Développements

Maxence Jauberty

August 13, 2024

Abstract

Ce document contient des développements mathématiques faits pour me faire réviser de nombreuses notions, dans un but de préparer une agrégation.

Contents

1 Demi-plan de Poincaré

Définition 1. *On appelle* demi-plan de Poincaré *l'ensemble suivant*

$$\mathcal{H} = \{z \in \mathbb{C} \mid \Im(z) > 0\} \cup \{\infty\}. \tag{1}$$

Sur le demi-plan de Poincaré, les droites, ou plus exactement les géodésiques, sont définies comme les demi-cercles dont le centre est sur l'axe des réels et les droites verticales, i.e. les droites passant par ∞. On notera $\mathcal{D}$ l'ensemble de ces géodésiques. On considère l'ensemble des transformations projectives inversibles, soit l'ensemble $PGL_2(\mathbb{R})$. De telles transformations ont la propriété de "préserver" l'infini. Autrement dit, pour $f \in PGL_2(\mathbb{R})$, on a $f(\infty) = \infty$. Pour tout autre point de $\mathbb{P}_1(\mathbb{C})$, f peut être considérée comme une transformation linéaire. On parle alors de *transformation de Moebius.*

Lemme 1. *Soient $z, w \in \mathcal{H}$, il existe une unique droite géodésique de $\mathcal{H}$ passant par z et w.*

Proposition 1. *$PSL_2(\mathbb{R})$ agit sur $\mathcal{H}$. De plus, il agit transitivement.*

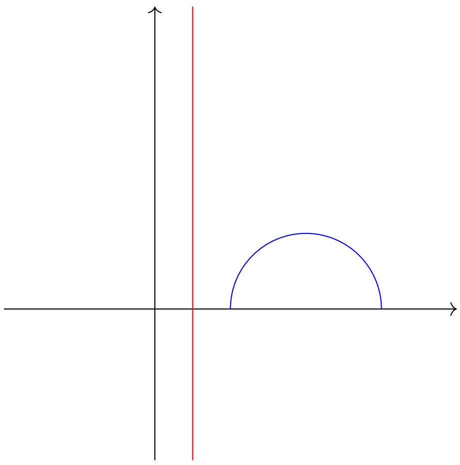

Figure 1: Exemple de géodésiques sur le demi-plan de Poincaré, à noter que les points qui sont sur l'axe des réels sont exclus des géodésiques.

2 Nombre moyen de points fixes

On considère la variable aléatoire Σ sur les permutations de $[n]$ qui suit une loi uniforme, i.e. $\forall \sigma \in \mathfrak{S}_n, \mathbb{P}(\Sigma = \sigma) = \frac{1}{n!}$. Notons $P(\Sigma)$ la variable aléatoire qui compte le nombre de points fixes de Σ. Nous souhaitons calculer l'espérance de $P(\Sigma)$, ainsi que sa variance.

Nous rappelons que $\mathfrak{S}_n$ est un groupe agissant sur $[n]$. Dès lors, nous pouvons espérer utiliser la théorie des actions de groupes.

Si on considère un groupe fini G agissant sur un ensemble X, on note X/G l'ensemble des orbites de X sous l'action de G et $\mathrm{Fix}(g)$ l'ensemble $\{x \in X,\ g.x = x\}$. Nous rappelons la formule de Burnside.

Théorème 1. *Soit G un groupe fini agissant sur un ensemble fini X. On a alors*

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)|. \tag{2}$$

On peut réécrire cette formule dans le cas où $X = [n]$ et $G = \mathfrak{S}_n$. On a alors

$$|[n]/\mathfrak{S}_n| = \sum_{\sigma \in \mathfrak{S}_n} \frac{P(\sigma)}{n!} = \mathbb{E}(P(\Sigma)). \tag{3}$$

Rappelons que l'action de $\mathfrak{S}_n$ sur $[n]$ est transitive, i.e. pour tout couple i, j il existe $\sigma \in \mathfrak{S}_n$ tel que $\sigma(x) = y$. Dès lors, on a $|[n]/\mathfrak{S}_n| = 1$. On en déduit alors que

$$\mathbb{E}(P(\Sigma)) = 1. \tag{4}$$

On peut également calculer la variance de $P(\Sigma)$.

$$\mathbb{E}(P(\Sigma)^2) = \sum_{\sigma \in \mathfrak{S}_n} \frac{P(\sigma)^2}{n!}. \tag{5}$$

3 Lemme de Zolotarev

Si X est un ensemble fini quelconque, nous notons $\mathfrak{S}_X$ le groupe des permutations de X. Nous rappelons qu'il existe un unique morphisme surjectif $\epsilon : \mathfrak{S}_X \longrightarrow \{-1, 1\}$ appelé signature.

Théorème 2. *Il existe un unique morphisme signature de $\mathfrak{S}_X$.*

Proof. On commence par montrer l'existence. On note $n = |X|$ et on considère l'application suivante

$$\Delta : \begin{cases} \mathbb{Z}^n & \longrightarrow \{-1, 1\} \\ (x_1, \dots, x_n) & \longmapsto \prod_{1 \leq i < j \leq n}^n x_j - x_i. \end{cases} \tag{6}$$

On peut faire agir $\mathfrak{S}_n$ sur l'ensemble des applications $\mathbb{Z}^n \to \mathbb{Z}$ par l'action suivante

$$\sigma \cdot f(x_1, \dots, x_n) = f(x_{\sigma(1)}, \dots, x_{\sigma(n)}). \tag{7}$$

On remarque ensuite que l'action d'une transposition sur Δ est d'en changer le signe.

Lemme 2. *Soit τ une transposition, alors $\tau \cdot \Delta = -\Delta$.*

On peut ensuite définir le morphisme ϵ_n comme le signe de Δ. Celui-ci est bien un morphisme car pour une transposition τ, on a

$$\epsilon_n(\sigma\tau) = \epsilon_n(\sigma)\epsilon_n(\tau) = -\epsilon_n(\sigma). \tag{8}$$

Or $\mathfrak{S}_n$ est engendré par les transpositions, donc ϵ_n est bien un morphisme de groupes. Par ailleurs, il est bien surjectif puisque $\epsilon_n(\tau) = -1$.
Il existe un isomorphisme de groupes entre $\mathfrak{S}_X$ et $\mathfrak{S}_n$. On note f un isomorphisme entre ces deux groupes. On peut donc définir $\epsilon = f \circ \epsilon_n$ qui est un morphisme signature.

Montrons que ce morphisme est unique. Soit ϵ' un autre morphisme signature non trivial, i.e. $\epsilon'(\tau) = -1$. Puisque $\mathfrak{S}_X$ est engendré par les transpositions, il existe pour $\sigma \in \mathfrak{S}_X$ une suite de transpositions $\tau_1, \dots, \tau_k$ telles que $\sigma = \tau_1 \dots \tau_k$. On a alors

$$\epsilon'(\sigma) = \epsilon'(\tau_1) \dots \epsilon'(\tau_k) = (-1)^k = \epsilon(\sigma). \tag{9}$$

□

Le lemme de Zolotarev est une conséquence directe de ce théorème.

Théorème 3. *Soit p premier et $a \in \mathbb{Z}/p\mathbb{Z}^\times$, on définit $\mathfrak{m}_a$ comme la multiplication par a dans $\mathbb{Z}/p\mathbb{Z}^\times$, i.e.*

$$\mathfrak{m}_a : \begin{cases} \mathbb{Z}/p\mathbb{Z}^\times & \longrightarrow \mathbb{Z}/p\mathbb{Z}^\times \\ x & \longmapsto ax. \end{cases} \tag{10}$$

Alors, $\mathfrak{m}_a$ *est une permutation de* $\mathbb{Z}/p\mathbb{Z}^\times$ *de signature* $\epsilon(\mathfrak{m}_a) = \left(\frac{a}{p}\right)$.

Proof. $\mathfrak{m}_a$ est une permutation car $\mathbb{Z}/p\mathbb{Z}$ est un corps, la bijection inverse est alors $\mathfrak{m}_{a^{-1}}$.

On peut ensuite remarquer que le symbole de Legendre est un morphisme de groupes de $\mathbb{Z}/p\mathbb{Z}^\times$ dans $\{-1, 1\}$ non trivial et surjectif. Cela conclut la preuve : $\epsilon(\mathfrak{m}_a) = \left(\frac{a}{p}\right)$. □

Le lemme de Zolotarev permet de faire un pont entre la théorie des nombres et la théorie des permutations. Si on considère, par exemple, $\mathfrak{m}_2$ peut se représenter comme la permutation suivante

$$\begin{pmatrix} 1 & 2 & \dots & \frac{p-1}{2} & \frac{p+1}{2} & \dots & p-2 & p-1 \\ 2 & 4 & \dots & p-1 & p+1 & \dots & p-4 & p-2 \end{pmatrix}. \tag{11}$$

On remarque que l'inversion se fait à partir de $\frac{p+1}{2}$ et $\epsilon(\mathfrak{m}_2) = (-1)^{\text{nb d'inversion}}$ donc

$$\epsilon(\mathfrak{m}_2) = (-1)^{\frac{p-1}{2} + \dots + 2 + 1}. \tag{12}$$

Il ne suffit que de calculer, $\frac{p-1}{2} + \dots + 2 + 1 = \frac{p^2-1}{8}$, d'où

$$\left(\frac{2}{p}\right) = \epsilon(\mathfrak{m}_2) = (-1)^{\frac{p^2-1}{8}}. \tag{13}$$