Développements

Maxence Jauberty

August 19, 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.*

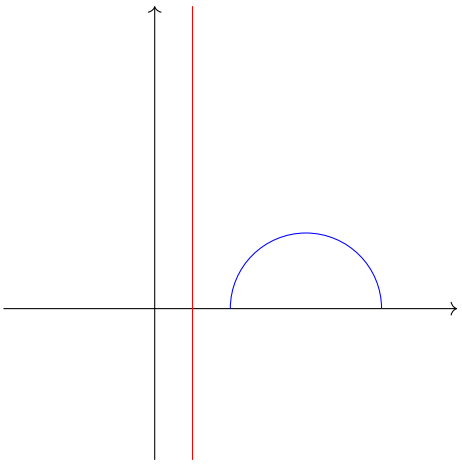

Figure 1: Exemple de géodésiques sur le demi-plan de Poincaré, à noter que les points qui sont sur l'axe des réels sont exclus des géodésiques.

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

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

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

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

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

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 $\tau_1, \ldots, \tau_k$ telles que $\sigma = \tau_1 \ldots \tau_k$. On a alors

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

□

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

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

Une application

On peut utiliser le lemme de Zolotarev pour démontrer la loi de réciprocité quadratique.

Théorème 4. *Soit p et q deux nombres premiers impairs, alors*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}. \tag{14}$$

Proof. D'abord, nous considérons l'isomorphisme $\phi : \mathbb{Z}_{pq} \longrightarrow \mathbb{Z}_p \times \mathbb{Z}_q$. On considère les deux permutations suivantes

$$\sigma : \begin{cases} \mathbb{Z}_p \times \mathbb{Z}_q & \longrightarrow \mathbb{Z}_p \times \mathbb{Z}_q \\ (x, y) & \longmapsto (qx + y, y) \end{cases} \tag{15}$$

$$\tau : \begin{cases} \mathbb{Z}_p \times \mathbb{Z}_q & \longrightarrow \mathbb{Z}_p \times \mathbb{Z}_q \\ (x, y) & \longmapsto (x, py + x) \end{cases}. \tag{16}$$

On définit ensuite ρ sur $\mathbb{Z}_{pq}$ par $\rho(x + qy) = px + y$. On peut alors remarquer que

$$\phi(qx + y) = (qx + y, y) = \sigma(x, y) \text{ et } \phi(px + y) = (x, py + x) = \tau(x, y). \tag{17}$$

Ainsi, $qx + y = \phi^{-1}(\sigma(x, y))$ et en appliquant ρ, on obtient $\rho(\phi^{-1}(\sigma(x, y))) = px + y$. Finalement, en appliquant ϕ, déduit l'égalité suivante

$$\phi \circ \rho \circ \phi^{-1} \circ \sigma = \tau. \tag{18}$$

Désormais, on peut considère les signatures de ces permutations.

$$\epsilon(\phi \circ \rho \circ \phi^{-1})\epsilon(\sigma) = \epsilon(\tau). \tag{19}$$

On sait que $\epsilon(\sigma) = \left(\frac{q}{p}\right)$ et $\epsilon(\tau) = \left(\frac{p}{q}\right)$. (A faire) De plus, $\epsilon(\phi \circ \rho \circ \phi^{-1}) = (-1)^{\frac{(p-1)(q-1)}{4}}$, d'où la loi de réciprocité

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}. \tag{20}$$

□

Une généralisation

Théorème 5. *Soit E un espace vectoriel sur un corps fini $\mathbb{F}_p$, alors pour tout automorphisme u de E, on a*

$$\epsilon(u) = \left(\frac{\det(u)}{p}\right). \tag{21}$$

où ϵ est le morphisme signature de $GL(E)$.

Proof. Remarquons que $SL(E)$ est le groupe dérivé de $GL(E)$. On en déduit que tout morphisme de $GL(E)$ vers un groupe abélien se factorise à travers l'abélianisé $GL(E)/SL(E)$. En particulier, si nous considérons le morphisme signature de $\mathfrak{S}_E$, nous avons l'existence de $f : \mathbb{F}_p^\times \longrightarrow \{-1, 1\}$ tel que $\epsilon = f \circ \det$ sur $GL(E)$.

De plus, f n'est pas un morphisme trivial, on peut, par exemple, prendre la multiplication par un élément générateur de $\mathbb{F}_p^\times$. Cet automorphisme est une permutation circulaire, ce qui permet simplement de déterminer que sa signature est -1. On en déduit que f n'est pas le morphisme trivial, donc $f = \left(\frac{\cdot}{p}\right)$ par unicité du symbole de Legendre. D'où

$$\epsilon(u) = \left(\frac{\det(u)}{p}\right). \tag{22}$$

□

4 Matrices stochastiques

Définition 2. *Une matrice $M \in \mathcal{M}_n(\mathbb{R})$ est dite stochastique si elle vérifie les conditions suivantes*

1. $M_{ij} \geq 0$ *pour tout* $i, j \in \{1, \dots, n\}$.
2. $\sum_{j=1}^{n} M_{ij} = 1$ *pour tout* $i \in \{1, \dots, n\}$.

Remarque 1. *Les matrices stochastiques sont souvent utilisées pour modéliser des chaînes de Markov en probabilités.*

En particulier, on peut définir une relation d'équivalence sur les états possibles de la chaîne de Markov associée à une matrice stochastique.

Définition 3. *Soit M une matrice stochastique, on définit la relation d'équivalence $\longleftrightarrow$ sur $\{1, \dots, n\}$ par*

$$i \leftrightarrow j \iff \exists k, k' \in \mathbb{N}, (e_i M^k)_j > 0 \text{ et } (e_j M^{k'})_i > 0. \tag{23}$$

On dit alors que i et j communiquent.

Remarque 2. *Si on considère un vecteur de probabilité ν_k qui représente la loi des états de la chaîne à un étape k, alors $\nu_{k+1} = \nu_k M$. On en déduit que $\nu_k = \nu_0 M^k$. Si $\nu_0 = e_i$, alors on étudie la chaîne qui part de l'état i, idem pour j. Si $i \longleftrightarrow j$, alors il est possible de passer de i à j en un nombre fini d'étapes, et réciproquement.*

Définition 4. *Soit M une matrice stochastique, elle est dite irréductible s'il n'existe qu'une unique classe d'équivalence pour la relation $\longleftrightarrow$.*

Remarque 3. *On peut montrer que si M est irréductible, alors pour tout $i, j \in \{1, \dots, n\}$, il existe $k \in \mathbb{N}$ tel que $(e_i M^k)_j > 0$. C'est une conséquence directe de la définition d'irréductibilité. On retrouve la définition classique de l'irréductibilité.*

En particulier, une propriété intéressante pour l'étude des chaînes de Markov est l'invariance de la mesure de probabilité. Dans le cas fini, comme nous l'étudions, cela revient le "bon" vecteur de probabilité initial qui assure la stabilité de la mesure.

$$\nu M = \nu. \tag{24}$$

Le problème de trouver une telle distibution initiale est finalement une recherche de vecteur propre associé à la valeur propre 1. Nous allons montrer par le théorème de Perron-Frobenius qu'une chaîne de Markov irréductible admet un tel vecteur propre, unique à une constante près.

Théorème 6 (Perron-Frobenius)**.** *Soit M une matrice stochastique irréductible, alors*

1. 1 *est valeur propre de* M*.*
2. *Il existe un unique vecteur propre à coefficients positifs de* M *associé à la valeur propre* 1 *à une constante près.*
3. *Toutes les valeurs propres de* M *sont de module strictement inférieur à* 1*.*

Proof. □

5 Formule de Mobius et dénombrements des polynômes irréductibles

Définition 5. *Soit $n \in \mathbb{N}$, on définit la fonction de Möbius $\mu : \mathbb{N} \to \mathbb{Z}$ par*

$$\mu(n) = \begin{cases} 0 & \text{si } n \text{ n'est pas produit de carrés,} \\ (-1)^k & \text{si } n \text{ est produit de } k \text{ nombres premiers distincts.} \end{cases} \tag{25}$$

Proposition 2. *Soit $n \geq 2$, alors*

$$\sum_{d|n} \mu(d) = 0. \tag{26}$$

Proof. On décompose n en produit de facteurs premiers

$$n = \prod_{i=1}^{k} p_i^{\alpha_i}. \tag{27}$$

On peut ensuite décomposer la somme, en tenant compte que $\mu(d) = 0$ si deux diviseurs premiers divisent d,

$$\sum_{d|n} = \mu(1) + \sum_{i=1}^{k} \mu(p_i) + \sum_{i \neq j} \mu(p_i p_j) + \ldots + \mu(p_1 \ldots p_n) \tag{28}$$

$$= \sum_{k=0}^{n} (-1)^k \binom{n}{k} \tag{29}$$

$$= 0. \tag{30}$$

□

Théorème 7 (Formule d'inversion de Möbius)**.** *Soit f une fonction arithmétique, on pose $g(n) = \sum_{d|n} f(d)$. Alors, on a*

$$f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right). \tag{31}$$

Proof. On a

$$\sum_{d|n} \mu(d) g\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \sum_{e|\frac{n}{d}} f(e) \tag{32}$$

$$= \sum_{de|n} f(e)\mu(d) \tag{33}$$

$$= \sum_{e|n} f(e) \sum_{d|\frac{n}{e}} \mu(d) \tag{34}$$

$$= f(n). \tag{35}$$

car $\sum_{d|\frac{n}{e}} \mu(d)$ vaut 0 si $e \neq n$ et 1 sinon. □

Application aux dénombrements de polynômes irréductibles sur $\mathbb{F}_q$

Définition 6. *Soit $\mathbb{K}$ un corps, un polynôme f de $\mathbb{K}[x]$ est dit irréductible si il n'est pas le produit de deux polynômes non inversibles de $\mathbb{K}[x]$, i.e.*

$$f = gh \implies g \in \mathbb{K}[x]^\times \text{ ou } h \in \mathbb{K}[x]^\times. \tag{36}$$

Proposition 3. *Soit q une puissance d'un nombre premier. On note $I(n,q)$ l'ensemble des polynômes irréductibles unitaires de degré n sur $\mathbb{F}_q$. Alors, on a*

$$x^{q^n} - x = \prod_{d|n} \left(\prod_{f \in I(d,q)} f \right) \tag{37}$$

Proof. Soit $d|n$, on considère $g \in I(d,q)$. On considère ensuite K le corps de rupture de g sur $\mathbb{F}_q$. K est une extension de degré d qui sera isomorphe à $\mathbb{F}_{q^d}$, en considérant K comme $\mathbb{F}_q-$ev de dimension d (en prenant α comme élément primitif). On sait que $\alpha^{q^d} = \alpha$ donc α est une racine de $x^{q^n} - x$. On en déduit donc que f divise $x^{q^n} - x$.

Réciproquement, supposons que f est un facteur irréductible de $x^{q^n} - x$. On note d le degré de f. Par ailleurs, f est scindé dans $\mathbb{F}_{q^n}$ donc les racines de f sont dans $\mathbb{F}_{q^n}$. En particulier, si on considère le corps de rupture K de f sur F_q, on sait que K est une extension de $\mathbb{F}_q$ de degré d.

$$\mathbb{F}_q \subset K \cong \mathbb{F}_{q^d} \subset \mathbb{F}_{q^n}. \tag{38}$$

On peut aussi construire $\mathbb{F}_{q^n}$ comme un corps de rupture pour un polynôme irréductible de degré k, d'où

$$[\mathbb{F}_{q^n} : \mathbb{F}_q] = [\mathbb{F}_{q^n} : \mathbb{F}_{q^d}][\mathbb{F}_{q^d} : \mathbb{F}_q]. \tag{39}$$

D'où $d|n$. □

Théorème 8.

$$|I(n,q)| = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d. \tag{40}$$

Proof. Utilisons la Proposition 3 et comparons les degrés de chaque côté :

$$q^n = \sum_{d|n} |I(d,q)| d. \tag{41}$$

Appliquons ensuite la formule d'inversion avec $n \mapsto |I(n,q)|$. On en déduit que

$$n|I(n,q)| = \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d. \tag{42}$$

Il suffit ensuite de diviser par n des deux côtés pour obtenir le résultat attendu

$$|I(n,q)| = \frac{1}{n}\sum_{d|n} \mu\left(\frac{n}{d}\right) q^d. \tag{43}$$

□

Remarque 4. *On récupère aussi un équivalent de* $|I(n,q)|$.

$$|I(n,q)| \sim \frac{q^n}{n}. \tag{44}$$

Pour cela, il suffit de remarquer les inégalités suivantes

$$\begin{aligned}
|\frac{1}{n}\sum_{d|n,d<n} \mu\left(\frac{n}{d}\right) q^d| &\leq \frac{1}{n}\sum_{d|n,d<n} |\mu\left(\frac{n}{d}\right) q^d| && (45)\\
&\leq \frac{1}{n}\sum_{d|n,d<n} q^d && (46)\\
&\leq \frac{1}{n}\sum_{d=1} q^{\lfloor \frac{n}{2} q^d \rfloor} && (47)\\
&= \frac{1}{n}\frac{q^{\lfloor \frac{n}{2} q^d \rfloor + 1} - 1}{q-1} && (48)
\end{aligned}$$

qui est un $o(q^n)$. *Ainsi,* $|I(n,q)| = \frac{q^n}{n} + o(q^n)$, *d'où* $|I(n,q)| \sim \frac{q^n}{n}$.