Développements

Maxence Jauberty

September 15, 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

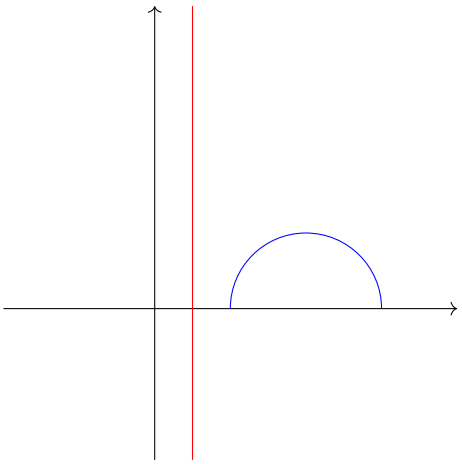

Figure 1: Exemple de géodésiques sur le demi-plan de Poincaré, à noter que les points qui sont sur l'axe des réels sont exclus des géodésiques.

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.*

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

6 Lemmes de Borel-Cantelli et applications à l'étude des nombres premiers

Premier lemme

Lemme 3. *Soit (A_n) une suite d'évènements tels que $\sum_{n\in\mathbb{N}} \Pr(A_n) < \infty$, alors $\mathbb{P}(A) = 0$ en notant $A = \limsup_n A_n$.*

Proof. A est aussi égal à $\bigcap_{n\in\mathbb{N}} \bigcup_{k\geq n} A_k$. On a alors $\mathbb{P}(A) = \lim_{n\to\infty} \mathbb{P}\left(\bigcup_{k\geq n} A_k\right)$. Or, $\mathbb{P}\left(\bigcup_{k\geq n} A_k\right) \leq \sum_{k\geq n} \mathbb{P}(A_k)$. En passant à la limite, on obtient $\mathbb{P}(A) = 0$. □

Une application du premier lemme est :

Proposition 4. *Soit X_n une suite de variables aléatoires et X une variable aléatoire discrète. On pose $A_n(\epsilon) = \{|X_n - X| > \epsilon\}$. Si pour tout $\epsilon > 0$, $\sum_{n\in\mathbb{N}} \Pr(A_n(\epsilon)) < \infty$, alors X_n converge presque sûrement vers X.*

Proof. Pour tout ϵ, on note $A(\epsilon) = \limsup_n A_n(\epsilon)$. D'après les hypothèses et le premier lemme de Borel-Cantelli, on a $\mathbb{P}(A(\epsilon)) = 0$ pour tout ϵ. On a alors

$$\mathbb{P}\left(\bigcup_{n\in\mathbb{N}} A\left(2^{-n}\right)\right) \leq \sum_{n\in\mathbb{N}} \mathbb{P}(A\left(2^{-n}\right)) = 0. \tag{49}$$

Par complémentaire, on a $\mathbb{P}(\bigcap_{n\in\mathbb{N}} \overline{A\left(2^{-n}\right)}) = 1$. Soit

$$\mathbb{P}(\bigcap_{n\in\mathbb{N}} \bigcup_{j\in\mathbb{N}} \bigcap_{k\geq j} \{|X_j - X| \leq 2^{-k}\}) = 1. \tag{50}$$

Ce qui permet de conclure que X_n converge presque sûrement vers X.

□

Deuxième lemme

Lemme 4. *Soit (A_n) une suite d'évènements indépendants. Si $\sum_{n\in\mathbb{N}} \mathbb{P}(A_n) = \infty$, alors $\mathbb{P}(A) = 1$ en notant $A = \limsup_n A_n$.*

Proof. Pour commencer, on va considérer le complémentaire de A, que l'on va noter B, donc

$$B = \bigcup_{n\in\mathbb{N}} \bigcap_{k\geq n} \overline{A_k}. \tag{51}$$

Remarquons que $\left(\bigcap_{k\geq n} \overline{A_k}\right)$ est une suite croissante d'évènements. On a alors

$$\mathbb{P}\left(\bigcup_{n\in\mathbb{N}} \bigcap_{k\geq n} \overline{A_k}\right) = \lim_{n\to\infty} \mathbb{P}\left(\bigcap_{k\geq n} \overline{A_k}\right). \tag{52}$$

Or, $\mathbb{P}\left(\bigcap_{k\geq n}\overline{A_k}\right) = \prod_{k\geq n}\mathbb{P}(\overline{A_k}) = \prod_{k\geq n}(1-\mathbb{P}(A_k))$. On peut alors appliquer l'inégalité de convexité suivante : $1-x \leq e^{-x}$.

$$\prod_{k\geq n}\mathbb{P}(\overline{A_k}) \leq \prod_{k\geq n} e^{-\mathbb{P}(A_k)} = e^{-\sum_{k\geq n}\mathbb{P}(A_k)}. \tag{53}$$

On peut aussi remarquer que $\lim_n -\sum_{k\geq n}\mathbb{P}(A_k) = -\infty$ puisqu'il s'agit du reste d'une suite divergente. Ainsi,

$$\lim_n \prod_{k\geq n}\mathbb{P}(\overline{A_k}) = 0. \tag{54}$$

Et donc, $\mathbb{P}(B) = 0$, ce qui permet de conclure que $\mathbb{P}(A) = 1$. □

On peut appliquer ce lemme pour démontrer la fameuse expérience de pensée des singes de Shakespeare.

Proposition 5. *Un singe tape au hasard sur un clavier (de 26 lettres) pour un temps infini. Alors on trouvera, presque sûrement, Hamlet dans le texte tapé.*

Proof. On suppose que la longueur de Hamlet est l. On note A_n l'évènement "Hamlet" est tapé entre les n et $n+l-1$ lettres. Les A_n sont indépendants et $\mathbb{P}(A_n) = 26^{-l}$. Et donc, $\sum_{n\in\mathbb{N}}\mathbb{P}(A_n) = \infty$. En utilisant le deuxième lemme, on a que $\mathbb{P}(A) = 1$ où $A = \limsup_n A_n$. C'est-à-dire que

$$\mathbb{P}\left(\bigcap_n \bigcup_{k\geq n} A_k\right) = 1. \tag{55}$$

Ce qui signifie que Hamlet sera presque sûrement tapé. □

Proposition 6. *Il n'existe pas de probabilité $\mathbb{P}$ sur $(\mathbb{N}^*, \mathcal{P}(\mathbb{N}^*))$ telle que $\mathbb{P}(n\mathbb{N}^*) = \frac{1}{n}$.*

Proof. Notons $A_n = n\mathbb{N}^*$ Supposons qu'une telle probabilité existe. Remarquons que si p et q deux premiers distincts, alors $A_p \cap A_q = A_{pq}$. En effet, on a généralement que $A_p \cap A_q \subset A_{pq}$ mais puisque p et q sont premiers, on a que $A_{pq} \subset A_p \cap A_q$ (plus généralement, cela est vrai pour deux nombres premiers entre eux). Par définition,

$$\mathbb{P}(A_p \cap A_q) = \mathbb{P}(A_{pq}) = \frac{1}{pq} = \mathbb{P}(A_p)\mathbb{P}(A_q). \tag{56}$$

On remarquera que pour un nombre arbitraire de premiers distincts, les A_p seront indépendants. Notons $p_1, ..., p_n, ...$ les nombres premiers rangés dans l'ordre croissant.

On sait que $\sum_{k=1}^{\infty}\frac{1}{p_k} = \infty$ donc d'après le deuxième lemme, on a que

$$\mathbb{P}\left(\limsup_n A_{p_n}\right) = 1. \tag{57}$$

Remarquons qu'il n'existe qu'un seul entier multiples d'une infinité de nombre premiers, il s'agit de 0 (ici exclu). De plus, $\limsup_n A_{p_n} \subset \{\text{entier multiple d'une infinité de premiers} = \emptyset\}$. On obtient une contradiction

$$\mathbb{P}\left(\limsup_n A_{p_n}\right) = \mathbb{P}(\emptyset) = 1. \tag{58}$$

Il n'existe donc pas de probabilité $\mathbb{P}$ sur $(\mathbb{N}^*, \mathcal{P}(\mathbb{N}^*))$ telle que $\mathbb{P}(n\mathbb{N}^*) = \frac{1}{n}$. □

On rappelle une preuve de la divergence de la série des inverses de nombres premiers, autant le faire avec des probabilités.

Proposition 7. *La série $\sum_{n\in\mathbb{N}} \frac{1}{p_n}$ diverge.*

Proof. On définit la probabilité suivante pour $s > 1$:

$$\mathbb{P}(\{n\}) = \frac{1}{\zeta(s)}\frac{1}{n^s} \tag{59}$$

où ζ est la fonction zêta de Riemann. On peut alors montrer que $\mathbb{P}$ est bien une probabilité. On reprend la notation A_p pour $p\mathbb{N}^*$. Remarquons déjà que pour un ensemble B, on a

$$\mathbb{P}(B) = \sum_{n\in B} \mathbb{P}(\{n\}) = \frac{1}{\zeta(s)} \sum_{n\in B} \frac{1}{n^s}. \tag{60}$$

En particulier, pour A_p avec p premier, on a

$$\mathbb{P}(A_p) = \frac{1}{\zeta(s)} \sum_{n\in p\mathbb{N}^*} \frac{1}{n^s} = \frac{1}{\zeta(s)} \sum_{n\in\mathbb{N}^*} \frac{1}{(pn)^s} = \frac{1}{p^s}. \tag{61}$$

On considère $q_1, ..., q_k$ un ensemble de nombres de premiers distincts

$$\mathbb{P}\left(\bigcap_{i=1}^k A_{q_i}\right) = \sum_{n\in\bigcap_{i=1}^k A_{q_i}} \mathbb{P}(\{n\}) \tag{62}$$

$$= \frac{1}{\zeta(s)} \sum_{n\in\mathbb{N}^*} \frac{1}{(q_1 \dots q_k n)^s} \tag{63}$$

$$= \prod_{i=1}^k \frac{1}{q_i^s} \qquad = \prod \mathbb{P}(A_{q_i}). \tag{64}$$

On en déduit que les (A_{p_i}) sont indépendants. Notons B l'ensemble des entiers qui ne sont multiples d'aucun nombre premier.

$$\mathbb{P}(B) = \mathbb{P}(\{1\}) + \mathbb{P}(B \setminus \{1\}) = \frac{1}{\zeta(s)} \tag{65}$$

car $\mathbb{P}(B \setminus \{1\}) = \mathbb{P}(\emptyset)$. Mais par définition :

$$\mathbb{P}(B) = \mathbb{P}\left(\bigcap_{k\geq 1} \overline{A_{p_k}}\right) \tag{66}$$

d'où

$$\mathbb{P}(B) = \prod_{k\geq 1} 1 - \frac{1}{p_k^s} = \frac{1}{\zeta(s)}. \tag{67}$$

Appliquons un logarithme :

$$-\log(\zeta(s)) = \sum_{k\geq 1} \log\left(1 - \frac{1}{p_k^s}\right). \tag{68}$$

Or, $\log(1-x) \leq -x$ pour $x \in [0,1]$ donc

$$-\log(\zeta(s)) \geq -\sum_{k\geq 1} \frac{1}{p_k^s}. \tag{69}$$

On en déduit

$$\log(\zeta(s)) \leq \sum_{k\geq 1} \frac{1}{p_k^s} \leq \sum_{k\geq 1} \frac{1}{p_k}. \tag{70}$$

Or, $\zeta(s)$ tend vers l'infini quand s tend vers 1, donc la série $\sum_{k\geq 1} \frac{1}{p_k}$ diverge. □

7 Composantes connexes de $\mathcal{GL}_n(\mathbb{R})$

Abstract

On montre que

Définition 7. *Une partie d'un espace topologique X est dite connexe par arcs si pour tout x, y dans X, il existe une application continue $\gamma : [0,1] \to X$ telle que $\gamma(0) = x$ et $\gamma(1) = y$.*

Remarque 5. *On appelera γ un chemin de x à y dans X. Sur le dessin, cela revient à montrer que l'on peut tracer un chemin continu n'importe quel couple de points.*

On pourra également considérer la relation d'équivalence $\longleftrightarrow$ sur X définie par

$$x \longleftrightarrow y \iff \exists \gamma : [0,1] \to X \text{ telle que } \gamma(0) = x \text{ et } \gamma(1) = y. \tag{71}$$

Pour un $x \in X$ donné, on pourra appelé $\mathcal{C}(x)$ la composante connexe par arcs de x. Dire que X est connexe par arcs est équivalent à dire que pour un $x \in X$, $\mathcal{C}(x) = X$.

Lemme 5. *Si f est une application continue de X dans Y, deux espaces topologiques, et que X est connexe par arcs, alors $f(X)$ est connexe par arcs dans Y.*

Proof. Soient $f(x_1), f(x_2) \in f(X)$. X est connexe par arcs donc il existe γ un chemin de x_1 vers x_2. $f \circ \gamma$ est alors un chemin de $f(x_1)$ vers $f(x_2)$. □

Proposition 8. *$\mathcal{GL}_n(\mathbb{R})$ n'est pas connexe par arcs.*

Proof. On remarquera que det est une application linéaire surjective et continue de $\mathcal{GL}_n(\mathbb{R})$ dans $\mathbb{R}^*$. Or, $\mathbb{R}^*$ n'est pas connexe par arcs. Par contraposée du lemme précédent, $\mathcal{GL}_n(\mathbb{R})$ n'est pas connexe par arcs. □

Nous allons en fait montrer que $\mathcal{GL}_n(\mathbb{R})$ admet deux composantes connexes par arcs.

Lemme 6. *$\mathcal{O}_n(\mathbb{R})$ admet deux composantes connexes par arcs, $\mathcal{O}_n^+$ et $\mathcal{O}_n^-$.*

Evidemment, $\mathcal{O}_n(\mathbb{R})$ n'est pas connexe par arcs. Simplement car un espace discret ne peut être connexe par arcs que s'il est réduit à un singleton, ce qui n'est pas le cas de $\det(\mathcal{O}_n(\mathbb{R}))$.

Proof. On note $R(\theta)$ une matrice de rotation θ. Soit $A \in \mathcal{O}_n^+(\mathbb{R})$. On sait qu'il existe une matrice orthogonale P telle que $A = PDP^{-1}$ où $D = \mathrm{Diag}(I_r, R(\pi), \ldots, R(\pi), R(\theta_1), \ldots, R(\theta_p))$.
On considère δ un chemin de π à 0. On pose $\Delta(t) = \mathrm{Diag}(I_r, R(\delta(t)), \ldots, R(\delta(t)))$.
Ensuite, on considère γ_i un chemin de θ_i à 0 dans $]-\pi, \pi[$.

On finit par poser $\Gamma(t) = P\text{Diag}(\Delta(t), R(\gamma_1(t)), \ldots, R(\gamma_p(t)))P^{-1}$. On a $\Gamma(0) = A$ et $\Gamma(1) = I_n$. $\theta \mapsto R(\theta)$ est continue, on en déduit que $t \mapsto \Delta(t)$ et $t \mapsto \Gamma(t)$ sont continues aussi. On conserve la forme de "diagonale de rotation" ce qui permet d'assurer que Γ est à valeurs dans $\mathcal{O}_n(\mathbb{R})$.

$$\det(\Gamma(t)) = \underbrace{\det(\Delta(t))}_{=1 \text{ ou } =(-1)^{2m}=1} \prod_{i=1}^{p} \underbrace{\det(R(\gamma_i(t)))}_{=1} = 1. \tag{72}$$

On a donc trouvé un chemin de A à I_n, ce qui suffit à montrer que $\mathcal{O}_n^+(\mathbb{R})$ est connexe par arcs.

La même démonstration se fait en créant un chemin vers $-1, \mathrm{I_{n-1}}$.

Finalement, il ne suffit que de montrer que $\mathcal{O}_n^+(\mathbb{R})$ et $\mathcal{O}_n^-(\mathbb{R})$ forment une partition de $\mathcal{O}_n(\mathbb{R})$, ce qui est trivial. On a donc montré que $\mathcal{O}_n(\mathbb{R})$ admet deux composantes connexes par arcs, $\mathcal{O}_n^+(\mathbb{R})$ et $\mathcal{O}_n^-(\mathbb{R})$. □

Lemme 7. *On note $\mathcal{S}_n^{++}(\mathbb{R})$ l'ensemble des matrices symétriques définies postives. Alors $\mathcal{S}_n^{++}(\mathbb{R})$ est connexe par arcs.*

Proof. La preuve est plus simple. On considère $A \in \mathcal{S}_n^{++}(\mathbb{R})$. D'après le théorème spectral, il existe une matrice orthogonale P telle que $A = PDP^{-1}$ avec $D = \text{Diag}(\lambda_1, \ldots, \lambda_n)$ et $\lambda_i > 0$. (Réciproquement, une matrice d'une telle forme est symétrique définie positive).
$\mathbb{R}_+^*$ est connexe par arcs donc il existe un chemin γ_i de λ_i) 1 dans $\mathbb{R}_+^*$. On pose ensuite $\Gamma(t) = P\text{Diag}(\gamma_1(t), \ldots, \gamma_n(t))P^{-1}$. Γ est continue, à valeurs dans $\mathcal{S}_n^{++}(\mathbb{R})$ et $\Gamma(0) = A$, $\Gamma(1) = I_n$. On a donc trouvé un chemin de A à I_n. $\mathcal{S}_n^{++}(\mathbb{R})$ est donc connexe par arcs. □

Lemme 8 (Décomposition(s) polaire(s))**.** *Soit $A \in \mathcal{GL}_n(\mathbb{R})$. Alors il existe $O \in \mathcal{O}_n(\mathbb{R})$ et $S \in \mathcal{S}_n^{++}(\mathbb{R})$ telles que*

$$A = SO. \tag{73}$$

De plus, si $\det(A) > 0$, alors $O \in \sqcup\rceil\S\sqcup\mathcal{O}_n^+(\mathbb{R})$ et si $\det(A) < 0$, alors $O \in \mathcal{O}_n^-(\mathbb{R})$.

Proof. A est inversible donc A^TA est symétrique définie positive.

$$A = AA^TA^{T^{-1}}. \tag{74}$$

AA^T est symétrique définie positive donc il existe S symétrique définie positive telle que $AA^T = S^2$. D'où $A = SS(A^T)^{-1}$. En posant $O = S(A^T)^{-1}$, on a bien $A = SO$.
Il reste à montrer que O est orthogonale. On a

$$O^TO = (S(A^T)^{-1})^T S(A^T)^{-1} = A^{-1}SS(A^T)^{-1} = I_n. \tag{75}$$

$$OO^T = S(A^T)^{-1}(S(A^T)^{-1})^T = S(A^T)^{-1}A^{-1}S = I_n. \tag{76}$$

Pour la remarque supplémentaire du lemme, on a $\det(A) = \det(S)\det(O)$. Or, $\det(S) > 0$ et $\det(O) = \det(A)$. □

Théorème 9. *$\mathcal{GL}_n(\mathbb{R})$ admet deux composantes connexes par arcs, $\mathcal{O}_n^+(\mathbb{R})\mathcal{S}_n^{++}(\mathbb{R})$ et $\mathcal{O}_n^-(\mathbb{R})\mathcal{S}_n^{++}(\mathbb{R})$.*

Proof. Le théorème est une utilisation de tous ces lemmes. Soit $A \in \mathcal{GL}_n(\mathbb{R})^+$, on considère sa décomposition polaire S, O, donc $O \in \mathcal{O}_n^+(\mathbb{R})$ et $S \in \mathcal{S}_n^{++}(\mathbb{R})$. On note Θ un chemin de O à I_n dans $\mathcal{O}_n^+(\mathbb{R})$ et Σ un chemin de S à I_n dans $\mathcal{S}_n^{++}(\mathbb{R})$. On pose $\Gamma(t) = \Theta(t)\Sigma(t)$. Γ est continue, à valeurs dans $\mathcal{GL}_n(\mathbb{R})^+$ et $\Gamma(0) = A$, $\Gamma(1) = I_n$. On a donc trouvé un chemin de A à I_n. On a donc montré que $\mathcal{GL}_n(\mathbb{R})^+$ est connexe par arcs.

On fait la même preuve pour $\mathcal{GL}_n(\mathbb{R})^-$ en créant un chemin vers $\mathrm{Diag}(-1, I_{n-1})$.

Puisque $\mathcal{GL}_n(\mathbb{R})^+$ et $\mathcal{GL}_n(\mathbb{R})^-$ forment une partition de $\mathcal{GL}_n(\mathbb{R})$, on a montré que $\mathcal{GL}_n(\mathbb{R})$ admet deux composantes connexes par arcs. □

8 Critère d'Eisenstein

Abstract

Le critère d'Eisenstein est un critère d'irréductibilité d'un polynôme. Dans sa forme la plus connue, il s'énonce ainsi : soit $P = \sum_{i=0}^{d} a_i X^i$ un polynôme à coefficients dans $\mathbb{Z}$. S'il existe un nombre premier p tel que p divise tous les coefficients sauf le dernier et que p^2 ne divise pas le premier coefficient, alors P est irréductible dans $\mathbb{Q}[X]$.

Nous en donnerons une généralisation dans le cas des polynômes à coefficients dans un anneau intègre.

Définition 8. *Soit $\mathcal{A}$ un anneau commutatif. Un idéal I est dit premier si pour tous $a, b \in \mathcal{A}$, si $ab \in I$, alors $a \in I$ ou $b \in I$.*

Remarque 6. *De manière équivalente, un idéal I est dit premier si $\mathcal{A}/I$ définit par passage au quotient un anneau intègre.*

Théorème 10 (Critère d'Eisenstein)**.** *Soit $\mathcal{A}$ un anneau intègre. Soit $P = \sum_{i=0}^{d} a_i x^i \in \mathcal{A}[x]$. S'il existe un idéal premier I de $\mathcal{A}$ tel que*

- *$\forall i \in \{0, ..., d-1\}, a_i \in I$,*
- *$a_d \notin I$,*
- *$a_0 \notin I^2$ (c'est-à-dire a_0 n'est pas le carré d'un élément de I),*

Alors P est irréductible dans $\mathcal{A}[x]$.

Proof. Supposons que $P = RQ$ avec $\deg(R) = m$ et $\deg(Q) = d - m$ avec $\deg(R) \geq 1$. Par réduction modulo I (i.e. considérer $\mathcal{A}/I[x]$), on a

$$P = RQ = a_d x^d \bmod I. \tag{77}$$

Or $\mathcal{A}/I$ est intègre donc $\mathcal{A}/I[x]$ est intègre. On en déduit que les réductions de R et Q sont de la forme $R = bx^m \bmod I$ et $Q = cx^{d-m} \bmod I$. En particulier, on en déduit que r_0 et g_0 sont dans I. Puisque $a_0 = r_0 g_0$, on en déduit que $a_0 \in I^2$. Cela contredit l'hypothèse du théorème, on en déduit que P est irréductible. □

Le théorème d'Eisenstein pour les polynômes à coefficients dans $\mathbb{Z}$ est un peu plus fort que le théorème général puisqu'on obtient une irréductibilité dans $\mathbb{Q}[X]$ et non dans $\mathbb{Z}[X]$. C'est l'objet de la proposition suivante, qui montre que les deux théorèmes sont équivalents.

Proposition 9. *Un polynôme $P \in \mathbb{Z}[X]$ est irréductible dans $Q[X]$ si et seulement si il est irréductible dans $\mathbb{Z}[X]$.*

Proof. Bien sûr, si P est irréductible dans $\mathbb{Q}[X]$, il est aussi dans $\mathbb{Z}[X]$. Supposons désormais qu'il le soit dans $\mathbb{Z}[X]$. Supposons qu'il existe $R, Q \in \mathbb{Q}[X]$ tels que $P = RQ$.

Il existe $q, r \in \mathbb{Z}$ tel que $qQ \in \mathbb{Z}[X]$ et $rR \in \mathbb{Z}[X]$. On peut ensuite écrire

$$qrP = qRrQ = c(qR)R'c(rQ)Q' \tag{78}$$

où R', Q' sont des polynômes à coefficients entiers et $c(R), c(Q)$ sont les pgcd des coefficients de R et Q. On en déduit que

$$qrc(P) = c(qR)c(rQ) \tag{79}$$

d'où $qrP = qrc(P)R'Q'$ et finalement que $P = c(P)R'Q'$. En conclusion, P est irréductible dans $\mathbb{Z}[X]$ puisque R', Q' sont de degrés supérieurs à 1, et $c(P)$ n'est qu'une constante entière. □

Corollaire 1 (Critère d'Eisenstein)**.** *Soit $P = \sum_{i=0}^{d} a_i X^i$ un polynôme à coefficients dans $\mathbb{Z}$. S'il existe un nombre premier p tel que p divise tous les coefficients sauf le dernier et que p^2 ne divise pas le premier coefficient, alors P est irréductible dans $\mathbb{Q}[X]$.*

Proof. On applique le théorème d'Eisenstein avec $\mathcal{A} = \mathbb{Z}$ et $I = (p)$. Ainsi, P est irréductible dans $\mathbb{Z}[X]$ donc dans $\mathbb{Q}[X]$ par la proposition précédente. □

Le critère d'Eisenstein est un critère d'irréductibilité puissant, en particulier lorsque l'on considère les fermés de Zariski. L'idée est de considérer $\mathcal{A}[x, y]$ comme $\mathcal{A}[x][y]$ et d'appliquer le critère d'Eisenstein sur $\mathcal{A}[x]$.

Exemple 1. *Soit $f = y^2 + yx^2 + x$. On peut considérer $I = (x)$. $f_0 = x \in I$ et $f_0 = x \notin I^2$, $f_1 = x^2 \in I$ et $f_2 = 1 \notin I$. On en déduit que f est irréductible dans $\mathbb{C}[x][y]$.*

De manière générale, on a le corollaire suivant :

Corollaire 2. *Soit $f \in \mathcal{A}[x, y]$ sous la forme $f = \sum_{i=0}^{d} f_i(x) y^i$. Si les f_i sont premiers entre eux et qu'il existe un polynôme irréductible $p(x)$ tel que $p(x)$ divise tous les f_i sauf le dernier et que $p^2(x)$ ne divise pas f_0, alors f est irréductible dans $\mathcal{A}[x, y]$.*

Le critère d'Eisenstein s'applique plus souvent sur des polynômes à coefficients entiers. On peut par exemple établir l'irréductibilité du p-ième polynôme cyclotomique.

$$\Phi_p(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \ldots + 1. \tag{80}$$

Corollaire 3. *Le p-ième polynôme cyclotomique est irréductible dans $\mathbb{Q}[X]$.*

Proof. On calcule d'abord $\Phi_p(X + 1)$

$$\Phi_p(X + 1) = \frac{(X + 1)^P - 1}{X} = \sum_{i=1}^{p} \binom{p}{i} X^{i-1}. \tag{81}$$

D'après le critère d'Eisenstein avec p, $\Phi_p(X+1)$ est irréductible dans $\mathbb{Q}[X]$. (p divise $\binom{p}{i}$ pour $i \in \{1, ..., p-1\}$, p^2 ne divise pas $\binom{p}{1}$ et p ne divise pas $\binom{p}{p}$). Si Φ_p était réductible, alors il existerait $R, Q \in \mathbb{Q}[X]$ tels que $\Phi_p = RQ$. On aurait alors

$$\Phi_p(X+1) = R(X+1)Q(X+1) = R'(X)Q'(X). \tag{82}$$

Ce qui contredirait l'irréductibilité de $\Phi_p(X+1)$. □

On conclut par un dernier corollaire intéressant.

Corollaire 4. $\mathbb{Q}[X]$ *admet des polynômes irréductibles de degré arbitrairement grand.*

Proof. On pose $P_n = X^n - 2$. On a directement par le critère d'Eisenstein que P_n est irréductible dans $\mathbb{Q}[X]$. □

9 Un anneau principal non euclidien

Abstract

Un résultat assez connu est qu'un anneau principal est euclidien. Naturellement, on peut se demander si la réciproque est vraie, i.e. si un anneau euclidien est forcément principal. On montre que l'anneau $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ est un anneau principal non euclidien.

On note $a = \frac{1+i\sqrt{19}}{2}$.

$$\mathbb{Z}[a] = \{x + ay, x, y \in \mathbb{Z}\} \tag{83}$$

On introduit la norme de $z = x + ay$:

$$N(z) = z\bar{z} = \left(x + \frac{y}{2}\right)^2 + \frac{19}{4}y^2 \tag{84}$$

Lemme 9. *Les inversibles de $\mathbb{Z}[a]$ sont ± 1.*

Proof. Soit $z = x + ay$ un élément inversible de $\mathbb{Z}[a]$. On a $N(zz^{-1}) = N(z)N(z^{-1}) = 1$ donc $N(z) = 1$. Or, $\frac{19}{4} > 1$ donc

$$\left(x + \frac{y}{2}\right)^2 + \frac{19}{4}y^2 > \left(x + \frac{y}{2}\right)^2 + y^2 \tag{85}$$

Si $y \neq 0$, alors $N(z) > 1$, donc $y = 0$. On en déduit

$$N(z) = x^2 = 1 \tag{86}$$

donc $x = \pm 1$, i.e. $z = \pm 1$. Et réciproquement, ± 1 sont inversibles dans $\mathbb{Z}[a]$. □

Nous allons premièrement montrer que $\mathbb{Z}[a]$ est un anneau non-euclidien. Pour cela, on montre le lemme suivant

Lemme 10. *Si $\mathcal{A}$ est un anneau euclidien, il existe $x \in \mathcal{A} \setminus \mathcal{A}^\times$ tel que la restriction de la projection de $\mathcal{A}$ sur $\mathcal{A}/(x)$ à $\mathcal{A}^\times \cup \{0\}$ soit surjective.*

Proof. Si $\mathcal{A}$ est un corps, $x = 0$ va convenir. Sinon, on note f le stathme associé à $\mathcal{A}$. On peut choisir x tel que $f(x)$ soit minimal. Si on réalise la division euclidienne d'un élément $a \in \mathcal{A}$ par x, on obtient

$$a = qx + r \tag{87}$$

Si on note π la projection de $\mathcal{A}$ sur $\mathcal{A}/(x)$, on a $\pi(a) = \pi(r)$. Puisque $f(r) < f(x)$, on a alors $r = 0$ ou $r \in \mathcal{A}^\times$, autrement on contredirait la définition de x. On conclut alors que pour tout $a \in \mathcal{A}$, il existe $r \in \mathcal{A}^\times \cup \{0\}$ tel que $\pi(a) = \pi(r)$.

De plus, on montre que (x) est un idéal maximal, si on considère un élément non nul de $\mathcal{A}/(x)$, on sait qu'il existe r inversible tel que $\pi(r) = \pi(a)$. On a alors que $\pi(r)\pi(r^{-1}) = \pi(a)\pi(r^{-1}) = \pi(1)$. On en déduit que $\pi(a)$ est inversible et donc que $\mathcal{A}/(x)$ est un corps. □

Proposition 10. *$\mathbb{Z}[a]$ n'est pas un anneau euclidien.*

Proof. Nous savons que les inversibles de $\mathbb{Z}[a]$ sont $-1, 1$. Supposons que $\mathbb{Z}[a]$ soit euclidien, il existe $z \in \mathbb{Z}[a] \setminus \mathbb{Z}[a]^\times$ vérifiant les propriétés du lemme précédent. On sait que π_z restreinte à $\mathbb{Z}[a]^\times \cup \{0\}$ est surjective. Autrement dit, $\pi_z(\{-1, 0, 1\}) = \mathbb{Z}[a]/(z)$. On a montré que (z) est un idéal maximal donc $\mathbb{Z}[a]/(z)$ est un corps de cardinal 2 ou 3. Or $\pi(\alpha)$ est racine du polynôme $X^2 - X + 5$, qui est irréductible sur $\mathbb{F}_2$ et $\mathbb{F}_3$. On a donc une contradiction. □

On peut ensuite montrer l'existence d'une pseudo-division euclidienne dans $\mathbb{Z}[a]$.

Proposition 11. *Pour tout $z \in \mathbb{Z}[a]$ et $w \in \mathbb{Z}[a] \setminus \{0\}$, il existe $q, r \in \mathbb{Z}[a]$ tels que*

$$z = qw + r \quad ou \quad 2z = qw + r \tag{88}$$

avec $N(r) < N(w)$.

Proof. On note $c = \frac{z}{w}$, on obtient alors

$$c = \frac{x_z + ay_z}{x_w + ay_w} \tag{89}$$

$$= \frac{x_z + ay_z}{x_w + ay_w} \frac{x_w - ay_w}{x_w - ay_w} \tag{90}$$

$$= \frac{x_z x_w + 19 y_z y_w}{x_w^2 + 19 y_w^2} + a \frac{x_w y_z - x_z y_w}{x_w^2 + 19 y_w^2} \tag{91}$$

On peut donc écrire $c = t + av$ avec $t, v \in \mathbb{Q}$. On pose ensuite $q = \lfloor t \rceil + a\lfloor v \rceil$ et $r = z - qw$. Supposons que □

Proposition 12. *$\mathbb{Z}[a]$ est un anneau principal.*

Proof. Remarquons premièrement que (2) est un idéal maximal.

$$\mathbb{Z}[a]/(2) \cong \mathbb{Z}[X]/(X^2 - X + 5)/2 \cong \mathbb{Z}[X]/(X^2 + X + 1). \tag{92}$$

On sait que $X^2 + X + 1$ est irréductible sur $\mathbb{Z}$. On déduit que $\mathbb{Z}[a]/(2)$ est un corps.

Soit I un idéal de $\mathbb{Z}[a]$. On considère $z \in I \setminus \{0\}$ tel que $N(z)$ soit minimal. Si $I = (z)$, alors I est principal. Sinon, on peut considère un élément $w \in I \setminus (z)$ et on applique le lemme de pseudo-division euclidienne. On obtient alors $q, r \in \mathbb{Z}[a]$ tels que $w = qz + r$ ou $2w = qz + r$ avec $N(r) < N(z)$. Supposons que $w = qz + r$. Alors $r = w - qz$ est dans I. On a forcément $r = 0$ sinon on contredirait la minimalité de $N(z)$. On en déduit que $w = qz$, ce qui est absurde. On en déduit que $2w = qz + r$. On a de la même manière nécessairement $r = 0$ donc $2w = qz$. (2) est premier et, a fortiori, est premier.

Ainsi, 2 divise q ou z. Si jamais $q = 2q'$, on a $w = 2q'z$ et on déduit que $w \in (z)$, ce qui est une contradiction. On en déduit que $z = 2z'$ et donc que $I = (z)$. □