoré par 0, et n'est pas vide puisque $\mathcal{B}$ est borné (autrement dit, il existe $M \in \mathbb{R}_+$ et $c \in \mathbb{C}$ tels que $\mathcal{B} \subset \overline{D}(c, M)$, ce qui montre que $\mathcal{C}_M \neq \emptyset$ et donc que M appartient à R). Le Théorème de la borne supérieure dans $\mathbb{R}$ montre que R possède une borne inférieure ρ.

Remarque : Tentons de dire simplement la chose : ρ est la borne inférieure de l'ensemble de tous les nombres positifs qui sont les rayons d'au moins une boule fermée contenant $\mathcal{B}$.

I.B.1.1.b. Par définition d'une borne inférieure dans $\mathbb{R}$,

$$\forall n \in \mathbb{N}^* \quad \exists r \in R \quad \rho \leq r < \rho + \frac{1}{n}.$$

Puisque $r \in R$, il existe $x_n \in \mathbb{C}$ tel que $\mathcal{B} \subset \overline{D}(x_n, r)$, et à fortiori

$$\mathcal{B} \subset \overline{D}(x_n, \rho + \frac{1}{n}).$$

I.B.1.2.a. Puisque $\mathcal{B}$ est bornée, il existe $M \in \mathbb{R}_+$ tel que $\mathcal{B} \subset \overline{D}(0, M)$. Pour tout $b \in \mathcal{B}$,

$$d(0, x_n) \leq d(0, b) + d(b, x_n) \leq M + \left(\rho + \frac{1}{n}\right) \leq M + \rho + 1.$$

La suite $(x_n)_n$ est donc incluse dans le compact $\overline{D}(0, M+\rho+1)$, et l'on peut en extraire une sous-suite convergente (caractérisation des compacts dans un espace métrique, Théorème de Bolzano-Weierstrass).

I.B.1.2.b. Notons $(x_{n_k})_k$ la sous-suite convergente vers $a \in \mathbb{C}$. On a

$$\forall k \quad \mathcal{B} \subset \overline{D}(x_{n_k}, \rho + \frac{1}{n_k}),$$

autrement dit pour tout $b \in \mathcal{B}$, $d(b, x_{n_k}) \leq \rho + \frac{1}{n_k}$. Si l'on fait tendre k vers $+\infty$ dans les deux membres de cette inégalité, on obtient (compte tenu de la continuité de l'application $x \mapsto d(b,x)$),

$$\forall b \in \mathcal{B} \quad d(b,a) \leq \rho,$$

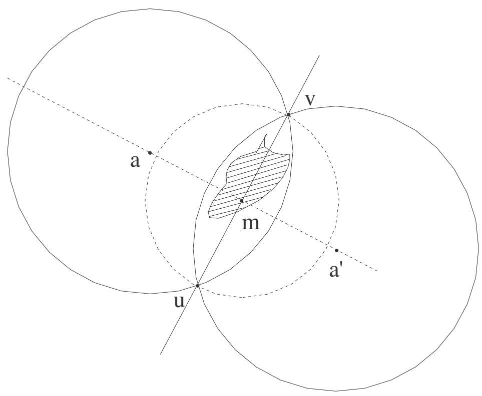
soit $\mathcal{B} \subset \overline{D}(a,\rho)$.

Remarque : Ainsi $\rho \in R$ et l'on peut écrire $\rho = \operatorname{Min} R$.

I.B.1.2.c. Supposons par l'absurde qu'il existe deux complexes a et a' vérifiant la propriété de la question (**c**). Alors $\mathcal{B} \subset \overline{D}(a,\rho) \cap \overline{D}(a',\rho)$ et les deux disques $\overline{D}(a,\rho)$ et $\overline{D}(a',\rho)$ sont sécants. Si u et v désignent les points d'intersections des frontières de ces disques, et m le milieu de $[uv]$ (voir dessin ci-dessous), on obtient

$$\mathcal{B} \subset \overline{D}(a,\rho) \cap \overline{D}(a',\rho) \subset \overline{D}(m,r)$$

où $r = d(m,v)$. Alors $r \in R$, ce qui contredit le choix de ρ puisque $r < \rho$ (d'après Pythagore).



I.B.2.1. Les isométries du plan sont les translations, les rotations, les réflexions et les réflexions glissées.

I.B.2.2.a. On procède par élimination.

▶ α) Si τ_1 est une translation de vecteur non nul u,

$$\tau_1(\mathcal{B}) = \mathcal{B}_1 \subset \mathcal{B} \Rightarrow \tau_1^2(\mathcal{B}) \subset \tau_1(\mathcal{B}) \subset \mathcal{B},$$

et ainsi de suite. On vérifie par récurrence que $\tau_1^n(\mathcal{B}) \subset \mathcal{B}$ pour tout $n \in \mathbb{N}^*$. La propriété est évidente au rang $n = 0$. Si elle est vraie au rang n, $\tau_1^n(\mathcal{B}) \subset \mathcal{B}$ entraîne

$$\tau_1^{n+1}(\mathcal{B}) = \tau_1(\tau_1^n(\mathcal{B})) \subset \tau_1(\mathcal{B})\mathcal{B}_1 \subset \mathcal{B}$$

et la propriété est encore vraie au rang $n+1$. Tout cela est absurde, puisque $\mathcal{B}$, bornée et non vide, ne peut pas être stable par une translation de vecteur non nul. En effet, si $b \in \mathcal{B}$, la suite de translatés $(b + nu)_{n\in\mathbb{N}}$ est dans $\mathcal{B}$ et n'est certainement pas bornée.

▶ β) Si τ_1 est une réflexion, elle est involutive et

$$\tau_1(\mathcal{B}) \subset \mathcal{B} \Rightarrow \mathcal{B} \subset \tau_1(\mathcal{B}).$$

Par suite $\tau_1(\mathcal{B}) = \mathcal{B}_1 = \mathcal{B}$, ce qui est absurde puisque $\mathcal{B}_1 \subsetneq \mathcal{B}$.

Remarque : Ce dernier point, rappelé par l'énoncé, est trivial. En effet, si l'on avait $\mathcal{B}_1 = \mathcal{B}$, on aurait $\tau_2(\mathcal{B}) = \mathcal{B}_2 = \emptyset$, ce qui est absurde puisque $\mathcal{B}$ n'est pas vide et que τ_2 est une application.

▶ γ) Si τ_1 est une réflexion glissée (sans point invariant), il existe une réflexion s et une translation t_u de vecteur u non nul appartenant à l'axe de la réflexion, telles que

$$\tau_1 = s \circ t_u = t_u \circ s.$$

Dans ce cas $\tau_1^2 = t_{2u}$ est une translation de vecteur non nul telle que $\tau_1^2(\mathcal{B}) \subset \mathcal{B}$. Il suffit de raisonner comme en α) pour conclure à une absurdité.

En conclusion, τ_1 et τ_2 seront des rotations, distinctes de l'identité (en effet, $\tau_1 = Id$ entraînerait $Id(\mathcal{B}) = \mathcal{B} = \mathcal{B}_1$, ce qui est absurde d'après la remarque ci-dessus).

Remarque : Nicolas Herla nous signale que l'utilisation d'un repère judicieux permet de prouver que τ_1 ne peut être ni une translation, ni une réflexion glissée. En effet, choisissons un premier axe de coordonnée dirigé et orienté par le vecteur $\overrightarrow{u}$ de la translation τ_1 (ou de la réflexion glissée écrite sous sa forme canonique), et notons $(a, 0)$ les coordonnées de $\overrightarrow{u}$ dans la base associée au repère (avec $a > 0$). Le réel $b = \operatorname{Sup}\{x \in \mathbb{R} / \ (x, y) \in \mathcal{B}\}$ est bien défini puisque la partie $\mathcal{B}$ est bornée, et il existe $(x_0, y) \in \mathcal{B}$ tel que $b - \frac{a}{2} < x_0 \leq b$ par définition d'une borne supérieure. Dans ce cas $\tau_1\left((x_0, y)\right) = (x_0 + a, y)$

appartient à $\tau_1(\mathcal{B}) = \mathcal{B}_1$, donc à $\mathcal{B}$, et $b < b + \frac{a}{2} < x_0 + a$, en contradiction avec la définition de b.

I.B.2.2.b. On a

$$\begin{cases} \mathcal{B} \subset \overline{D}(a,\rho) \Rightarrow \mathcal{B}_1 = \tau_1(\mathcal{B}) \subset \overline{D}(\tau_1(a),\rho) \\ \mathcal{B} \subset \overline{D}(a,\rho) \Rightarrow \mathcal{B}_2 = \tau_2(\mathcal{B}) \subset \overline{D}(\tau_2(a),\rho) \end{cases}$$

donc

$$\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2 \subset \overline{D}(\tau_1(a),\rho) \cap \overline{D}(\tau_2(a),\rho).$$

Si l'on suppose par l'absurde que $\tau_1(a) \neq \tau_2(a)$, on montre (en raisonnant comme en **I.B.1.2.c**) l'existence d'un point m et d'un réel positif $r < \rho$ tels que

$$\mathcal{B} \subset \overline{D}(\tau_1(a),\rho) \cap \overline{D}(\tau_2(a),\rho) \subset \overline{D}(m,r).$$

C'est absurde. Donc $\tau_1(a) = \tau_2(a)$ et l'on a les trois inclusions

$$\mathcal{B} \subset \overline{D}(\tau_1(a),\rho), \quad \mathcal{B} \subset \overline{D}(\tau_2(a),\rho) \quad \text{et} \quad \mathcal{B} \subset \overline{D}(a,\rho).$$

L'unicité du disque fermé de rayon minimum contenant $\mathcal{B}$ montre alors que $\tau_1(a) = \tau_2(a) = a$.

I.B.2.2.c. On a

$$\tau_1(\tau_2(\mathcal{B})) \subset \tau_1(\mathcal{B}_2) \subset \tau_1(\mathcal{B}) = \mathcal{B}_1.$$

Les rotations τ_1 et τ_2 sont de même centre a, donc commutent entre elles. Ainsi

$$\tau_1(\tau_2(\mathcal{B})) = \tau_2(\tau_1(\mathcal{B})) \subset \tau_2(\mathcal{B}_1) \subset \tau_2(\mathcal{B}) = \mathcal{B}_2.$$

Finalement $\tau_1(\tau_2(\mathcal{B})) \subset \mathcal{B}_1 \cap \mathcal{B}_2$, ce qui est absurde puisque $\mathcal{B}_1 \cap \mathcal{B}_2 = \emptyset$ et $\tau_1(\tau_2(\mathcal{B})) \neq \emptyset$.

Remarque : Il peut paraître surprenant de trouver une isométrie f qui transforme une partie $\mathcal{B}$ du plan en une partie $f(\mathcal{B})$ strictement incluse dans $\mathcal{B}$. Nicolas Herla nous propose de choisir $\mathcal{B} = \{ue^{ik\theta 2\pi} \,/\, k \in \mathbb{N}\}$, où $u \in \mathbb{C}$ et $\theta \in \mathbb{R}\backslash\mathbb{Q}$. La rotation $f(z) = e^{i\theta 2\pi}z$ est telle que $f(\mathcal{B}) \subset \mathcal{B}$ mais u n'appartient pas à $f(\mathcal{B})$.

Partie II : Paradoxe de Sierpinski-Mazurkiewicz

II.1. Si x appartient à $t(\mathcal{D}) \cap r(\mathcal{D})$, il existe deux polynômes P et Q de $\mathcal{P}_{\mathbb{N}}$ tels que $x = t(P(u)) = r(Q(u))$. Cela s'écrit $P(u)+1 = uQ(u)$ et montre que u annule le polynôme $P(X) - XQ(X) + 1$ à coefficients dans $\mathbb{Z}$. La transcendance de u donne $P(X) - XQ(X) + 1 = 0$. Dans ce cas $P(0) = -1$, et l'on obtient une absurdité puisque tous les coefficients de $P(X)$ appartiennent à $\mathbb{N}$.

II.2. ▶ Le résultat indiqué par l'énoncé est trivial : tout polynôme P de $\mathcal{P}_{\mathbb{N}}$ s'écrit sous l'une des formes suivantes : $P = R + 1$ (avec $P \in \mathcal{P}_{\mathbb{N}}$) s'il possède un terme constant non nul, ou $P = XS$ (avec $S \in \mathcal{P}_{\mathbb{N}}$) dans le cas contraire.

▶ Posons

$$\mathcal{D}_1 = t(\mathcal{D}) = \{P(u) + 1 \,/\, P \in \mathcal{P}_{\mathbb{N}}\} \quad \text{et} \quad \mathcal{D}_2 = r(\mathcal{D}) = \{uP(u) \,/\, P \in \mathcal{P}_{\mathbb{N}}\}.$$

On a déjà prouvé que $\mathcal{D}_1 \cap \mathcal{D}_2 = \emptyset$ à la question **II.1**, et pour pouvoir affirmer que $\mathcal{D}$ est $\mathfrak{I}_2$-dédoublable, il reste seulement à vérifier que $\mathcal{D} = \mathcal{D}_1 \cup \mathcal{D}_2$. Clairement $\mathcal{D}_1 \cup \mathcal{D}_2 \subset \mathcal{D}$. Réciproquement, si $x \in \mathcal{D}$, x s'écrit $x = P(u)$ avec $P \in \mathcal{P}_{\mathbb{N}}$. De deux choses l'une :

- ou bien P s'écrit $R + 1$ avec $P \in \mathcal{P}_{\mathbb{N}}$, et dans ce cas

$$x = P(u) = R(u) + 1 = t(R(u)) \in t(\mathcal{D}) = \mathcal{D}_1,$$

- ou bien P s'écrit XS avec $S \in \mathcal{P}_{\mathbb{N}}$, et

$$x = P(u) = uR(u) = r(R(u)) \in r(\mathcal{D}) = \mathcal{D}_2.$$

Partie III : Parties dédoublables de $\mathbb{R}$

III.A.1. L'application

$$\begin{array}{rccc} \Phi : & B_S(p) \times B_S(q) & \to & B_S(p+q) \\ & (x, y) & \mapsto & xy \end{array}$$

est bien définie car, si $l_S(x) \leq p$ et $l_S(y) \leq q$, alors $l_S(xy) \leq p + q$. Montrons qu'elle est surjective. Si $z \in B_S(p+q)$, $l_S(z) \leq p+q$ donc z s'écrit $z = a_1...a_m$ avec $m \leq p + q$ et $a_i \in S$ pour tout i. On peut toujours écrire $z = xy$ avec $x = a_1...a_p$ et $y = a_{p+1}...a_m$. Alors $x \in B_S(p)$, $y \in B_S(q)$ et $z = xy = \Phi(x, y)$.

La surjectivité de Φ permet d'écrire

$$|B_S(p+q)| \leq |B_S(p)| \times |B_S(q)|,$$

c'est-à-dire $\gamma_S(p+q) \leq \gamma_S(p)\gamma_S(q)$.

III.A.2.a. Par division euclidienne, $n = pq + r$ avec $0 \leq r < p$. On a

$$\begin{aligned} v_n \leq v_p + \frac{p}{n} v_1 \quad &\Leftrightarrow \quad \frac{\ln \gamma_S(n)}{n} \leq \frac{\ln \gamma_S(p)}{p} + \frac{p}{n} \ln \gamma_S(1) \\ &\Leftrightarrow \quad p \ln \gamma_S(n) \leq n \ln \gamma_S(p) + p^2 \ln \gamma_S(1). \quad (1) \end{aligned}$$

Par ailleurs, **III.A.1** permet d'écrire les majorations suivantes :

$$\gamma_S(n) = \gamma_S(pq+r) \leq \gamma_S(pq)\gamma_S(r) \leq \gamma_S(p)^q \gamma_S(1)^r$$

d'où

$$\begin{aligned} \ln \gamma_S(n) &\leq q \ln \gamma_S(p) + r \ln \gamma_S(1), \\ p \ln \gamma_S(n) &\leq pq \ln \gamma_S(p) + pr \ln \gamma_S(1). \quad (2) \end{aligned}$$

Comme $pq \leq n$ et $pr < p^2$, (2) entraîne (1), et permet de conclure.

III.A.2.b. Posons $v = \operatorname{Inf} v_n$. Pour tout $\varepsilon > 0$, il existe un entier p tel que $v \leq v_p < v + \varepsilon$. Pour tout entier naturel n non nul, on a donc

$$v \leq v_n \leq v_p + \frac{p}{n} v_1 < v + \varepsilon + \frac{p}{n} v_1.$$

Il existe $N > 0$ tel que $n > N$ entraîne $\frac{p}{n} v_1 \leq \varepsilon$. Par conséquent

$$\forall \varepsilon > 0 \quad \exists N > 0 \quad n > N \Rightarrow v \leq v_n \leq v + 2\varepsilon \Rightarrow |v - v_n| < 2\varepsilon,$$

et $\lim v_n = v$.

III.A.3. On a

$$c_S(n) = (\gamma_S(n))^{\frac{1}{n}} = e^{\frac{1}{n} \ln \gamma_S(n)} = e^{v_n}$$

donc $\lim_{n \to +\infty} c_S(n) = e^v$ et $C_S = e^v$. D'autre part, pour tout $n \in \mathbb{N}^*$,

$$\gamma_S(n) \geq 1 \Rightarrow v_n = \frac{\ln \gamma_S(n)}{n} \geq 0 \Rightarrow e^{v_n} \geq 1$$

donc $C_S = e^v \geq 1$ en passant à la limite dans la dernière l'inégalité.

III.A.4. Si G contient un sous-groupe H à croissance exponentielle, il existe une partie finie symétrique S de H telle que $C_S = \lim_{n \to +\infty} c_S(n) > 1$. Mais S

est à fortiori une partie finie symétrique S de G, et vérifie toujours $C_S > 1$, donc G est à croissance exponentielle.

III.A.5. Soit G un groupe abélien et $S = \{s_1, ..., s_m\}$ une partie finie symétrique de G de cardinal m. L'ensemble $B_S(n)$ est formé des éléments x qui s'écrivent $x = s_1...s_p$ avec $1 \leq p \leq n$. Comme G est commutatif, on peut toujours rassembler les éléments s_i intervenant dans l'écriture $x = s_1...s_p$ et écrire $x = s_1^{\alpha_1}, ..., s_m^{\alpha_m}$ avec $(\alpha_1, ..., \alpha_m) \in \mathbb{N}^m$ et $\alpha_1 + ... + \alpha_m = p$. On sait que

$$|\{(\alpha_1, ..., \alpha_m) \in \mathbb{N}^m \,/\, \alpha_1 + ... + \alpha_m = p\}| = \binom{p+m-1}{m-1}.$$

Le cardinal $|B_S(n)|$ sera donc majoré par

$$\sum_{p=1}^{n} \binom{p+m-1}{m-1} = \binom{n+m}{m} - 1.$$

On aura donc $|B_S(n)| \leq \binom{n+m}{m}$ et

$$c_S(n) = (|B_S(n)|)^{\frac{1}{n}} \leq \binom{n+m}{m}^{\frac{1}{n}}.$$

Cela entraîne $C_S = \lim_{n\to+\infty} c_S(n) \leq 1$, soit $C_S = 1$ puisque l'inégalité $C_S \geq 1$ est toujours vraie (**III.A.3**). Cela prouve que la croissance de G est sous-exponentielle.

Remarque : La limite $\lim_{n\to+\infty} \binom{n+m}{m}^{\frac{1}{n}} = 1$ s'obtient en passant au logarithme. En effet

$$\begin{aligned} \frac{1}{n} \ln \binom{n+m}{m} &= \frac{1}{n} \ln \frac{(n+m)(n+m-1)...(n+1)}{m!} \\ &= \frac{\ln(n+m)}{n} + ... + \frac{\ln(n+1)}{n} - \frac{\ln m!}{n} \end{aligned}$$

tend vers 0 lorsque n tend vers $+\infty$.

III.B.1. f appartient à $\mathfrak{I}_1$ si et seulement si c'est une applicatin affine de $\mathbb{R}$ dans $\mathbb{R}$ de partie linéaire une application orthogonale de $\mathbb{R}$. Les seules applications orthogonales de la droite sont $\pm Id$, donc f sera soit une translation, soit une symétrie centrale.
Une autre façon de répondre à la question consiste à poser $v = f(0)$, puis à rappeler la définition d'une application affine :

$$\forall x \in \mathbb{R} \quad f(x) - f(0) = \pm Id(x - 0),$$

pour obtenir directement $f(x) = ux + v$ avec $u = \pm 1$.

III.B.2. Si t et ε' vérifient $\varepsilon \circ s = t \circ \varepsilon'$, de deux choses l'une :

- ou bien $\varepsilon \circ s \in \mathfrak{I}_1^+$, et nécessairement $\varepsilon' \in \mathfrak{I}_1^+$ (puisque $t \in \mathfrak{I}_1^+$ fait partie de nos hypothèses) donc $\varepsilon' = Id$ et $t = \varepsilon \circ s$.

- ou bien $\varepsilon \circ s \notin \mathfrak{I}_1^+$, ce qui entraîne $\varepsilon' \notin \mathfrak{I}_1^+$ donc $\varepsilon' = -Id$ et $t = \varepsilon \circ s \circ \varepsilon'$.

L'unicité de la décomposition est démontrée. L'existence ne pose aucun problème : il suffit de vérifier que les décompositions proposées ci-dessus conviennent (par exemple, dans le premier cas, $\varepsilon' = Id$ et $t = \varepsilon \circ s$ permettent d'obtenir la décomposition $\varepsilon \circ s = t \circ \varepsilon'$, et t est bien une isométrie positive).

III.B.3. Tout élément τ de $B_S(n)$ s'écrit sous la forme $\tau = s_1 \circ ... \circ s_m$ où $s_i \in S$ et $m \leq n$. On va montrer la propriété suivante par récurrence finie sur m (pour m variant de 1 à n) :

$H(m)$: $\tau = s_1 \circ ... \circ s_m$ s'écrit sous la forme $\tau = t_1 \circ ... \circ t_m \circ (\pm Id)$ avec $t_i \in T$.

La propriété est triviale si $m = 1$, puisque s_1 s'écrit $t \circ \varepsilon'$ d'après **III.B.2**. Si la propriété est vraie jusqu'au rang $m-1$, avec $m \leq n$, montrons-là au rang m. Pour cela, considérons un élément $\tau = s_1 \circ ... \circ s_m$. On peut écrire

$$\tau = (s_1 \circ ... \circ s_{m-1}) \circ s_m = t_1 \circ ... \circ t_{m-1} \circ \varepsilon' \circ s_m$$

par application de l'hypothèse récurrente. Comme il existe $t_m \in T$ et $\varepsilon'' = \pm Id$ tels que $\varepsilon' \circ s_m = t_m \circ \varepsilon''$ (cf. **III.B.2**), on obtient bien $\tau = t_1 \circ ... \circ t_{m-1} \circ t_m \circ \varepsilon''$ de la forme voulue.

III.B.4. La question précédente montre que tout élément τ appartenant à $B_S(n)$ s'écrit $\tau = t_1 \circ ... \circ t_m \circ (\pm Id)$ avec $t_i \in T$ et $m \leq n$, autrement dit comme le produit d'un élément $t_1 \circ ... \circ t_m$ de $B_T(n)$ et de $\pm Id$. Le groupe $\mathfrak{I}_1^+$ est commutatif, donc $|B_T(n)| \leq \binom{n+m}{m}$ (cf. solution de **III.A.5**) et l'on en déduit

$$|B_S(n)| \leq 2 \times |B_T(n)| \leq 2\binom{n+m}{m}.$$

Ainsi $C_S = \lim_{n \to +\infty} (|B_S(n)|)^{\frac{1}{n}} \leq \lim_{n \to +\infty} \left(2\binom{n+m}{m}\right)^{\frac{1}{n}} = 1$, soit $C_S = 1$ puisque l'on a toujours $C_S \geq 1$ d'après **III.A.3**. Le groupe $\mathfrak{I}_1$ est donc bien à croissance sous-exponentielle.

III.C.1. Si $x \in \gamma_s(\mathcal{D}) \cap \gamma_{s'}(\mathcal{D})$, il existe y et z tels que

$$s_1 \circ ... \circ s_n(y) = s'_1 \circ ... \circ s'_n(z). \quad (\natural)$$

Supposons par l'absurde que $s \neq s'$. Il existe $k \in [1..n]$ tel que $s_i = s'_i$ pour tout $i \leq k$ et $s_k \neq s'_k$. Alors

$$(\natural) \Leftrightarrow s_k \circ ... \circ s_n (y) = s'_k \circ ... \circ s'_n (z) .$$

Puisque $s_k \neq s'_k$, on aura par exemple $s_k = \tau_1$ et $s'_k = \tau_2$, et

$$\tau_1 (s_{k+1} \circ ... \circ s_n (y)) = \tau_2 \left(s'_{k+1} \circ ... \circ s'_n (z)\right) ,$$

ce qui est absurde puisque $s_{k+1} \circ ... \circ s_n (y) \in \mathcal{D}$ et $s'_{k+1} \circ ... \circ s'_n (z) \in \mathcal{D}$ entraînent

$$\tau_1 (s_{k+1} \circ ... \circ s_n (y)) \in \mathcal{D}_1 \quad \text{et} \quad \tau_2 \left(s'_{k+1} \circ ... \circ s'_n (z)\right) \in \mathcal{D}_2,$$

bien que $\mathcal{D}_1 \cap \mathcal{D}_2 = \emptyset$.

III.C.2. La question précédente montre que

$$s \neq s' \Rightarrow \gamma_s (\mathcal{D}) \cap \gamma_{s'} (\mathcal{D}) = \emptyset \Rightarrow s_1 \circ ... \circ s_n \neq s'_1 \circ ... \circ s'_n.$$

Toutes les composées $s_1 \circ ... \circ s_n$ sont distinctes entre elles lorsque les s_i sont choisies dans $\{\tau_1, \tau_2\}$. Il existe 2^n telles composées, et ces composées appartiennent toutes à $B_S (n)$. On a donc prouvé l'inégalité $2^n \leq |B_S (n)|$. Cette inégalité entraîne $2 \leq \lim_{n\to+\infty}(|B_S (n)|)^{\frac{1}{n}} = C_S$.

III.C.3. Le groupe $\mathfrak{I}_1$ est à croissance sous-exponentielle (**III.B.4**), donc $C_S = 1$ quelle que soit la partie finie symétrique S. Mais l'on vient d'exhiber une partie finie symétrique S pour laquelle $C_S \geq 2$. C'est absurde. Il n'existe donc aucune partie $\mathfrak{I}_1$-dédoublable de $\mathbb{R}$.

III.D. Si $\mathfrak{I}_2$ était à croissance sous-exponentielle, on pourrait raisonner comme en **III.C.3** pour montrer qu'aucune partie de $\mathbb{C}$ n'est $\mathfrak{I}_2$-dédoublable, contredisant alors la partie **II**. Ainsi $\mathfrak{I}_2$ est un groupe à croissance exponentielle

Partie IV : Un groupe paradoxal

IV.A.1. La matrice $T = \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix}$ est nilpotente et vérifie $T^2 = 0$. La formule du binôme de Newton (que l'on peut utiliser car I et T commutent entre eux) donne :

$$\forall k \in \mathbb{N} \quad A^k = (I + T)^k = I^k + kT = \begin{pmatrix} 1 & 2k \\ 0 & 1 \end{pmatrix} .$$

On constate que

$$\begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix} = I,$$

donc que $A^{-1} = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}$.
On utilisant à nouveau la formule du binôme comme précédemment pour calculer $(A^{-1})^{k'}$ si $k' \in \mathbb{N}$, on déduit alors sans peine que

$$\forall k \in \mathbb{Z}_- \quad A^k = \begin{pmatrix} 1 & 2k \\ 0 & 1 \end{pmatrix}.$$

En conclusion

$$\forall k \in \mathbb{Z} \quad A^k = \begin{pmatrix} 1 & 2k \\ 0 & 1 \end{pmatrix}.$$

De la même manière, on montrerait que

$$\forall k \in \mathbb{Z} \quad B^k = \begin{pmatrix} 1 & 0 \\ 2k & 1 \end{pmatrix}.$$

Remarque : On aurait aussi pu calculer A^k et B^k en raisonnant par récurrence. Attention : quatre raisonnements par récurrence sont nécessaires pour tout démontrer.

IV.A.2. Montrons seulement l'affirmation (1), la preuve de (2) étant du même genre.

$$A^k \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 & 2k \\ 0 & 1 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x + 2ky \\ y \end{pmatrix}$$

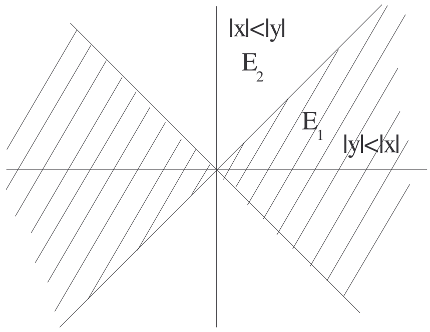
et il s'agit de prouver l'implication

$$\begin{pmatrix} x \\ y \end{pmatrix} \in E_2 \Rightarrow \begin{pmatrix} x + 2ky \\ y \end{pmatrix} \in E_1,$$

i.e. $(|x| < |y| \Rightarrow |y| < |x + 2ky|)$ $(\flat)$. Si $|x| < |y|$, on peut écrire

$$|x + 2ky| \geq ||x| - |2ky|| \geq |2ky| - |x| > |2ky| - |y| = (2\,|k| - 1)\,|y| \geq |y|$$

puisque $|k| \in \mathbb{N}^*$, et l'implication $(\flat)$ est prouvée.



IV.B.1. De façon générale, le sous-groupe engendré par deux éléments A et B est donnée par $\Gamma = < A, B > = \left\{A^{k_1}B^{l_1}...A^{k_m}B^{l_m} \,/\, m \in \mathbb{N} \quad k_i, l_i \in \mathbb{Z}\right\}$. Le tableau devient trivial compte tenu des notations choisies par l'énoncé.

IV.B.2.a. $U_3 = P_0M_0 = I$ entraîne $P_0 = M_0^{-1} \in (\Gamma_1 \cap \Gamma_2) \setminus \{I\}$, ce qui est absurde puisque aucune des matrices de la forme B^k ne peut s'écrire sous la forme A^l.

IV.B.2.b. On a $U_6X_2 = \Pi_s M_{s+1}X_2 = (M_1P_1)\ldots(M_sP_s)\,M_{s+1}X_2$, et de proche en proche (**IV.A.2**) :

$$\begin{aligned} X_2 \in E_2 \quad &\Rightarrow \quad M_{s+1}X_2 \in E_1 \\ &\Rightarrow \quad P_sM_{s+1}X_2 \in E_2 \\ &\Rightarrow \quad \ldots \Rightarrow U_6X_2 = (M_1P_1)\ldots(M_sP_s)\,M_{s+1}X_2 \in E_1. \end{aligned}$$

Cela prouve à fortiori que $U_6X_2 \neq X_2$, donc que $U_6 \neq I$.

IV.B.2.c. • $U_5 = P_0\Pi_r = P_0\,(M_1P_1)\ldots(M_rP_r)$. Si $M_{r+1} \in \Gamma_1 \setminus \{I\}$,

$$M_{r+1}^{-1}U_5M_{r+1} = (M_{r+1}^{-1}P_0)\,(M_1P_1)\ldots(M_rP_r)\,M_{r+1} = \Pi_{r+1}M_{r+1}.$$

$\Pi_{r+1}M_{r+1}$ est du type (6) donc différente de I d'après **IV.B.2.b**.
Donc $M_{r+1}^{-1}U_5M_{r+1} \neq I$, et cela entraîne $U_5 \neq I$.

• De même $U_4 = \Pi_n = (M_1P_1)\ldots(M_nP_n)$ donc

$$P_{n+1}^{-1}U_4P_{n+1} = P_{n+1}^{-1}\,(M_1P_1)\ldots(M_nP_nP_{n+1}) = P_{n+1}^{-1}\Pi'_n$$

est du type (5). Ainsi $P_{n+1}^{-1}U_4P_{n+1} \neq I$ d'où $U_4 \neq I$.

IV.B.2.d. $U_7 = P_0\Pi_tM_{t+1}$ donc

$$M_{t+2}^{-1}U_7M_{t+2} = M_{t+2}^{-1}P_0\Pi_tM_{t+1}M_{t+2} = \Pi_{t+1}\,(M_{t+1}M_{t+2})$$

est du type (6), donc $M_{t+2}^{-1}U_7M_{t+2} \neq I$ et $U_7 \neq I$.

IV.B.3.a.

$$\begin{aligned}\Pi_n = \Pi'_n \quad &\Leftrightarrow \quad \Pi'_n \Pi_n^{-1} = I \\ &\Leftrightarrow \quad \left(M'_1 P'_1\right) ... \left(M'_n P'_n\right) \left(P_n^{-1} M_n^{-1}\right) ... (P_1^{-1} M_1^{-1}) = I. \quad (*)\end{aligned}$$

Raisonnons par l'absurde. Supposons qu'il existe au moins un indice i tel que $M_i \neq M'_i$ ou $P_i \neq P'_i$. L'un au moins des deux maximums suivants existe alors :

$$j = \operatorname{Max}\left\{i \in [1..n] \ / \ P_i \neq P'_i\right\} \quad \text{ou} \quad k = \operatorname{Max}\left\{i \in [1..n] \ / \ M_i \neq M'_i\right\}.$$

Choisissons celui qui existe, disons j, et dans le cas où ils existeraient tous les deux, supposons (sans restreindre la généralité) que $j \geq k$. $(*)$ s'écrit alors

$$\left(M'_1 P'_1\right) ... (M'_j P'_j)((P_j^{-1} M_j^{-1} ... (P_1^{-1} M_1^{-1}) = I.$$

Le premier membre de cette égalité est du type (6), donc ne peut pas être égal à l'identité. C'est absurde.

IV.B.3.b. La question précédente montre que

$$\left(M'_1 P'_1\right) ... \left(M'_n P'_n\right) = (M_1 P_1) ... (M_n P_n) \Rightarrow (\forall i \quad M_i = M'_i \text{ et } P_i = P'_i),$$

et prouve qu'il existe au moins 2^{2n} éléments dans $B_S(2n)$. Donc

$$\left(2^{2n}\right)^{\frac{1}{2n}} \leq |B_S(2n)|^{\frac{1}{2n}}$$

et en passant à la limite,

$$2 \leq \lim_{n \to +\infty} |B_S(2n)|^{\frac{1}{2n}} = C_S.$$

Cela prouve que Γ est à croissance exponentielle. Le groupe $\mathrm{SL}_2(\mathbb{Z})$ le sera aussi d'après **III.A.4**.

IV.C.1. • Type (4) : $\Pi_n^k = I \Rightarrow \Pi_{kn} = I$, ce qui est absurde d'après **IV.B.2.c**.

• Type (7) : $(P_0 \Pi_t M_{t+1})^k = I \Rightarrow P_0 \Pi'_s M_{t+1} = I$, absurde d'après **IV.B.2.d**.

• Type (3) : $(P_0 M_0)^k = I \Rightarrow P_0 \Pi_s M_0 = I$, absurde d'après **IV.B.2.d**.

IV.C.2.a. Ici U est du type (6), i.e.

$$U = U_6 = \Pi_s M_{s+1} = (M_1 P_1) ... (M_s P_s) M_{s+1},$$

et vérifie $U_6^k = I$. Si $V_1 = M_{s+1} U_6 M_{s+1}^{-1}$, alors $V_1^k = M_{s+1} U_6^k M_{s+1}^{-1} = I$, soit

$$\begin{aligned}M_{s+1}\left[(M_1 P_1) ... (M_s P_s) M_{s+1}\right] ... \left[(M_1 P_1) ... (M_s P_s) M_{s+1}\right] M_{s+1}^{-1} &= I \\ \left[((M_{s+1} M_1) P_1)(M_2 P_2) ... (M_s P_s) M_{s+1}\right] ... \left[(M_1 P_1) ... (M_s P_s)\right] &= I.\end{aligned}$$

Si $M_{s+1}M_1 \neq I$, le premier membre de la dernière égalité est de la forme Π_n, donc du type (4), et ne peut jamais égaler l'identité d'après **IV.B.2.c**. Donc $M_{s+1}M_1 = I$. On prouverait de la même façon que $P_sP_1 = I$.

IV.C.2.b. Puisque $M_{s+1}M_1 = I$ et $P_sP_1 = I$, et puisque toutes les matrices qui interviennent sont inversibles (elles appartiennent toutes à $\mathrm{SL}_2(\mathbb{Z})$), on obtient $M_{s+1} = M_1^{-1}$ et $P_s = P_1^{-1}$. Donc

$$\begin{aligned} U_6 &= (M_1P_1)\ldots(M_sP_s)\,M_{s+1} \\ &= (M_1P_1)\,[(M_2P_2)\ldots(M_{s-1}P_{s-1})\,M_s]\,(M_1P_1)^{-1} \end{aligned}$$

et U_6 est semblable à $(M_2P_2)\ldots(M_{s-1}P_{s-1})\,M_s$, ce que nous noterons

$$U_6 \sim (M_2P_2)\ldots(M_{s-1}P_{s-1})\,M_s.$$

On continue :

$$U_6 \sim (M_2P_2)\ldots(M_{s-1}P_{s-1})\,M_s \sim (M_3P_3)\ldots(M_{s-2}P_{s-2})\,M_s \sim \ldots$$

Finalement, on obtient

$$U_6 \sim MPM' \quad \text{ou} \quad U_6 \sim M,$$

et une absurdité dans les deux cas. En effet, M^k est toujours distinctes de I. Quant à $(MPM')^k$, il suffit de recommencer le raisonnement de **IV.C.2.a** avec MPM' à la place de U_6 (c'est licite, puisque MPM' est du type (6)) pour obtenir $M' = M^{-1}$, donc $U_6 \sim MPM' \sim P$, puis de remarquer que P^k est toujours distinctes de I.

IV.C.3. Soit $U_5 = P_0\Pi_r = P_0\,(M_1P_1)\ldots(M_rP_r)$. Pour tout M du type (2),

$$MU_5M^{-1} = MP_0\,(M_1P_1)\ldots(M_rP_r)\,M^{-1} = \Pi_{r+1}M^{-1}$$

est du type (6). Puisque $U_5 \sim MU_5M^{-1}$, et qu'aucune matrice du type (6) n'est idempotente d'après **IV.C.2.b**, il en sera de même de U_5.

IV.C.4. Si U est d'ordre fini dans Γ, c'est-à-dire s'il existe un entier naturel non nul k tel que $U^k = I$, nous venons de voir que U n'est pas du type (3), (4), (5), (6), (7). Comme U ne peut pas être du type (1) ou (2) (puisque A^k ou B^k vaut l'identité si et seulement si $k = 0$: c'est le calcul des matrices A^k et B^k fait en **IV.A.1** qui nous le montre), on aura nécessairement $U = I$.

IV.D. Notons simplement (0) la partie formée par les matrices de type (0), etc. Le tableau ci-dessous nous montre l'action de la multiplication par A ou B sur chacun des types (0) à (7) de matrices. Commentons par exemple la cinquième colonne. Une matrice Π du type (4) multipliée à gauche par A donne $A\Pi = A\,(M_1P_1)\,...\,(M_nP_n)$ et pour $M_1 = A^{-1}$, on obtient une matrice du type $P_1\,(M_2P_2)\,...\,(M_nP_n) = P\Pi$, c'est-à-dire du type (5), ou encore une matrice du type $A\left(A^{-1}P_1\right) = P_1$ du type (1).

(0) I	(1) P	(2) M	(3) PM	(4) Π	(5) PΠ	(6) ΠM	(7) PΠM	
		AM donne I (0)		A(MP)... donne IP(MP)... (5) ou A(MP)=P (1)		AΠM donne PΠM (7) ou PM (3)		A
	BP donne I (0)		BPM donne M (2)		BPΠ donne Π (4)		BPΠM donne ΠM (6)	B

Mais ce tableau ne suffit pas pour conclure : nos tentatives pour obtenir quatre parties disjointes sont des échecs. Nous sommes obligés d'affiner l'action de A et de partager nos classes de matrices en deux. Prenons par exemple les matrices du type (2). Ces matrices sont de la forme $M = A^k$ avec $k \in \mathbb{N}^*$. Notons $(2)_+$ l'ensemble des matrices du type A^k avec $k > 0$ et $(2)\_$ celui formé par les matrices du type A^k avec $k < 0$. On remarque que

$$A\,(2)\_ = \{A^{k+1}\,/\,k<0\} = \{...,A^{-2},A^{-1},I\} = (2)\_ \cup (0)\,.$$

L'action de A sur $(2)\_$ continue de nous fournir les matrices du type (0), et nous offre toutes les matrices du type $(2)\_$. De la même façon, on définit

$$\begin{aligned}(4)\_ &= \{\Pi\,/\,\Pi = (A^kP_1)(M_2P_2)\,...(M_nP_n) \text{ avec } k<0\},\\ (6)\_ &= \{\Pi M\,/\,\Pi M = (A^kP_1)(M_2P_2)\,...(M_nP_n)M \text{ avec } k<0\},\end{aligned}$$

et les parties $(4)_+$ et $(6)_+$ correspondantes. On a

$$\begin{aligned}A\,(4)\_ &= (1)\cup(5)\cup(4)\_\,,\\ A\,(6)\_ &= (3)\cup(7)\cup(6)\_\,.\end{aligned}$$

On recommence avec des ensembles adaptés à la multiplication par B. On pose

$$\begin{aligned}
(1)_- &= \{P \,/\, P = B^k \text{ avec } k < 0\},\\
(3)_- &= \{PM \,/\, PM = B^k M \text{ avec } k < 0\},\\
(5)_- &= \{P\Pi \,/\, P\Pi = B^k \Pi \text{ avec } k < 0\},\\
(7)_- &= \{P\Pi M \,/\, P\Pi M = B^k \Pi M \text{ avec } k < 0\},
\end{aligned}$$

et bien entendu $(1)_+ = (1) \setminus (1)_-$, $(3)_+ = (3) \setminus (3)_-$, $(5)_+ = (5) \setminus (5)_-$et $(7)_+ = (7) \setminus (7)_-$. Le tableau ci-dessous récapitule les actions de A et B sur ces différents types de matrices. La première colonne donne le type de matrice T, la seconde et la troisième les types de matrices AT et BT obtenues.

Matrice T du type :	AT	BT
$(1)_-$		$(0) \cup (1)_-$
$(2)_-$	$(0) \cup (2)_-$	
$(3)_-$		$(2) \cup (3)_-$
$(4)_-$	$(1) \cup (5) \cup (4)_-$	
$(5)_-$		$(4) \cup (5)_-$
$(6)_-$	$(3) \cup (7) \cup (6)_-$	
$(7)_-$		$(6) \cup (7)_-$

Les ensembles $\mathcal{Q}_1$, $\mathcal{Q}_2$, $\mathcal{R}_1$, $\mathcal{R}_2$ sont définis dans le tableau ci-dessous :

$\mathcal{Q}_1 = (2)_+ \cup (4)_+ \cup (6)_+$	$\mathcal{Q}_2 = (2)_- \cup (4)_- \cup (6)_-$
$\mathcal{R}_1 = (1)_+ \cup (3)_+ \cup (5)_+ \cup (7)_+$	$\mathcal{R}_2 = (1)_- \cup (3)_- \cup (5)_- \cup (7)_-$

et l'on obtient

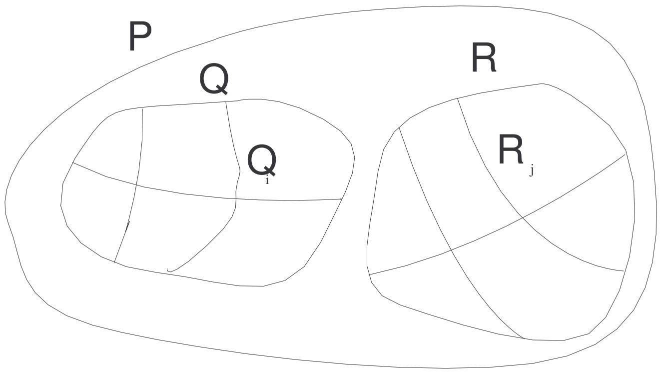
$A\mathcal{Q}_2 = (0) \cup (2)_- \cup (1) \cup (5) \cup (4)_- \cup (3) \cup (7) \cup (6)_-$
$B\mathcal{R}_2 = (0) \cup (1)_- \cup (2) \cup (3)_- \cup (4) \cup (5)_- \cup (6) \cup (7)_-$

On a bien $\Gamma = \mathcal{Q}_1 \cup A\mathcal{Q}_2 = \mathcal{R}_1 \cup B\mathcal{R}_2$, et les parties $\mathcal{Q}_1$, $\mathcal{Q}_2$, $\mathcal{R}_1$, $\mathcal{R}_2$ sont non vides et deux à deux disjointes.

Partie V : Ensembles G-paradoxaux

V.A.1. L'ensemble $\mathcal{P}$ est G-paradoxal s'il contient deux parties non vides et disjointes $\mathcal{Q}$ et $\mathcal{R}$, chacune d'elle pouvant être découpée en un nombre fini de morceaux $\mathcal{Q}_i$ et $\mathcal{R}_j$ puis réarrangée sous l'action de G pour redonner $\mathcal{P}$.
Le groupe Γ agit sur lui-même grâce à sa multiplication, autrement dit si $M \in \Gamma$ et $N \in \Gamma$, on pose $M \star N = MN$. Avec cette définition, le découpage

de la question **IV.D** montre que Γ est Γ-paradoxal : on prend $\mathcal{Q} = \mathcal{Q}_1 \cup \mathcal{Q}_2$, $\mathcal{R} = \mathcal{R}_1 \cup \mathcal{R}_2$, et l'on a $\Gamma = \mathcal{Q}_1 \cup (A \star \mathcal{Q}_2) = \mathcal{R}_1 \cup (B \star \mathcal{R}_2)$.



V.A.2. Le sous-groupe G de $\mathfrak{S}_E$ opère sur E de façon canonique en posant

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

Si $\mathcal{D}$ est une partie G-dédoublable de E, il existe deux parties $\mathcal{D}_1$, $\mathcal{D}_2$ disjointes et non vides de E telles que :

- $\mathcal{D} = \mathcal{D}_1 \cup \mathcal{D}_2$ (réunion disjointe),
- $\exists g_1, g_2 \in G \quad g_1(\mathcal{D}) = \mathcal{D}_1$ et $g_2(\mathcal{D}) = \mathcal{D}_2$.

Par conséquent $\mathcal{D} = g_1^{-1}(\mathcal{D}_1) = g_2^{-1}(\mathcal{D}_2)$ et $\mathcal{D}$ est G-paradoxale (la partition de $\mathcal{D}_i$ utilisée ici pour satisfaire la définition d'un ensemble G-paradoxal donnée au début de la partie **V** est réduite à sa plus simple expression : c'est $\{\mathcal{D}_i\}$).

V.A.3. Si $x \in E$, il existe un ensemble T tel que l'intersection de T avec chacune des Γ-orbites $\mathcal{O}_x = \{U \star x \,/\, U \in \Gamma\}$, x parcourant E, soit réduite à un singleton (le problème nous demande d'admettre l'existence de cet ensemble T, autrement le recours à l'axiome du choix est indispensable). On a

$$E = \Gamma \star T. \quad (1)$$

En effet, l'inclusion $\Gamma \star T \subset E$ est triviale, et réciproquement, si $x \in E$, alors $\mathcal{O}_x \cap T = \{y_x\}$ est un singleton, et il existe $U \in \Gamma$ tel que $U \star x = y_x$, ce qui entraîne $x = U^{-1} \star y_x \in \Gamma \star T$.

Reprenons les notations du IV.D, et notons $\mathcal{Q}_1$, $\mathcal{Q}_2$, $\mathcal{R}_1$, $\mathcal{R}_2$ des parties de Γ non vides et deux à deux disjoints, telles que

$$\Gamma = \mathcal{Q}_1 \cup (A \star \mathcal{Q}_2) = \mathcal{R}_1 \cup (B \star \mathcal{R}_2).$$

Introduisons les quatre parties suivantes de E :

$$\mathcal{Q}_1 \star T, \quad \mathcal{Q}_2 \star T, \quad \mathcal{R}_1 \star T, \quad \text{et} \quad \mathcal{R}_2 \star T. \quad (2)$$

Lemme : Les quatre parties énumérées en (2) sont disjointes deux à deux.

Preuve du Lemme : Montrons seulement que $(\mathcal{Q}_1 \star T) \cap (\mathcal{Q}_2 \star T) = \varnothing$, les autres intersections se traitant de la même façon. S'il existait $(t_1, t_2) \in T^2$ et $(U_1, U_2) \in \mathcal{Q}_1 \times \mathcal{Q}_2$ tels que

$$U_1 \star t_1 = U_2 \star t_2,$$

on aurait $(U_2^{-1}U_1) \star t_1 = t_2$. Mais alors t_1 et t_2 seraient des éléments de T situés dans la même orbite, donc $t_1 = t_2$. Ainsi

$$(U_2^{-1}U_1) \star t_1 = t_1$$

et l'on peut utiliser l'hypothèse

$$\forall U \in \Gamma \backslash \{I\} \quad \forall x \in E \quad U \star x \neq x$$

(qui s'interprète en disant que "l'action de groupe n'admet aucun point fixe") pour obtenir $U_2^{-1}U_1 = I$, donc $U_1 = U_2$. C'est absurde car $\mathcal{Q}_1$ et $\mathcal{Q}_2$ sont disjoints. ■

Finalement

$$\Gamma = \mathcal{Q}_1 \cup (A \star \mathcal{Q}_2) = \mathcal{R}_1 \cup (B \star \mathcal{R}_2).$$

entraîne (par (1) et le Lemme précédent) :

$$\begin{aligned} E = \Gamma \star T &= (\mathcal{Q}_1 \star T) \cup (A \star (\mathcal{Q}_2 \star T)) \\ &= (\mathcal{R}_1 \star T) \cup (B \star (\mathcal{R}_2 \star T)) \end{aligned}$$

(unions disjointes). L'ensemble E est donc paradoxal, comme on le voit en prenant les deux parties

$$\mathcal{Q} = (\mathcal{Q}_1 \star T) \cup (\mathcal{Q}_2 \star T) \quad \text{et} \quad \mathcal{R} = (\mathcal{R}_1 \star T) \cup (\mathcal{R}_2 \star T)$$

et en choisissant $g_1 = h_1 = I$, $g_2 = A$ et $h_2 = B$ (avec les notations de la définition d'un ensemble paradoxal donnée au début de la partie V).

V.B.1. • L'application $h_M : H^2 \to H^2$ est bien définie. Pour le voir, il s'agit de prouver deux choses :

- premièrement, que le dénominateur $cx + d$ ne s'annule jamais lorsque x décrit H^2. C'est vrai, parce que $\operatorname{Im} x > 0$ et que c et d sont des réels (si $c \neq 0$,

$\operatorname{Im}(cx+d) = c \operatorname{Im} x \neq 0$ donc $cx+d \neq 0$, et si $c=0$, nécessairement $d \neq 0$ puisque $\det M = 1$, et le problème ne se pose pas).

- deuxièmement, que $h_M(x)$ appartient à H^2 pour tout x appartenant à H^2. On a

$$\begin{aligned}
\operatorname{Im}(h_M(x)) &= \operatorname{Im}\left(\frac{ax+b}{cx+d}\right) = \operatorname{Im}\left(\frac{(ax+b)(c\overline{x}+d)}{|cx+d|^2}\right) \\
&= \operatorname{Im}\left(\frac{bc\overline{x}+adx}{|cx+d|^2}\right) = \frac{(ad-bc)\operatorname{Im} x}{|cx+d|^2} = \frac{\operatorname{Im} x}{|cx+d|^2}, \quad (*)
\end{aligned}$$

donc $\operatorname{Im} x > 0$ entraîne $\operatorname{Im}(h_M(x)) > 0$, et le résultat est montré.

• Montrons maintenant que $h_M : H^2 \to H^2$ est bijective. Pour tout $y \in H^2$,

$$\begin{aligned}
h_M(x) = y &\Leftrightarrow \frac{ax+b}{cx+d} = y \\
&\Leftrightarrow ax+b = cxy+dy \\
&\Leftrightarrow x(a-cy) = dy-b \\
&\Leftrightarrow x = \frac{dy-b}{-cy+a},
\end{aligned}$$

où l'on a pu diviser par $-cy+a$ puisque $-cy+a \neq 0$ (toujours le même raisonnement : si $c \neq 0$, $-cy+a \neq 0$ car $\operatorname{Im} y > 0$ et $c, a \in \mathbb{Z}$, et si $c=0$, $a \neq 0$ car $\det M = 1$). Pour conclure, il reste seulement à vérifier que x appartient bien à H^2. Ce sont les égalités $(*)$ qui nous donnent la solution. En effet, $x = \frac{dy-b}{-cy+a}$ si et seulement si $h_M(x) = y$, et d'après $(*)$: $\operatorname{Im} y > 0$ entraîne $\operatorname{Im} x > 0$, soit $x \in H^2$.

Remarque : On a prouvé que $h_M^{-1} = h_{M^{-1}}$, ce qui ne nous surprendra pas puisque $M \mapsto h_M$ est un morphisme de groupes.

V.B.2.a. Notons

$$\begin{array}{rccc}
\varphi : & \mathrm{SL}_2(\mathbb{Z}) & \to & \mathfrak{S}_{H^2} \\
& M & \mapsto & h_M
\end{array}$$

le morphisme admis par l'énoncé. On a

$$\begin{aligned}
M \in \operatorname{Ker}\varphi &\Leftrightarrow h_M = Id_{H^2} \\
&\Leftrightarrow \forall x \in H^2 \quad h_M(x) = x \\
&\Leftrightarrow \forall x \in H^2 \quad \frac{ax+b}{cx+d} = x \\
&\Leftrightarrow \forall x \in H^2 \quad cx^2 + (d-a)x - b = 0. \quad (*)
\end{aligned}$$

$(*)$ signifie que le polynôme $cx^2 + (d-a)x - b$ à coefficients réels admet une infinité de racines, et l'on en déduit qu'il est nul. Ainsi $b = c = 0$ et $a = d$.

Comme $ad - bc = 1$, on obtient $a = \pm 1$, et $h_M = \pm Id$. La réciproque étant triviale, on peut conclure à $\operatorname{Ker}\varphi = \{\pm Id\}$.

V.B.2.b. Soit $\widetilde{\varphi} = \varphi|_\Gamma : \Gamma \to \varphi(\Gamma) = \overline{\Gamma}$ la restriction de φ à Γ, où l'on a aussi restreint l'ensemble d'arrivée. $\widetilde{\varphi}$ est toujours un morphisme de groupes, surjectif par construction. Pour vérifier qu'il est injectif, il faut rappeler que les seules matrices M possibles pouvant appartenir à $\operatorname{Ker}\widetilde{\varphi}$ sont celles de $\operatorname{Ker}\varphi$, autrement dit $\pm Id$, et que $-Id$ n'appartient pas à Γ d'après la description de ce groupe donné à la question **IV.B.1**. Ainsi $\operatorname{Ker}\widetilde{\varphi} = \{Id\}$ et $\widetilde{\varphi}$ est injective.

V.B.3.a. On a

$$h_M(x) = x \Leftrightarrow \frac{ax+b}{cx+d} = x \Leftrightarrow cx^2 + (d-a)x - b = 0. \quad (*)$$

• Si $c \neq 0$, le discriminant du trinôme intervenant dans $(*)$ vaut

$$\Delta = (d-a)^2 + 4bc = (d-a)^2 + 4(ad-1) = (a+d)^2 - 4 = (\operatorname{Tr}(M))^2 - 4.$$

$\triangleright$ Si $\Delta \geq 0$, l'équation $(*)$ admet une ou deux solutions réelles, donc hors de H^2.

$\triangleright$ Si $\Delta < 0$, c'est-à-dire si $|\operatorname{Tr}(M)| < 2$, l'équation $(*)$ admet deux solutions complexes (non réelles) conjuguées, et l'une d'entre elle appartient nécessairement au demi-plan H^2. On peut donc conclure :

(α) Si $c \neq 0$, h_M admet au moins un point fixe dans H^2 si et seulement si $|\operatorname{Tr}(M)| < 2$.

• Si $c = 0$, $ad = 1$ et

$$\begin{aligned} h_M(x) = x \quad &\Leftrightarrow \quad (d-a)x - b = 0 \\ &\Leftrightarrow \quad (d-a)x = b \quad (**) \end{aligned}$$

$\triangleright$ Si $a = d$ et $b = 0$, tous les points de H^2 sont invariants par h_M, et $h_M = Id$.
$\triangleright$ Si $a = d$ et $b \neq 0$, h_M n'admet aucun point fixe.
$\triangleright$ Si $a \neq d$, h_M admet un unique point fixe d'affixe $b/(d-a)$, qui n'appartient pas à H^2.

En conclusion :

(β) Si $c = 0$, h_M admet au moins un point fixe dans H^2 si et seulement si $h_M = Id$.

Les assertions (α) et (β) montrent que h_M admet au moins un point fixe dans H^2 si et seulement si $|\operatorname{Tr}(M)| < 2$ ou bien $h_M = Id$.

V.B.3.b. Si $h_M = Id$, le résultat annoncé est trivial. Supposons donc h_M distinct de Id. Par hypothèse $|\operatorname{Tr}(M)| = |d-a| < 2$. Comme a et d sont entiers, on aura $d-a \in \{-1,0,1\}$, donc

$$\frac{d-a}{2} \in \left\{-\frac{1}{2}, 0, \frac{1}{2}\right\}.$$

Il existe un réel θ tel que $\cos\theta = \frac{d-a}{2}$, et l'on sait que l'on peut choisir θ dans l'ensemble $\left\{\frac{\pi}{3}, \frac{\pi}{2}, \frac{2\pi}{3}\right\}$. Le polynôme caractéristique de la matrice M est

$$\begin{aligned}\chi_M(X) &= X^2 - \operatorname{Tr}(M)\,X + \det M \\ &= X^2 - 2\cos\theta X + 1 = (X - e^{i\theta})(X - e^{-i\theta}),\end{aligned}$$

donc M admet deux valeurs propres distinctes dans $\mathbb{C}$. Cela montre que M est diagonalisable, et semblable à la matrice $\begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta}\end{pmatrix}$.
Comme

$$\theta \in \left\{\frac{\pi}{3}, \frac{\pi}{2}, \frac{2\pi}{3}\right\},$$

cela entraîne $M^k = I$ avec $k = 3$, 4 ou 6. Finalement, on a trouvé un entier naturel k non nul tel que $M^k = I$, et puisque $M \mapsto h_M$ est un morphisme de groupes, on en déduit $h_{M^k} = h_M^k = Id$ et donc que h_M est un élément d'ordre fini de $\mathfrak{S}_{H^2}$.

V.B.4. L'isomorphisme de groupes $\widetilde{\varphi} : \Gamma \to \overline{\Gamma}$ introduit en **V.B.2.b** applique les éléments d'ordres finis de Γ sur les éléments d'ordres finis de $\overline{\Gamma}$ (et conserve leurs ordres). On a vu que I était le seul élément d'ordre fini de Γ (**IV.C**), et l'on peut donc affirmer que $\widetilde{\varphi}(I) = Id$ est le seul élément d'ordre fini de $\overline{\Gamma}$.
Cela étant, considérons un élément h_M de $\overline{\Gamma} \setminus \{Id\}$. Si h_M possédait un point fixe, h_M serait d'ordre fini d'après **V.B.3**, ce qui est absurde.

V.B.5. On considère l'opération de Γ sur H^2 :

$$\begin{array}{ccc} \Gamma \times H^2 & \to & H^2 \\ (M,x) & \mapsto & M \star x = h_M(x). \end{array}$$

D'après **V.B.4**, cette action de groupes n'ademt pas de points fixes, et la question **V.A.3** montre que H^2 est paradoxal.

V.C.1. Avant de commencer, notons qu'avec la notation h_M héritée de la partie **V.B**,

$$\begin{array}{cccc} \gamma_U : & \mathbb{R}^2 & \to & \mathbb{R}^2 \\ & p & \mapsto & U \star p = h_U(p), \end{array}$$

si bien que l'on puisse écrire $\gamma_U = h_U$ et $\Gamma_g = \{\gamma_U \,/\, U \in \Gamma\} = \{h_U \,/\, U \in \Gamma\}$.
Soient $\gamma \in \Gamma_g$ et $p, q \in \mathbb{R}^2$. Il existe $U \in \Gamma$ tel que $\gamma = \gamma_U = h_U$. Il s'agit de prouver l'implication

$$p \sim q \Rightarrow \gamma_U\,(p) \sim \gamma_U\,(q)$$

c'est-à-dire, en notant $p = (x, y)$ et $q = (x', y')$,

$$\left(x - x', y - y'\right) \in \mathbb{Z}^2 \Rightarrow (ax + by - (ax' + by'), cx + dy - (cx' + dy')) \in \mathbb{Z}^2.$$

L'implication est triviale puisque $ax + by - (ax' + by') = a(x - x') + b(y - y')$ est un entier comme une somme de produits d'entiers, la seconde coordonnée se traitant de la même façon.

V.C.2. ▶ Si $\gamma \in \Gamma_g = \{\gamma_U \,/\, U \in \Gamma\}$, on pose

$$\begin{array}{cccc} \widehat{\gamma}: & \Delta & \to & \Delta \\ & p & \mapsto & \widehat{\gamma\,(p)} \end{array}$$

où $\widehat{\gamma\,(p)}$ représente l'unique élément de Δ dans la classe de $\gamma\,(p)$ pour la relation γ. Autrement dit $\widehat{\gamma\,(p)} \in \Delta$ et $\widehat{\gamma\,(p)} \sim \gamma\,(p)$.
Pour tous $\gamma_1, \gamma_2 \in \Gamma_g$ et pour tout $p \in \Delta$,

$$\widehat{\gamma}_1 \circ \widehat{\gamma}_2\,(p) = \widehat{\gamma}_1\,[\widehat{\gamma}_2\,(p)] = \widehat{\gamma}_1\,(q) = r$$

avec $q \in \Delta$ et $q \sim \gamma_2\,(p)$, mais aussi $r \in \Delta$ et $r \sim \gamma_1\,(q)$. On a aussi

$$\widehat{\gamma_1 \circ \gamma_2}\,(p) = s \text{ où } s \in \Delta \text{ et } s \sim \gamma_1 \circ \gamma_2\,(p)\,.$$

Comme

$$q \sim \gamma_2\,(p) \overset{\textbf{V.C.1}}{\Rightarrow} \gamma_1\,(q) \sim \gamma_1 \circ \gamma_2\,(p) \Rightarrow r \sim s,$$

et comme

$$\left.\begin{array}{l} r \sim s \\ r, s \in \Delta \end{array}\right\} \Rightarrow r = s \Rightarrow \widehat{\gamma}_1 \circ \widehat{\gamma}_2\,(p) = \widehat{\gamma_1 \circ \gamma_2}\,(p)\,,$$

on a prouvé que

$$\forall p \in \Delta \quad \widehat{\gamma}_1 \circ \widehat{\gamma}_2\,(p) = \widehat{\gamma_1 \circ \gamma_2}\,(p)$$

autrement dit, que $\widehat{\gamma}_1 \circ \widehat{\gamma}_2 = \widehat{\gamma_1 \circ \gamma_2}$.
On en déduit

$$\forall \gamma \in \Gamma_g \quad \widehat{\gamma} \circ \widehat{\gamma^{-1}} = \widehat{Id_{\mathbb{R}^2}} = Id_\Delta = \widehat{\gamma^{-1}} \circ \widehat{\gamma}$$

et cela prouve que $\widehat{\gamma} \in \mathfrak{S}_\Delta$, et que $\widehat{\gamma}^{-1} = \widehat{\gamma^{-1}}$. L'application

$$\begin{array}{cccc} \Theta: & (\Gamma_g, \circ) & \to & (\mathfrak{S}_\Delta, \circ) \\ & \gamma & \mapsto & \widehat{\gamma} \end{array}$$

est donc bien définie, et c'est un morphisme de groupes.

▶ Montrons que Θ est injectif. Supposons que $\widehat{\gamma} = Id_\Delta$. Alors

$$\forall p \in \Delta \quad \gamma(p) \sim p.$$

De deux choses l'une :

a) Ou bien $\gamma(\Delta) \subset \Delta$, et l'application linéaire γ laisse fixe tous les points de Δ, donc à fortiori une base de $\mathbb{R}^2$, et l'on a $\gamma = Id_{\mathbb{R}^2}$.

b) Ou bien $\gamma(\Delta)$ n'est pas inclus dans Δ, et le parallélogramme $\gamma(\Delta)$ rencontre forcément au moins un carré C de $\mathbb{R}^2$ du type $C = [k, k+1[\times[l, l+1[$ (où $k, l \in \mathbb{N}$) suivant un polygone non aplati $P = \gamma(\Delta) \cap C$. Dans ce cas, il existe une translation t de vecteur dans $\mathbb{Z}^2$ telle que $t(P) \subset \Delta$, et

- $P' = \gamma^{-1}(P)$ est un polygone non aplati inclus dans Δ,

- $\widehat{\gamma}$ et $t \circ \gamma$ coïncident sur P' (cela provient de la définition de $\widehat{\gamma}$ via la relation d'équivalence $\sim$).

Puisque $\widehat{\gamma} = Id_\Delta$, on en déduit que l'application affine $t \circ \gamma$ admet au moins trois points fixes non alignés (dans P'), et donc que $t \circ \gamma = Id_{\mathbb{R}^2}$. Par suite $\gamma = t^{-1}$, et $\gamma = Id_{\mathbb{R}^2}$ (puisque γ est linéaire).

V.C.3. Θ définit une bijection de Γ_g sur son image $\Theta(\Gamma_g) = \widehat{\Gamma_g}$, donc tout revient à prouver que Γ_g est dénombrable. L'application $U \mapsto \gamma_U$ est une surjection de Γ sur $\Gamma_g = \{\gamma_U \,/\, U \in \Gamma\}$ (en fait une bijection, mais on peut s'en passer), donc il suffit de prouver que le sous-groupe Γ de $\mathrm{SL}_2(\mathbb{Z})$ engendré par les matrices A et B est dénombrable pour conclure à la dénombrabilité de Γ_g et de $\widehat{\Gamma_g}$.

Posons $S = \{A, A^{-1}, B, B^{-1}\}$ et notons $B_S(n) = \{U \in \Gamma \,/\, l_S(U) \leq n\}$ comme en **III.A**. Puisque

$$\Gamma = \bigcup_{n \in \mathbb{N}} B_S(n),$$

l'ensemble Γ est dénombrable comme une réunion dénombrable d'ensembles dénombrables.

V.C.4.a. L'ensemble $\bigcup_{n\in\mathbb{N}}(C_0 \cap \mathcal{D}_n)$ est une réunion dénombrable d'ensembles finis (puisqu'une droite coupe un cercle en au plus deux points). C'est donc un ensemble au plus dénombrable qui ne peut, en aucun cas, coïncider avec le cercle C_0 qui, lui, n'est ni fini, ni dénombrable (si s désigne un point de C_0 et si T désigne la tangente à C_0 issue du point de C_0 diamétralement opposé à s, la projection stéréographique π qui au point m de $C_0 \backslash \{s\}$ fait correspondre l'intersection des droites (sm) et T, est bijective, et montre que

$C_0\backslash\{s\}$ est équipotent à $\mathbb{R}$, et par conséquent que C_0 n'est certainement pas dénombrable !).

V.C.4.b. On a

$$F=\left\{p\in\Delta\,/\,\exists\widehat{\gamma}\in\widehat{\Gamma_g}\backslash\{Id\}\quad\widehat{\gamma}(p)=p\right\}=\bigcup_{\gamma\in\Gamma_g\backslash\{Id\}}\mathrm{Fix}\,(\widehat{\gamma})$$

où $\mathrm{Fix}\,(\widehat{\gamma})=\{p\in\Delta\,/\,\widehat{\gamma}(p)=p\}$ désigne l'ensemble des points fixes de $\widehat{\gamma}$. On peut écrire :

$$p\in\mathrm{Fix}\,(\widehat{\gamma})\Leftrightarrow\left\{\begin{array}{l}\widehat{\gamma}(p)=p\\ p\in\Delta\end{array}\right.\Leftrightarrow\left\{\begin{array}{l}\gamma(p)\sim p\\ p\in\Delta\end{array}\right.\Leftrightarrow\left\{\begin{array}{l}(\gamma-Id)(p)\in\mathbb{Z}^2\\ p\in\Delta\end{array}\right.$$

d'où

$$\mathrm{Fix}\,(\widehat{\gamma})=\left((\gamma-Id)^{-1}\left(\mathbb{Z}^2\right)\right)\cap\Delta.$$

L'application $\gamma-Id$ est un endomorphisme de $\mathbb{R}^2$ distinct de l'identité, donc $\dim\mathrm{Ker}\,(\gamma-Id)=0$ ou 1. On envisage les deux cas :

▶ Si $\mathrm{Ker}\,(\gamma-Id)=\{0\}$, $\gamma-Id$ est un automorphisme de $\mathbb{R}^2$ et l'image réciproque $(\gamma-Id)^{-1}\left(\mathbb{Z}^2\right)$ est équipotente à $\mathbb{Z}^2$.

▶ Si $\dim\mathrm{Ker}\,(\gamma-Id)=1$, $\mathrm{Ker}\,(\gamma-Id)$ est une droite vectorielle D^γ, et pour tout $p\in\mathbb{Z}^2$, l'image réciproque $(\gamma-Id)^{-1}(\{p\})$ est une droite affine D^γ_p de direction D^γ, et

$$(\gamma-Id)^{-1}\left(\mathbb{Z}^2\right)=\bigcup_{p\in\mathbb{Z}^2}D^\gamma_p.$$

Ainsi

$$F=\bigcup_{\gamma\in\Gamma_g\backslash\{Id\}}\mathrm{Fix}\,(\widehat{\gamma})=\bigcup_{\gamma\in\Gamma_g\backslash\{Id\}}\left((\gamma-Id)^{-1}\left(\mathbb{Z}^2\right)\right)\cap\Delta=F_0\cup F_1$$

où

$$F_0=\bigcup_{\substack{\gamma\in\Gamma_g\backslash\{Id\}\\ \text{et }\ \mathrm{Ker}(\gamma-Id)=\{0\}}}\left((\gamma-Id)^{-1}\left(\mathbb{Z}^2\right)\cap\Delta\right)$$

est au plus dénombrable comme une réunion au plus dénombrable (Γ_g est dénombrable d'après **V.C.3**) d'ensembles au plus dénombrables, et où

$$F_1=\bigcup_{\substack{\gamma\in\Gamma_g\backslash\{Id\}\\ \text{et }\ \dim\mathrm{Ker}(\gamma-Id)=1}}\ \bigcup_{p\in\mathbb{Z}^2}\left(D^\gamma_p\cap\Delta\right).$$

On en déduit

$$C_0\cap F=(C_0\cap F_0)\cap(C_0\cap F_1)$$

L'ensemble $C_0 \cap F_0$, inclus dans F_0 au plus dénombrable, est au plus dénombrable. Puisque $C_0 \subset \Delta$, on a

$$C_0 \cap F_1 = \bigcup_{\substack{\gamma \in \Gamma_g \backslash \{Id\} \\ \text{et } \dim \operatorname{Ker}(\gamma - Id) = 1}} \bigcup_{p \in \mathbb{Z}^2} \left(C_0 \cap D_p^\gamma\right)$$

et chaque ensemble $C_0 \cap D_p^\gamma$ est au plus dénombrable d'après **V.C.4.a**. Par suite $C_0 \cap F_1$ est au plus dénombrable comme réunion dénombrable d'ensembles au plus dénombrables. Finalement $C_0 \cap F$ est au plus dénombrable, et

$$\left.\begin{array}{l} C_0 \cap F \text{ au plus dénombrable} \\ C_0 \text{ ni fini, ni dénombrable} \end{array}\right\} \Rightarrow C_0 \cap F \subsetneq C_0.$$

V.C.5. Si l'intérieur de F n'était pas vide, il existerait une boule ouverte de rayon strictement positif incluse dans F. A fortiori, il existerait alors un cercle C_0 inclus dans cette boule, et donc aussi dans F, en contradiction avec la question **V.C.4.b**.

V.C.6. ▶ Puisque F est d'intérieur vide, F est strictement inclus dans Δ et la partie $\mathcal{P} = \Delta \backslash F$ n'est pas vide. La partie $\mathcal{P}$ est bornée puisque incluse dans Δ, qui est borné. On peut considérer l'action du groupe Γ sur Δ définie par

$$\begin{array}{lcl} \Gamma \times \Delta & \to & \Delta \\ (U, p) & \mapsto & U \star p = \widehat{\gamma}_U(p). \end{array}$$

Cette action est bien définie, puisque l'application

$$\begin{array}{lcl} (\Gamma, \times) & \to & (\mathfrak{S}_\Delta, \circ) \\ U & \mapsto & \widehat{\gamma}_U \end{array}$$

est un homomorphisme de groupes comme la composée des deux homomorphismes

$$\begin{array}{lcl} (\Gamma, \times) & \to & (\Gamma_g, \circ) \\ U & \mapsto & \gamma_U \end{array} \quad \text{et} \quad \begin{array}{lcl} (\Gamma_g, \circ) & \to & (\mathfrak{S}_\Delta, \circ) \\ \gamma & \mapsto & \widehat{\gamma}. \end{array}$$

▶ Montrer que le groupe Γ opère sur $\mathcal{P}$ revient à prouver que $\mathcal{P}$ est stable sous l'action de Γ que l'on vient de définir, c'est-à-dire

$$\forall p \in \mathcal{P} \quad \forall U \in \Gamma \quad U \star p \in \mathcal{P}.$$

On raisonne par l'absurde. S'il existe $p \in \mathcal{P}$ et $U \in \Gamma$ tels que $U \star p \in F$, il existe $V \in \Gamma \backslash \{I\}$ tel que $\widehat{\gamma}_V(U \star p) = U \star p$. Par suite $V \star (U \star p) = U \star p$, donc $\left(U^{-1}VU\right) \star p = p$ et $p \in \operatorname{Fix}(\widehat{\gamma}_{U^{-1}VU})$. Puisque $p \in \mathcal{P}$, cela entraîne $U^{-1}VU = I$, donc $V = I$, ce qui est absurde.

▶ Finalement Γ opère sur $\mathcal{P}$, et par construction, cette action de groupe ne possède aucun point fixe. La question **V.A.3** nous montre alors que $\mathcal{P}$ est Γ-paradoxale.

That's all, Folks !

Quelques réflexions au sujet de l'épreuve :

La question **V.A.3** et les questions **V.C.2** à **V.C.6** étaient trop difficiles, qu'on les cherche en temps limité ou non.

Le rapport du jury concernant cette agrégation interne indique qu'aucun des candidats n'a effectivement abordé la cinquième partie. Il précise que "les candidats ont essentiellement traité les Parties I, II, III-A et IV" et que "les copies les plus fournies ne comportent que quelques incursions dans la dernière partie".
Pouvait-il en être autrement ?

Le même rapport explique que le "sujet a été conçu pour présenter une difficulté progressive et éviter tout grappillage" et que "le barème récompensait largement les candidats rigoureux ayant traité les deux premières parties". On peut donc dire, sans risquer de se tromper, qu'un candidat ayant traité presque complètement les deux premières parties obtenait son admissibilité.

Cela rejoint une remarque générale que l'on peut faire au sujet des problèmes de concours, tous infaisables pendant le temps imparti, mais dont il suffit d'en traiter le tiers, en rédigeant convenablement, pour avoir de fortes chances d'assurer son admissibilité.

Je serais même tenté d'énoncer (ici et pour la première fois !) une **"loi du 4-3-2"** selon laquelle résoudre et rédiger environ la quart, le tiers ou la moitié du problème donnerait respectivement des chances, de fortes chances, ou la quasi-certitude d'être admissible !
Il s'agit, bien entendu, d'une loi statistique basée sur l'expérimentation, les barres de l'admissibilité étant appelées à varier d'une année à l'autre en suivant les trois paramètres fondamentaux :

- nombre de candidat (en particulier nombre de candidats suffisamment préparés au concours),

- niveau de difficulté du problème,

- nombre de places au concours.

Quant à la façon d'estimer quelle fraction de l'ensemble on a traité, je pense que le plus simple et le plus efficace consiste à compter absolument toutes

les questions posées dans le problème, quelles qu'elles soient, puis calculer le quotient entre le nombre de questions résolues et rédigées, et le nombre total des questions du problème.
J'insiste : il ne s'agit pas de dénombrer le nombre de "questions numérotées", mais le nombre de questions réellement posées (en comptant le nombre de fois où l'on est sollicité par l'énoncé via des mots comme "montrer", "déduire", "établir", "vérifier"...). Une question "numérotée" est souvent constituée de plusieurs questions réellement posées. Et il s'agit ici de dénombrer toutes les questions de la même manière, les questions formulées rapidement ou très "simples" à résoudre comptant autant que les autres.

En poussant le raisonnement jusqu'au bout, on peut même en déduire une **méthodologie de préparation au concours**, et admettre

> qu'une forme de préparation suffisante à l'écrit d'un concours peut raisonnablement consister à s'entraîner sur de nombreuses annales corrigées en se bornant à traiter seulement le tiers ou la moitié des questions posées dans chacun des problèmes.

Le jour J, on tente de résoudre le plus de questions possibles, sans oublier de les rédiger avec rigueur et avec précision. Le correcteur récompense ensuite réellement les qualités montrées par le candidat à l'occasion de la résolution de chaque question, quelle que soit la difficulté de celle-ci.

Pour ce problème d'agrégation, le rapport du jury a clairement insisté sur le fait qu'il existait "suffisamment de questions, dont certaines élémentaires ou ne faisant appel qu'à des qualités de rigueur, pour que les notes obtenues témoignent assez justement des compétences de chacun."