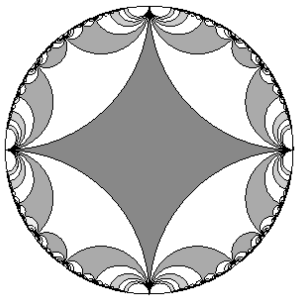
Université Claude Bernard–Lyon I
CAPES de Mathématiques : épreuve 2
Année 2006–2007

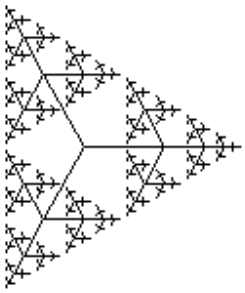
CAPES blanc
21/12/2006

Le problème s'articule autour du groupe engendré par les matrices

$$U = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \quad \text{et} \quad V = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}.$$

Après une première partie de préliminaires, on montre qu'il est libre, ce qui conduit au premier dessin ; on l'utilise pour énumérer les triplets pythagoriciens, solutions entières de l'équation célèbre : $x^2 + y^2 = z^2$, avec l'arbre du deuxième dessin.





On se place "dans" l'ensemble des nombres complexes $\mathbb{C}$. Quand il sera question de géométrie, on considèrera $\mathbb{C}$ comme un plan affine euclidien orienté, de la façon usuelle. On identifiera un "point du plan" et son "affixe".

On note $\mathbb{P}^1 = \mathbb{C} \cup \{\infty\}$ l'ensemble obtenu en ajoutant un élément noté ∞ à l'ensemble des nombres complexes $\mathbb{C}$. On étend partiellement les opérations de $\mathbb{C}$ à $\mathbb{P}^1$ par les conventions :

$$\forall a \in \mathbb{C}, \quad a + \infty = \infty + a = -\infty = \infty, \quad \frac{a}{\infty} = 0.$$

Noter que $0 \times \infty$, $\infty - \infty$ et $0/0$ ne sont pas définis.

Soit $GL_2(\mathbb{C})$ le groupe des matrices 2×2 complexes inversibles et, pour $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{C})$,

$$\begin{array}{rccl} h_A : & \mathbb{P}^1 & \longrightarrow & \mathbb{P}^1 \\ & z & \longmapsto & \left\{ \begin{array}{ll} \dfrac{az+b}{cz+d} & \text{si } z \in \mathbb{C} \text{ et } cz+d \neq 0, \\ \infty & \text{si } z \in \mathbb{C} \text{ et } cz+d = 0, \\ a/c & \text{si } z = \infty \text{ et } c \neq 0, \\ \infty & \text{si } z = \infty \text{ et } c = 0. \end{array} \right. \end{array}$$

Avec les conventions sur le calcul avec ∞, et en écrivant

$$h_A(\infty) = \frac{a + \frac{b}{\infty}}{c + \frac{d}{\infty}} = \frac{a}{c},$$

on réunit toutes les formules en une seule : $h_A(z) = (az+b)/(cz+d)$ pour tout $z \in \mathbb{P}^1$.
Une homographie est une application de $\mathbb{P}^1$ dans $\mathbb{P}^1$ de la forme h_A. Par abus, on appellera parfois homographie la restriction d'une telle application à certaines parties.

I Généralités sur les homographies

I.A Composition d'homographies

I.A.1) Vérifier que si A et A' sont deux éléments de $GL_2(\mathbb{C})$, on a : $h_A \circ h_{A'} = h_{AA'}$.
I.A.2) En déduire que l'ensemble des homographies est un sous-groupe du groupe des bijections de $\mathbb{P}^1$. En particulier, on déterminera l'application réciproque d'une homographie.
I.A.3) Vérifier que pour tout $A \in GL_2(\mathbb{C})$ et tout $\lambda \in \mathbb{C}^*$, on a : $h_A = h_{\lambda A}$.
I.A.4) Inversement, montrer que si A et A' sont deux éléments de $GL_2(\mathbb{C})$ tels que $h_A = h_{A'}$, il existe $\lambda \in \mathbb{C}$ tel que $A' = \lambda A$.

I.B Homographies et birapport

Etant donné quatre complexes distincts z_1, z_2, z_3 et z_4, on définit leur birapport par :

$$[z_1, z_2, z_3, z_4] = \frac{z_1 - z_3}{z_1 - z_4} \times \frac{z_2 - z_4}{z_2 - z_3}.$$

Cette définition s'étend à quatre éléments de $\mathbb{P}^1$. Par exemple, on a : $[\infty, 0, 1, z_4] = z_4$.

On fixe quatre complexes distincts z_1, z_2, z_3 et z_4.
I.B.1) Montrer qu'il existe une unique homographie h telle que

$$h(z_1) = \infty, \quad h(z_2) = 0, \quad h(z_3) = 1.$$

I.B.2) Que vaut $h(z_4)$?
I.B.3) Soit g une homographie. Notons, pour $i \in \{1, 2, 3, 4\}$, $z_i' = g(z_i)$ et h' l'homographie telle que $h'(z_1') = \infty$, $h'(z_2') = 0$, $h'(z_3') = 1$. Montrer sans calculs que $h = h' \circ g$, et en déduire que l'on a :

$$[g(z_1), g(z_2), g(z_3), g(z_4)] = [z_1, z_2, z_3, z_4].$$

I.C Homographies et cercles

Rappel : quatre points distincts A, B, C, D sont cocycliques ou alignés si, et seulement si

$$(\widehat{\overrightarrow{AC}, \overrightarrow{AD}}) \equiv (\widehat{\overrightarrow{BC}, \overrightarrow{BD}}) \ [\pi].$$

I.C.1) Vérifier que quatre points sont cocycliques ou alignés si, et seulement si leur birapport est réel.
I.C.2) En déduire que l'image d'un cercle ou d'une droite par une homographie est un cercle ou une droite.

I.C.3) Exemple
On note j l'homographie définie par

$$\forall z \in \mathbb{P}^1 \setminus \{0, \infty\}, \quad j(z) = \frac{1}{z} \ ; \quad j(0) = \infty \ ; \quad j(\infty) = 0.$$

a. Montrer que j envoie la droite $\{z \in \mathbb{C} : \operatorname{Re} z = 1\}$ sur le cercle de centre $\frac{1}{2}$ et de rayon $\frac{1}{2}$ (privé de 0).

b. Montrer que pour $s > 1$, j envoie la droite $D_s = \{z \in \mathbb{C} : \operatorname{Re} z = s\}$ sur un cercle contenu dans le disque ouvert Q^+ délimité par le cercle précédent (privé de 0).

c. En déduire que j envoie le demi-plan $P^+ = \{z \in \mathbb{C} : \operatorname{Re} z > 1\}$ sur le disque ouvert Q^+.

d. Donner sans justification l'image de la droite $\{\operatorname{Re} z = -1\}$ et du demi-plan $\{\operatorname{Re} z < -1\}$.

II Le groupe $\Gamma(2) = \langle u, v\rangle$: un groupe libre

On note $u = h_U$ et $v = h_V$ les homographies définies par :

$$\forall z \in \mathbb{P}^1, \quad u(z) = z + 2, \quad v(z) = \frac{z}{2z+1}.$$

On note $\Gamma(2)$ le groupe engendré par u et v dans le groupe des homographies. On note aussi

$$P^- = \{z \in \mathbb{C},\ \mathrm{Re}\, z < -1\}, \quad P^+ = \{z \in \mathbb{C},\ \mathrm{Re}\, z > 1\}, \quad P_0 = \{z \in \mathbb{C},\ -1 < \mathrm{Re}\, z < 1\},$$

$$Q^- = \left\{z \in \mathbb{C},\ \left|z + \frac{1}{2}\right| < \frac{1}{2}\right\}, \quad Q^+ = \left\{z \in \mathbb{C},\ \left|z - \frac{1}{2}\right| < \frac{1}{2}\right\}, \quad Q_0 = \mathbb{C} \setminus \overline{Q^+ \cup Q^-}.$$

II.A Le groupe $\Gamma(2)$

On note Γ' l'ensemble des homographies de la forme $w_1^{k_1} w_2^{k_2} \cdots w_n^{k_n}$, où $n \in \mathbb{N}^*$, $(w_1, \ldots, w_n) \in \{u, v\}^n$ et $(k_1, \ldots, k_n) \in \mathbb{Z}^n$.

II.A.1) Démontrer que Γ' est un sous-groupe du groupe des homographies et que $\Gamma' = \Gamma(2)$.

II.A.2) Soit $g \in \Gamma(2) \setminus \{\mathrm{Id}\}$. Démontrer qu'il existe un entier $n \in \mathbb{N}^*$, ainsi que $(w_1, \ldots, w_n) \in \{u, v\}^n$ et $(k_1, \ldots, k_n) \in \mathbb{Z}^{*n}$ tels que

$$g = w_1^{k_1} w_2^{k_2} \cdots w_n^{k_n} \quad \text{et} \quad \forall i \in \{1, \ldots, n-1\},\ w_i \neq w_{i+1}.$$

II.B Action de u et v sur certains disques

II.B.1) Représenter sur un dessin P^+, P^-, Q^+, Q^- et $F = P_0 \cap Q_0$.

II.B.2) Vérifier que l'image de P_0 par une puissance quelconque non nulle u^k, $k \neq 0$ de u est contenu soit dans P^+, soit dans P^-, selon le signe de k.

II.B.3) On note j l'homographie définie par $j(z) = 1/z$. Vérifier que $juj^{-1} = v$.

II.B.4) On a vu en I.C.3) que $j(P^\pm) = Q^\pm$. Qu'en déduit-on sur $v^k(Q_0)$, pour $k \in \mathbb{Z}$, $k \neq 0$?

II.B.5) En déduire que

$$\forall k \in \mathbb{N}^*,\ \forall \varepsilon, \eta \in \{+, -\}, \quad u^{\varepsilon k}(Q^\eta) \subset P^\varepsilon \quad \text{et} \quad v^{\varepsilon k}(P^\eta) \subset Q^\varepsilon.$$

II.C Liberté de $\Gamma(2)$

II.C.1) Soit $n \in \mathbb{N}^*$, $(w_1, \ldots, w_n) \in \{u, v\}^n$ et $(k_1, \ldots, k_n) \in \mathbb{Z}^{*n}$ tels que $w_i \neq w_{i+1}$ pour $1 \leq i \leq n-1$. On pose $g = w_1^{k_1} w_2^{k_2} \cdots w_n^{k_n}$.

a. Démontrer que g envoie $F = P_0 \cap Q_0$ dans un des disques P^+, P^-, Q^+, Q^-.

b. En déduire que g n'est pas l'identité.

II.C.2) Soit $n, n' \in \mathbb{N}^*$, $(w_1, \ldots, w_n) \in \{u, v\}^n$, $(w'_1, \ldots, w'_{n'}) \in \{u, v\}^{n'}$ et $(k_1, \ldots, k_n) \in \mathbb{Z}^{*n}$, $(k'_1, \ldots, k'_{n'}) \in \mathbb{Z}^{*n'}$ tels que $w_i \neq w_{i+1}$ et $w'_i \neq w'_{i+1}$ pour $1 \leq i \leq n'-1$.

On suppose que $w_1^{k_1} w_2^{k_2} \cdots w_n^{k_n} = {w'}_1^{k'_1} {w'}_2^{k'_2} \cdots {w'}_{n'}^{k'_{n'}}$.

Démontrer que $n = n'$, $(w_1, \ldots, w_n) = (w'_1, \ldots, w'_{n'})$ et $(k_1, \ldots, k_n) = (k'_1, \ldots, k'_{n'})$.

II.D Domaine fondamental

Soit

$$\mathbb{H} = \{z \in \mathbb{C} \ :\ \mathrm{Im}\, z > 0\}.$$

Dans cette question, on montre que les images de l'adhérence $\overline{F}$ de F par les éléments de $\Gamma(2)$ recouvrent $\mathbb{H}$.

On fixe $z \in \mathbb{H}$, et on note

$$\mathcal{O}_z = \{g(z) \ :\ g \in \Gamma(2)\} \quad \text{et} \quad \mathcal{I}_z = \{\mathrm{Im}\, z' \ :\ z' \in \mathcal{O}_z\}$$

II.D.1) Montrer que pour $g \in \Gamma(2)$ et $z \in \mathbb{H}$, on a :

$$\operatorname{Im} g(z) = \frac{\operatorname{Im} z}{|cz+d|^2}.$$

II.D.2) Soit $\varepsilon > 0$. Montrer que l'ensemble $\mathcal{I}_z \cap [\varepsilon, +\infty[$ est fini.
(Indication : $|cz+d| \geq |c\operatorname{Im}(z)|$ et $|cz+d| \geq |d| - |cz|$.)
II.D.3) En déduire que l'ensemble $\mathcal{I}_z$ possède un élément maximal.
II.D.4) Soit $z' \in \mathcal{O}_z$ un élément dont la partie imaginaire est maximale. Vérifier qu'il existe $g \in \Gamma(2)$ tel que $-1 \leq \operatorname{Re} g(z') \leq 1$ et $\operatorname{Im} g(z') = \operatorname{Im} z'$.
II.D.5) Soit $z'' \in Q^+$. Montrer que $\operatorname{Im} v(z'') > \operatorname{Im} z''$. Donner sans démonstration un énoncé analogue pour Q^-.
II.D.6) En déduire que $g(z') \in \overline{F}$.
II.D.7) Montrer enfin que z est l'image d'un élément de $\overline{F}$ par un élément de $\Gamma(2)$.

III Le groupe $\tilde{\Gamma} = \operatorname{Ker}(PSL_2(\mathbb{Z}) \to PSL_2(\mathbb{Z}/2\mathbb{Z})$

On rappelle que

$$U = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \quad \text{et} \quad V = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}.$$

III.A Le groupe $\tilde{\Gamma}$, un groupe presque libre

On note $\mathcal{M}_2(\mathbb{Z})$ l'ensemble des matrices 2×2 à coefficients entiers et

$$\tilde{\Gamma} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_2(\mathbb{Z}) : \ ad - bc = 1, \quad a \equiv d \equiv 1 \ [2], \quad b \equiv c \equiv 0 \ [2] \right\}.$$

III.A.1) Montrer que $\tilde{\Gamma}$ est un sous-groupe de $GL_2(\mathbb{C})$ contenant U et V.
III.A.2) Soit a et c deux entiers non nuls tels que $|a| \neq |c|$. Vérifier que l'un des deux entiers $\Big||a| - 2|c|\Big|$ et $\Big||c| - 2|a|\Big|$ est strictement plus petit que $\max(|a|, |c|)$.
III.A.3) On définit une fonction $\delta : \tilde{\Gamma} \to \mathbb{N}$ par :

$$\delta(A) = \max(|a|, |c|) \quad \text{si } A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

a. Vérifier que pour tout $A \in \tilde{\Gamma}$, on a : $\delta(A) \geq 1$.

b. Montrer que pour tout $A \in \tilde{\Gamma}$, si $\delta(A) > 1$, il existe $W \in \{U, U^{-1}, V, V^{-1}\}$ tel que $\delta(WA) < \delta(A)$.

III.A.4) Montrer, par récurrence sur $\delta(A)$, que pour tout $A \in \tilde{\Gamma} \setminus \{\mathrm{Id}\}$, il existe $\varepsilon \in \{-1, 1\}$, $r \in \mathbb{N}^*$, $(W_1, \ldots, W_r) \in \{U, V\}^r$ et $(k_1, \ldots, k_r) \in \mathbb{Z}^{*r}$ tels que

$$A = \varepsilon W_1^{k_1} W_2^{k_2} \cdots W_r^{k_r} \quad \text{et} \quad \forall i \in \{1, \ldots, n-1\}, \ W_i \neq W_{i+1}.$$

III.A.5) En utilisant I.A.4) et II.C.2), montrer qu'une telle décomposition est unique.

III.B Complétions d'une colonne

III.B.1) Soit $m, n \in \mathbb{Z}$ avec $m \wedge n = 1$. Montrer qu'il existe $p, q \in \mathbb{Z}$ tel que $mq - np = 1$.
III.B.2) On suppose que m est impair et n est pair. Montrer qu'il existe $(p, q) \in \mathbb{Z}^2$ tel que

$$\begin{pmatrix} m & p \\ n & q \end{pmatrix} \in \tilde{\Gamma}.$$

III.B.3) Plus précisément, soit $(p,q),(p',q') \in \mathbb{Z}^2$. Montrer que les matrices

$$A = \begin{pmatrix} m & p \\ n & q \end{pmatrix} \quad \text{et} \quad A' = \begin{pmatrix} m & p' \\ n & q' \end{pmatrix}$$

appartiennent à $\tilde{\Gamma}$, si, et seulement s'il existe $k \in \mathbb{Z}$ tel que $A' = AU^k$.

III.C La bijection Φ

On note $\Phi : \tilde{\Gamma} \to \tilde{\Gamma}$, $A \mapsto DAD^{-1}$, où $D = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$. Calculer $\Phi(A)$ en fonction de A.

IV Enumération des triplets pythagoriciens

On appelle triplet pythagoricien (TP) un triplet $(x,y,z) \in \mathbb{Z}^3$ d'entiers tel que

$$x^2 + y^2 = z^2.$$

On dira qu'un TP est primitif (x,y,z) si x, y et z sont premiers entre eux dans leur ensemble, positif si x, y et z sont strictement positifs.

IV.A Réduction aux TP primitifs

IV.A.1) Vérifier que tout TP différent de $(0,0,0)$ est de la forme (dx', dy', dz'), où $d \in \mathbb{N}^*$ et (x',y',z') est un TP primitif.

IV.A.2) Montrer que si (x,y,z) est un TP primitif, alors x, y et z sont premiers entre eux deux à deux, et que x et y sont de parité différente. (En particulier, z est impair.)

IV.B Paramétrage des TP primitifs

Soit $t \in \mathbb{R}$ et $1+2it$ un point de la tangente en 1 au cercle unité. On note Z l'intersection du cercle unité et de la droite contenant -1 et $1+2it$.

IV.B.1) Faire un dessin.

IV.B.2) Quelle relation y a-t-il entre t et l'argument de Z ? En déduire que l'on a :

$$Z = \frac{1-t^2}{1+t^2} + \frac{2t}{1+t^2}\, i.$$

IV.B.3) Montrer que t est rationnel si, et seulement si les parties réelle et imaginaire de Z sont rationnelles.

IV.B.4) En déduire que (x,y,z) est un TP primitif si, et seulement s'il existe $m,n \in \mathbb{Z}$, premiers entre eux et de parités différentes, tels que

$$\begin{cases} x = m^2 - n^2 \\ y = 2mn \\ z = m^2 + n^2 \end{cases} \quad \text{ou} \quad \begin{cases} x = 2mn \\ y = m^2 - n^2 \\ z = m^2 + n^2. \end{cases}$$

IV.C Enumération des TP primitifs positifs

On note $\mathcal{T}$ l'ensemble des TP primitifs positifs (x,y,z) dont le premier élément x est impair, et on considère l'application

$$\begin{array}{rccc} f : & \tilde{\Gamma} & \longrightarrow & \mathcal{T} \\ & \begin{pmatrix} m & p \\ n & q \end{pmatrix} & \longmapsto & \left(|m^2-n^2|, 2|mn|, m^2+n^2\right). \end{array}$$

IV.C.1) Vérifier que f est surjective.

IV.C.2) Vérifier que, pour $A, A' \in \tilde{\Gamma}$, on a :

$$f(A) = f(A') \iff \exists \varepsilon \in \{-1,1\},\ \exists k \in \mathbb{Z},\ A' = \varepsilon A U^k \text{ ou } A' = \varepsilon \Phi(A) U^k.$$

IV.C.3) Montrer que tout élément de $\mathcal{T}$ est l'image par f d'un unique

$$U^{k_1} V^{\ell_1} U^{k_2} V^{k_2} \cdots U^{k_s} V^{\ell_s}, \quad \text{où } s \geq 1,\ k_1 \in \mathbb{Z},\ k_2, \cdots, k_s \in \mathbb{Z}^*,\ \ell_1, \ldots, \ell_{s-1} \in \mathbb{Z}^*,\ \ell_s \in \mathbb{N}^*.$$

Commentaires picturaux : *Le premier dessin de l'introduction représente F et ses images par les éléments de $\Gamma(2)$, vus après application de l'homographie $h : z \mapsto (z-i)/(z+i)$. Quant à l'arbre pour paramétrer $\mathcal{T}$, il commence ainsi :*