4.1.2 Corrigé de la première épreuve écrite

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

A. Etude d'un premier exemple
1.

(a) Par hypothèse : $2 = |x - y| \leqslant |x| + |-y| \leqslant 1 + 1 = 2$, ce qui impose : $|x| = |-y| = 1$, et : $\exists\lambda \in \mathbb{R}_+, -y = \lambda x$ (cas d'égalité de l'inégalité triangulaire d'une norme euclidienne). Ainsi : $\lambda = 1$, $y = -x$ puis $\dfrac{x+y}{2} = 0$.

(b) Par contraposition, supposons $w \in B = \tau(A)$ et écrivons $w = \tau(a)$ avec $a \in A$. $|w - \tau(0)| = |\tau(a) - \tau(0)| = |a| \leqslant 1$ (τ est une isométrie).

(c) Par hypothèse, $\tau(0) \in B$. Ainsi $\tau(0) \neq 0$ et on peut considérer le diamètre $[u, v]$ orthogonal à $[0, \tau(0)]$. Par construction : $|u - \tau(0)| > 1$ et $|v - \tau(0)| > 1$, u et v sont dans A.

(d) Comme τ est affine elle conserve le milieu et $\tau(0)$ est le milieu de $[\tau(u), \tau(v)]$. Or, $|\tau(u) - \tau(v)| = |u - v| = 2$, avec : $\tau(u)$ et $\tau(v)$ dans $B = \tau(A) \subset \overline{D}$. Selon le (a), 0 est le milieu du segment $[\tau(u), \tau(v)]$. De là : $\tau(0) = 0 \in B \cap A$, la contradiction suit.

2.

Si $\overline{D}$ est $\mathcal{I}_2$-dédoublable, on peut écrire : $\overline{D} = A \amalg B$ avec : $\tau_1(\overline{D}) = A$, $\tau_2(\overline{D}) = B$ (τ_1, τ_2 sont dans $\mathcal{I}_2$). On peut toujours supposer que 0 est dans A et on pose alors : $\tau = \tau_2 \circ \tau_1^{-1}$ pour avoir : $\tau \in \mathcal{I}_2$, et $\tau(A) = B$. On sait alors que ces hypothèses mènent à une contradiction.

B. Cas des parties bornées
B 1. Disque enveloppant minimal
1.

(a) La partie $\mathcal{B}$ étant bornée, il existe $r_0 \geqslant 0$ tel que : $\mathcal{B} \subset \overline{D}(0, r_0)$ et donc $r_0 \in R$ puisque $0 \in \mathcal{C}_{r_0}$.

(b) $\inf R = \rho < \rho + \dfrac{1}{n}$; il existe donc r_n dans R tel que : $\rho \leqslant r_n < \rho + \dfrac{1}{n}$. De là : $\mathcal{C}_{r_n} \neq \emptyset$ et il existe x_n dans $\mathbb{C}$ tel que : $\mathcal{B} \subset \overline{D}(x_n, r_n) \subset \overline{D}\left(x_n, \rho + \dfrac{1}{n}\right)$.

2.

(a) et (b)
– Grâce au 1.(b), on dispose d'une suite $(x_n)_{n\in\mathbb{N}^*}$ telle que :

$$(*) \qquad \forall n \in \mathbb{N}^*, \forall b \in \mathcal{B}, |x_n - b| \leqslant \rho + \frac{1}{n}.$$

– Cette suite complexe est donc clairement bornée ($\mathcal{B} \neq \emptyset$) et si $\left(x_{\alpha(n)}\right)_{n\in\mathbb{N}^*}$ est extraite, convergente, de limite notée a, l'énoncé $(*)$ donne immédiatement : $\forall b \in \mathcal{B}, |a - b| \leqslant \rho$.

(c) Par l'absurde, soit $a_1 \neq a_2$ vérifiant : $\mathcal{B} \subset \overline{D}(a_1, \rho)$ et $\mathcal{B} \subset \overline{D}(a_2, \rho)$. Clairement (faire un dessin) : $\mathcal{B} \subset \overline{D}(a_1, \rho) \cap \overline{D}(a_2, \rho) \subset \overline{D}(c, r)$ avec : $c = \dfrac{a_1 + a_2}{2}$, et $r = \sqrt{\rho^2 - \dfrac{|a_1 - a_2|^2}{4}} < \rho$. Contradiction.

B 2. Conclusion
1.

Pour $\mathcal{I}_2^+$: les translations, les rotations. Pour $\mathcal{I}_2^-$(isométries indirectes) : les réflexions, les symétries glissées dont la forme réduite est : $s \circ t = t \circ s$ (s : réflexion, t :translation).

2.

(a) La clef : $\tau_i(\mathcal{B}) = \mathcal{B}_i \subsetneq \mathcal{B}$ pour $i = 1, 2$. Cela interdit : $\tau_i^2 = Id$ et τ_i ne peut donc pas être une réflexion. On en déduit aussi : $\forall n \in \mathbb{N}^*, \tau_i^n(\mathcal{B}) \subsetneq \mathcal{B}$, avec $\mathcal{B}$ bornée non vide. Il est donc impossible que τ_i soit une translation, même dans le "cas limite" $\tau_i = Id_{\mathbb{C}}$. En conséquence : τ_i ne peut pas être une symétrie glissée. Sinon, lorsque $\tau_i = s \circ t$ est sa forme réduite, on a : $\forall n \in \mathbb{N}^*, \tau_i^{2n}(\mathcal{B}) = t^{2n}(\mathcal{B}) \subset \mathcal{B}$. Bilan : τ_1 et τ_2 ne peuvent être que des rotations différentes de $Id_{\mathbb{C}}$.

(b) Soit $\overline{D}$ le disque fermé de rayon minimum contenant $\mathcal{B}$; on note a son centre et ρ son rayon (*confer* **B.**). Pour i fixé, $\mathcal{B} = \tau_i^{-1}(\mathcal{B}_i) \subset \tau_i^{-1}(\overline{D})$. Comme τ_i est une isométrie, $\tau_i^{-1}(\overline{D})$ est un disque fermé de rayon ρ (et de centre $\tau_i^{-1}(a)$). Par unicité de $\overline{D}$: $\tau_i^{-1}(\overline{D}) = \overline{D}$ et par unicité du centre de $\overline{D}$: $\tau_i(a) = a$. De là, selon (b), $a = \omega_i$ et donc : $\omega_1 = \omega_2$.

(c) Il en résulte que les rotations τ_i commutent et en particulier : $\tau_2 \circ \tau_1(\mathcal{B}) = \tau_1 \circ \tau_2(\mathcal{B})$. Or, $\tau_2(\tau_1(\mathcal{B})) = \tau_2(\mathcal{B}_1) \subset \tau_2(\mathcal{B}) = \mathcal{B}_2$, et de même : $\tau_1(\tau_2(\mathcal{B})) \subset \mathcal{B}_1$. La contradiction résulte alors des hypothèses : $\mathcal{B} \neq \emptyset$ et $\mathcal{B}_1 \cap \mathcal{B}_2 = \emptyset$. Bilan : aucune partie bornée (non vide) de $\mathbb{C}$ n'est $\mathcal{I}_2$-dédoublable.

Partie II : Le paradoxe de SIERPINSKI-MAZURKIEWICZ

1.

Par l'absurde, il existe P, Q dans $\mathcal{P}_{\mathbb{N}}$ tels que : $P(u) + 1 = uQ(u)$. Donc : $R(u) = 0$ avec : $R = 1 + P - XQ$ dans $\mathbb{Q}[X]$, ce qui contredit le statut de u puisque $R \neq 0$ ($R(0) = 1 + P(0) > 0$).

2.

Le coefficient constant de P est $\geqslant 1$ ou bien nul, ce qui justifie l'alternative. On pose : $\mathcal{D}_1 = \{(R+1)(u), R \in \mathcal{P}_{\mathbb{N}}\} = t(\mathcal{D})$ et $\mathcal{D}_2 = \{(XS)(u), S \in \mathcal{P}_{\mathbb{N}}\} = s(\mathcal{D})$. L'alternative ci-dessus donne : $\mathcal{D} = \mathcal{D}_1 \cup \mathcal{D}_2$ et le 1. donne $\mathcal{D}_1 \cap \mathcal{D}_2 = \emptyset$. Comme s et t sont dans $\mathcal{I}_2$, $\mathcal{D}$ est $\mathcal{I}_2$-dédoublable.

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

A. La croissance d'un groupe
1.

Essentiellement : $B_S(p+q) \subset B_S(p)B_S(q)$ car avec des notations évidentes $s_1 \cdots s_{p+q} = (s_1 \cdots s_p)(s_{p+1} \cdots s_{p+q})$

2.

(a) $u_1 = v_1$, et $u_p = \log \gamma_S(p) \geqslant 0$. Si $n = pq + r$, $0 \leqslant r < p$, on a :

$$u_n \leqslant qu_p + u_r \leqslant \frac{n-r}{p} u_p + rv_1 \leqslant nv_p + pv_1.$$

(b) A chaque $\varepsilon > 0$ on associe $p_\varepsilon \geqslant 1$ vérifiant $v_{p_\varepsilon} < v + \varepsilon$, et aussi $N_{\varepsilon, p_\varepsilon} \geqslant 1$ tel que : $\forall n \geqslant N$, $\frac{p_\varepsilon}{n} v_1 \leqslant \varepsilon$. Ainsi, pour $n \geqslant N$, $v \leqslant v_n \leqslant v + 2\varepsilon$ grâce au (a).

3.

$c_S(n) = \exp v_n \to \exp v \geqslant 1$.

4.

La définition montre qu'un groupe contenant un sous-groupe à croissance exponentielle est aussi à croissance exponentielle.

5.

Soit $S = \{s_1, \cdots, s_r\}$ une partie finie et symétrique de G. Comme G est abélien, tout élément de $B_S(n)(n \geqslant 1)$ s'écrit sous la forme : $s_1^{p_1} \cdots s_r^{p_r}$ avec $0 \leqslant p_1 + \cdots + p_r \leqslant n$ et $p_k \geqslant 0$. Donc, de façon très grossière, $\gamma_S(n) \leqslant (n+1)^r$ et $C_S = 1$.

B. La croissance du groupe $\mathcal{I}_1$

1.

Les applications affines : $s : x \mapsto ux + v$ avec u et v réels. Les isométries affines sont donc obtenues avec $u = \pm 1$, et les isométries directes avec $u = 1$.

2.

Il suffit de choisir $\varepsilon' = \pm Id$ de façon à avoir : $\varepsilon \circ s \circ \varepsilon' := t \in \mathcal{I}_1^+$. Avec les notations ci-dessus, $\varepsilon' = u\varepsilon$ s'impose clairement. Remarque : un tel couple (ε', t) est unique.

3.

Soit τ dans $B_S(n)$, $\tau = s_1 \circ \cdots \circ s_r$ avec $r \leqslant n$, $s_k \in S$. Selon le 2., on peut écrire : $s_1 = t_1 \circ \varepsilon_1'$; $\varepsilon_1' \circ s_2 = t_2 \circ \varepsilon_2'$; $\cdots$; $\varepsilon_{r-1}' \circ s_r = t_r \circ \varepsilon_r'$ (avec des notations évidentes). De là : $\tau = t_1 \circ \cdots \circ t_r \circ \varepsilon_r'$. Finalement, $\sigma = t_1 \circ \cdots t_r$ et $\varepsilon = \varepsilon_r'$ conviennent puisque les t_k sont dans T.

4.

Selon 3., $B_S(n) \subset B_T(n) \circ \{\pm Id\}$, donc $\gamma_S(n) \leqslant 2\gamma_T(n)$ et $C_S \leqslant C_T$. De plus, $C_T = 1$ puisque $\mathcal{I}_1^+$ est Abélien. Donc $C_S = 1$ et le résultat suit puisque S est arbitraire.

C. Conclusion

1.

Notons r le plus petit des indices i tels que : $s_i \neq s_i'$. Chaque s_k laisse stable $\mathcal{D}$ et : $s_r(\mathcal{D}) \cap s_r'(\mathcal{D}) \subset \mathcal{D}_1 \cap \mathcal{D}_2 = \emptyset$. De là :

$$s_r\left(s_{r+1} \circ \cdots \circ s_n(\mathcal{D})\right) \cap s_r'\left(s_{r+1}' \circ \cdots \circ s_n'(\mathcal{D})\right) = \emptyset.$$

Or, pour $i < r$, $s_i = s_i'$ et on a affaire à des bijections, de sorte que : $\gamma_s(\mathcal{D}) \cap \gamma_{s'}(\mathcal{D}) = \emptyset$.

2.

Selon le 1., pour $s \neq s'$ on a $\gamma_s \neq \gamma_{s'}$. On vient donc de construire 2^n éléments distincts de $B_S(n)$ et donc $\gamma_S(n) \geqslant 2^n$, soit : $C_S \geqslant 2$.

3.

Supposer l'existence d'une partie $\mathcal{I}_1$-dédoublable de $\mathbb{R}$ permet donc de contredire le caractère sous-exponentiel de la croissance de $\mathcal{I}_1$ ($C_S = 1$).

D. Application

On sait qu'il existe une partie $\mathcal{D}$ de $\mathbb{C}$ non-vide et $\mathcal{I}_2$-dédoublable (*confer* II.). En reprenant mutatis mutandis les raisonnements de la section III.C., on dispose d'une partie S de $\mathcal{I}_2$ pour laquelle $C_S \geqslant 2$. Ainsi, $\mathcal{I}_2$ est à croissance exponentielle.

Partie IV : Un groupe "paradoxal"

A. Calculs préliminaires

1.

$$A^k = \begin{pmatrix} 1 & 2k \\ 0 & 1 \end{pmatrix},\ B^k = \begin{pmatrix} 1 & 0 \\ 2k & 1 \end{pmatrix} \text{ pour } k \text{ dans } \mathbb{Z}.$$

On se contente de vérifier (1). $M = A^k$ avec $|k| \geqslant 1$; $X_2 = \begin{pmatrix} x \\ y \end{pmatrix} \in E_2$ avec $|x| < |y|$.
$MX_2 = \begin{pmatrix} x + 2ky \\ y \end{pmatrix}$; $|x + 2ky| \geqslant 2|k||y| - |x| > |y|$. $MX_2 \in E_1$.

B. Description de Γ

1.

On construit les éléments de Γ comme des "mots" dont les "lettres" sont puisées dans $\Gamma_1 \cup \Gamma_2$. La discussion porte sur le nombre de "lettres" puisées, I étant une "lettre" à part entière. Une "lettre" : I, P_0, M_0. Deux "lettres" : les précédents, ainsi que : P_0M_0, M_1P_1. Trois "lettres" : les précédents, ainsi que : $P_0(M_1P_1)$, $(M_1P_1)M_2$. Quatre "lettres" : les précédents, ainsi que : $P_0(M_1P_1)M_2$, $(M_1P_1)(M_2P_2)$. On fait ainsi apparaître les huit types annoncés, et aucun nouveau type n'apparaît lorsque la construction se poursuit.

2.

(a) $P_0M_0 = I$ nécessite $M_0 = P_0^{-1}$ et donc : $M_0 \in \Gamma_1 \cap \Gamma_2 = \{I\}$ (voir A.1.) ce qui n'est pas.

(b) Selon A.2., $M_{s+1}E_2 \subset E_1$ et $\Pi_s E_1 \subset E_1$, ainsi : $U_6E_2 \subset E_1$ ce qui impose $U_6 \neq I$.

(c) On considère $M_0U_5M_0^{-1} = (M_0P_0)\Pi_r M_0^{-1}$ où $M_0 \in \Gamma_1 \backslash \{I\}$. Cette matrice est du type U_6 et elle est donc distincte de I, il en résulte : $U_5 \neq I$. On considère $M_0U_4M_0^{-1} = ((M_0M_1)P_1)\cdots(M_nP_n)M_0^{-1}$ avec $M_0 \in \Gamma_1 \backslash \{I, M_1^{-1}\}$. Cette matrice est encore du type U_6, ce qui impose : $U_4 \neq I$.

(d) On considère : $M_{t+1}U_7M_{t+1}^{-1} = (M_{t+1}P_0)\Pi_t$ qui est du type U_4. Donc : $U_7 \neq I$.

3.

(a) Par hypothèse : $I = \Pi'_n \Pi_n^{-1} = M'_1 P'_1 \cdots M'_n (P'_n P_n^{-1}) M_n^{-1} \cdots P_1^{-1} M_1^{-1}$. Les matrices M_i, P_i, M'_i, P'_i étant toutes distinctes de I on doit avoir : $P'_n = P_n$ (sinon : $\Pi'_n \Pi_n^{-1}$ est du type U_6). Il faut alors, pour la même raison, que : $M'_n = M_n$, etc $\cdots$

(b) Fixons $n \geqslant 1$ et considérons $\Pi_n = M_1 P_1 \cdots M_n P_n$ avec : $M_i = A^{\pm 1}$, $P_i = B^{\pm 1}$. Par construction : $\Pi_n \in B_S(2n)$ et les Π_n ainsi obtenus (n fixé) sont deux à deux distincts (question précédente). Ainsi, $\gamma_S(2n) \geqslant 2^{2n}$ et $C_S \geqslant 2$. Le groupe Γ (et donc aussi $SL_2(\mathbb{Z})$) est à croissance exponentielle.

C. Eléments d'ordre fini de Γ

1.

U_4^k (resp. U_7^k) est encore du type (4) (resp. du type (7)) et de ce fait on ne peut avoir : $U_4^k = I$ (resp. $U_7^k = I$). $U_3^k \neq I$ si $k = 1$ et même si $k \geqslant 2$ car alors U_3^k est du type (7).

2.

(a) $V_1 = M_{s+1}\Pi_s = ((M_{s+1}M_1)P_1)(M_2P_2)\cdots(M_sP_s)$. Si $M_{s+1}M_1 \neq I$, V_1 est du type (4), ce qui interdit $V_1^k = I$ (question précédente) et contredit l'hypothèse. Ainsi $M_{s+1}M_1 = I$. $V_2 = (M_2P_2)\cdots(M_s(P_sP_1))$ (en tenant compte de $M_{s+1}M_s = I$) ce qui impose $P_sP_1 = I$. Sinon, V_2 est du type (4) et $V_2^k \neq I$, puis $V_1^k \neq I$, ce qui n'est pas.

(b) On vient de décrire une procédure de conjugaison qui permet "d'effacer" la première et la dernière "lettre" d'un "mot" de type U_6 ou U_5. Précisément, si $s \geqslant 2$:

$$\begin{array}{ccccc} \text{type } U_6 & \longrightarrow & \text{type } U_5 & \longrightarrow & \text{type } U_6 \\ U = U_6 & & V_1 & & V_2. \end{array}$$

En réitérant, on construit un conjugué U' de $U = U_6$ qui est dans $\Gamma_1 \cup \Gamma_2$ et qui est donc d'ordre fini ($U'^k = I$). De là : $U' = I$ (*confer* A.1.), puis $U_6 = I$, ce qui n'est pas. Autrement dit : U ne peut pas être du type U_6.

3.

$W = M_{r+1}^{-1} U_5 M_{r+1}$ est du type (6), ce qui interdit $W^k = I$ (question précédente) et interdit aussi : $U_5^k = I$.

4.

L'étude qui précède montre que U ne peut être que du type (0), (1) ou (2). Comme de plus I est le seul élément d'ordre fini de $\Gamma_1 \cup \Gamma_2$ (confer A.1.), c'est que : $U = I$.

D. Conclusion

Q_1 (resp. Q_2) est la partie formée des "mots" dont la "première lettre" est A (resp. A^{-1}). Plus précisément :

Q_1	les $M_0 = A^k$ ($k \geqslant 1$)	les U_4 ou U_6 tels que : $\exists l \geqslant 1, M_1 = A^l$
Q_2	les $M_0 = A^{-k}$ ($k \geqslant 1$)	les U_4 ou U_6 tels que : $\exists l \geqslant 1, M_1 = A^{-l}$

Notons U_4^- et U_6^- les types rencontrés dans la dernière case de ce tableau. On obtient alors :

AQ_2	A^{-k} $(k \geqslant 0)$	U_4^-, U_6^- si $l \geqslant 2$	U_5, U_7 si $l = 1\,;\, n, s \geqslant 2$	P_1 si $l = n = 1$	P_1M_2 si $l = s = 1$

Bilan : $\mathcal{Q}_1 \cup A\mathcal{Q}_2 = \Gamma$. De même, on définit la partie $\mathcal{R}_1$ (resp. $\mathcal{R}_2$) formée des "mots" dont la "première lettre" est B (resp. B^{-1}), et on obtient : $\mathcal{R}_1 \cup B\mathcal{R}_2 = \Gamma$. Finalement, le fait que les parties $\mathcal{Q}_1$, $\mathcal{Q}_2$, $\mathcal{R}_1$, $\mathcal{R}_2$ soient disjointes résulte de la propriété admise dans le texte ainsi que de l'injectivité des suites $\left(A^k\right)_{k\in\mathbb{Z}}$ et $\left(B^k\right)_{k\in\mathbb{Z}}$. Remarques :

- On a clairement : $\Gamma \backslash \{I\} = \mathcal{Q}_1 \cup \mathcal{Q}_2 \cup \mathcal{R}_1 \cup \mathcal{R}_2$.
- Le B. prouve que Γ est le produit libre des groupes Γ_1 et Γ_2 (lemme du ping-pong), chacun étant isomorphe à $\mathbb{Z}$ (*confer* A.). Ainsi Γ est le groupe libre de rang 2 engendré par A et B et le résultat admis au D. suit.

Partie V : Ensembles G-paradoxaux

A. Exemples

1.

On fait opérer le groupe Γ sur lui-même par translations : $U * V = UV$, puis on exploite le IV.D.

2.

Comme $G \subset \sigma_E$, G opère sur E de façon naturelle ($g * x = g(x)$) et si $\mathcal{D}$ est G-dédoublable on dispose de parties $\mathcal{D}_1$, $\mathcal{D}_2$ disjointes telles que : $g_1^{-1} * \mathcal{D}_1 = \mathcal{D} = g_2^{-1} * \mathcal{D}_2$ pour des g_i convenables dans G. $\mathcal{D}$ est donc G-paradoxale.

3.

Soit T une partie de E qui rencontre chaque Γ-orbite selon un singleton (l'axiome du choix valide l'existence de T tant qu'on ne sait rien sur E). Par construction : $E = \Gamma * T$. Avec les notations du IV.D., considérons les parties de E : $\mathcal{Q}_1 * T$; $\mathcal{Q}_2 * T$; $\mathcal{R}_1 * T$; $\mathcal{R}_2 * T$. Comme l'action est supposée être sans points fixes (hypothèse de l'énoncé), ces quatre parties de E sont deux à deux disjointes. En effet, pour fixer les idées, si : $U_1 * t_1 = U_2 * t_2$ avec : $t_1, t_2 \in T$ et : $U_1 \in \mathcal{Q}_1$, $U_2 \in \mathcal{Q}_2$, alors $(U_2^{-1}U_1) * t_1 = t_2$ et donc $t_1 = t_2$ (ils sont dans la même Γ-orbite), puis $U_1 = U_2$ (l'action est sans points fixes), ce qui assure la contradiction puisque : $\mathcal{Q}_1 \cap \mathcal{Q}_2 = \emptyset$. Comme $\Gamma = \mathcal{Q}_1 \cup A\mathcal{Q}_2 = \mathcal{R}_1 \cup B\mathcal{R}_2$, on obtient, via l'action de Γ sur E : $E = (\mathcal{Q}_1 * T) \cup (A * (\mathcal{Q}_2 * T))$ et $E = (\mathcal{R}_1 * T) \cup (B * (\mathcal{R}_2 * T))$. Bilan : E est Γ-paradoxal, avec : $\mathcal{Q} = (\mathcal{Q}_1 * T) \amalg (\mathcal{Q}_2 * T)$; $\mathcal{Q} = (\mathcal{R}_1 * T) \amalg (\mathcal{R}_2 * T)$, les partitions étant évidentes ($m = n = 2$) ; $g_1 = h_1 = I$; $g_2 = A$, $h_2 = B$.

B. Le plan hyperbolique est Γ-paradoxal

1. et 2.(a)

trivial, simple calcul, usuel de surcroît.

(b) $-I \notin \Gamma$ puisque $(-I)^2 = I$ et qu'il n'y a pas d'éléments d'ordre fini dans $\Gamma \backslash \{I\}$ (*confer* IV.C.). L'injectivité du morphisme restreint à Γ en résulte.

3.

(a) Procédons de façon "culinaire". Soit $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ dans $SL_2(\mathbb{Z})$ et x dans $\mathbb{H}^2$ avec $h_M(x) = x$, cela s'écrit : $cx^2 + (d-a)x - b = 0$ (E). Cas 1 : $c = 0$ et donc $a = d(= \pm 1)$, puis $b = 0$, ainsi : $h_M = id$. Cas 2 : $c \neq 0$; les racines complexes de (E) sont donc x et $\overline{x} \neq x$, elles sont non-réelles et donc $0 > \Delta = (d-a)^2 + 4bc = (a+d)^2 - 4$, et $|tr(M)| < 2$.

(b) Notoirement : $M^2 - (tr(M))M + I = 0$ $(det(M) = 1)$. Si $tr(M) = 0$, $M^2 = -I$ et donc $h_M^2 = id$. Si $tr(M) = \pm 1$ et même $tr(M) = 1$ (quitte à prendre $-M$), alors $M^2 = M - I$ donc $M^3 = M^2 - M = -I$, d'où $h_M^3 = id$. Si $|tr(M)| \geqslant 2$ alors $h_M = id$.

4.

Soit h dans $\overline{\Gamma} \setminus \{id\}$; si h fixe un point de $\mathbb{H}^2$, $h \neq id$ est d'ordre fini dans le groupe $\overline{\Gamma}$ (3.(b)) et la contradiction résulte de l'isomorphisme en Γ et $\overline{\Gamma}$, puisque dans $\Gamma \setminus \{id\}$ il n'y a pas d'éléments d'ordre fini.

5.

Grâce au morphisme $U \longrightarrow h_U$ de Γ vers $\overline{\Gamma} \subset (\sigma_{\mathbb{H}^2}, \circ)$, on fait opérer Γ sur $\mathbb{H}^2$ en posant : $U * x = h_U(x)$. Selon 4., cette action est sans points fixes et donc $\mathbb{H}^2$ est Γ-paradoxal (*confer* V.A.3.). Remarque : les parties qui rendent Γ-paradoxal l'ensemble $\mathbb{H}^2$ peuvent être prises boréliennes et l'axiome du choix est donc ici totalement superflu.

C. Une partie bornée de $\mathbb{R}^2$ et Γ-paradoxale

1.

C'est le point-clef. Ecrivons $\gamma = \gamma_U$ avec $U = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$; γ est linéaire et $\gamma(\mathbb{Z}^2) = \mathbb{Z}^2$ puisque $U \in M_2(\mathbb{Z})$. Donc, si $p \sim q$: $\gamma(p) - \gamma(q) = \gamma(p-q) \in \gamma(\mathbb{Z}^2) \subset \mathbb{Z}^2$.

2.

Selon 1., $\forall a, b \in \mathbb{R}^2, a \sim b \Rightarrow \widehat{\gamma(a)} = \widehat{\gamma(b)}$ et en particulier :
$\forall a \in \mathbb{R}^2, \widehat{\gamma(\widehat{a})} = \widehat{\gamma(a)}$. Pour γ_1, γ_2 dans Γ_g et p dans Δ :

$$\widehat{\gamma_1} \circ \widehat{\gamma_2}(p) = \widehat{\gamma_1}(\widehat{\gamma_2}(p)) = \widehat{\gamma_1}(\widehat{\gamma_2(p)}) = \widehat{\gamma_1(\widehat{\gamma_2(p)})} = \widehat{\gamma_1(\gamma_2(p))} = \widehat{\gamma_1 \circ \gamma_2}(p).$$

Ainsi, $\widehat{\gamma_1} \circ \widehat{\gamma_2} = \widehat{\gamma_1 \circ \gamma_2}$. En conséquence : si $\gamma \in \Gamma_g$, $\widehat{\gamma} \circ \widehat{\gamma^{-1}} = \widehat{id_{\mathbb{R}^2}} = id_\Delta = \widehat{\gamma^{-1}} \circ \widehat{\gamma}$. Donc $\widehat{\gamma}$ est bijective de bijection réciproque $\widehat{\gamma^{-1}}$. De là, l'application : $\gamma \mapsto \widehat{\gamma}$ est un morphisme du groupe Γ_g vers le groupe $(\sigma_\Delta, \circ)$. Reste donc à prouver le caractère injectif de ce morphisme : Λ. Soit γ dans Γ_g tel que $\widehat{\gamma} = id_\Delta$. Cas 1 : $\gamma(\Delta) \subset \Delta$, alors $\widehat{\gamma} = \gamma|_\Delta^\Delta$ et γ, linéaire, fixe tous les points de Δ, donc une base de $\mathbb{R}^2$: $\gamma = id_{\mathbb{R}^2}$. Cas 2 : $\gamma(\Delta)$ n'est pas inclus dans Δ. Le parallélogramme $\gamma(\Delta)$ rencontre selon un polygone non aplati l'un des huit carrés C_k qui entourent Δ. On note $P = \gamma(\Delta) \cap C_{k_0}$ ce polygone et τ_0 la translation de vecteur dans $\mathbb{Z}^2$ telle que : $\tau_0(P) \subset \Delta$. Par construction : (1) $P' = \gamma^{-1}(P)$ est un polygone non aplati contenu dans Δ et (2) $\widehat{\gamma}$ et $\tau_0 \circ \gamma$ coïncident sur P'. Comme $\widehat{\gamma} = id_\Delta$, l'application affine $\tau_0 \circ \gamma$ fixe au moins trois points non alignés du plan complexe (de P'), d'où : $\tau_0 \circ \gamma = id_{\mathbb{C}}$, puis $\gamma = \tau_0^{-1}$ et enfin $\tau_0^{-1} = id_{\mathbb{C}}$ puisque γ est linéaire, c'est-à-dire $\gamma = id_{\mathbb{C}}$. Les groupes Γ_g et $\widehat{\Gamma_g}$ sont donc isomorphes via Λ.

3.

Il suffit de montrer que Γ est dénombrable. Notons $S = \{A^{\pm 1}, B^{\pm 1}\}$. $\Gamma = \cup_{n \in \mathbb{N}} B_S(n)$, où chaque ensemble $B_S(n) = \{U \in \Gamma, l_S(U) \leqslant n\}$ est fini. Le résultat suit puisque : une réunion dénombrable d'ensembles dénombrables est encore dénombrable.

4.

(a) Une droite coupe le cercle C_0 en au plus deux points et donc, pour chaque n, $C_0 \cap \mathcal{D}_n$ est fini. De là, $\cup_{n \in \mathbb{N}}(C_0 \cup \mathcal{D}_n)$ est dénombrable, alors que C_0 ne l'est pas puisque : si $p_0 \in C_0$, $C_0 \backslash \{p_0\}$ est équipotent à une droite (par projection stéréographique) et donc à $\mathbb{R}$. Bilan : $\cup_{n \in \mathbb{N}}(C_0 \cap \mathcal{D}_n) \subsetneq C_0$.

(b) Pour γ dans Γ_g, notons $Fix(\widehat{\gamma})$ l'ensemble des points fixes de $\widehat{\gamma}$. Ainsi : $F = \cup_{\gamma \in \Gamma_g \backslash \{id_{\mathbb{C}}\}} Fix(\widehat{\gamma})$. Pour p dans Δ et γ dans $\Gamma_g \backslash \{id_{\mathbb{C}}\}$: $p \in Fix(\widehat{\gamma}) \Leftrightarrow \gamma(p) \sim p \Leftrightarrow (\gamma - id)(p) \in \mathbb{Z}^2$. Finalement : $Fix(\widehat{\gamma})$ est la trace sur Δ de la préimage de $\mathbb{Z}^2$ par l'endomorphisme $L = \gamma - id$ de $\mathbb{R}^2$. Comme $L \neq 0$, deux cas sont possibles. Cas 1 : $KerL = \{0\}$. $L^{-1}(\mathbb{Z}^2)$ est équipotent à $\mathbb{Z}^2$. Cas 2 : $KerL := D$ est une droite vectorielle. Pour chaque p de $\mathbb{Z}^2$, $L^{-1}(\{p\})$ est une droite affine dirigée par D et donc $L^{-1}(\mathbb{Z}^2)$ est une réunion dénombrable de droites affines, toutes parallèles à D. Comme $\mathbb{Z}^2$ est dénombrable, on peut écrire : $L^{-1}(\mathbb{Z}^2) = \cup_{m \in \mathbb{N}} D_m$. Bilan : $F = F_0 \cup F_1$, où F_0 est une partie dénombrable de Δ et $F_1 = \cup_{m \in \mathbb{N}}(\Delta \cap D_m)$. En conséquence : $C_0 \cap F = (C_0 \cap F_0) \cup (C_0 \cap F_1)$ et comme $C_0 \subset \Delta$, on a : $C_0 \cap F_1 = \cup_{m \in \mathbb{N}}(C_0 \cap D_m)$. Pour respecter l'homogénéité des écritures, on est donc amené à dire que : $C_0 \cap F_0 = \cup_{p \in F_0 \cap C_0}(C_0 \cap T_p)$, où T_p est la tangente en p à C_0. Comme $F_0 \cap C_0$ est dénombrable (avec F_0) et qu'une réunion de deux ensembles dénombrables est encore dénombrable, on peut finalement écrire : $C_0 \cap F = \cup_{n \in \mathbb{N}}(C_0 \cap \mathcal{D}_n)$, où : $(\mathcal{D}_n)_{n \in \mathbb{N}}$ est une suite de droites affines de $\mathbb{R}^2$. De là, via le (a), $C_0 \cap F \subsetneq C_0$.

5.

On vient de démontrer que chaque cercle C_0 de rayon strictement positif, contenu dans Δ, n'est pas inclus dans F. Ainsi, F est d'intérieur vide dans $\mathbb{R}^2$ (on a réussi à se passer du théorème de Baire...).

6.

Selon le 5., on a en particulier $F \subsetneq \Delta$ (et même $\overset{\circ}{F} = \emptyset$ dans Δ), donc $\mathcal{P} = \Delta \backslash F \neq \emptyset$. Pour U dans Γ et p dans Δ, on pose : $U * p = \widehat{\gamma}_U(p)$. On définit ainsi une opération du groupe Γ sur l'ensemble Δ puisque les applications suivantes sont des morphismes de groupes (la première est même un isomorphisme) :

$\begin{array}{ccc} \Gamma & \rightarrow & \Gamma_g \\ U & \mapsto & \gamma_U \end{array}$; $\begin{array}{ccc} \Gamma_g & \rightarrow & (\sigma_\Delta, \circ). \\ \gamma & \mapsto & \widehat{\gamma} \end{array}$ Montrons que $\mathcal{P}$ est une partie stable sous cette action, au sens suivant : $\forall p \in \mathcal{P}$, $\forall U \in \Gamma$, $U * p \in \mathcal{P}$. Par l'absurde, il existe $U \in \Gamma$ et p dans $\mathcal{P}$ tels que : $U * p \in F$; d'où V dans $\Gamma \backslash \{I\}$ tel que : $\widehat{\gamma}_V(U * p) = U * p$. Cela s'écrit : $V * (U * p) = V * p$, soit $(U^{-1}VU) * p = p$ et donc : $p \in Fix(\widehat{\gamma}_W)$ avec $W = U^{-1}VU$ ce qui impose, par définition de $\mathcal{P}$, $W = I$ puis $V = I$, ce qui n'est pas. Bilan : Le groupe Γ opère sur la partie bornée, non vide, $\mathcal{P}$; de plus, par construction, cette action est sans points fixes et $\mathcal{P}$ est Γ-paradoxale (*confer* V.A.3.).