Exercice 1.. **Sous-monoïdes de $\mathbb{N}$. Constante de Frobénius**

Soient a et b deux entiers naturels > 1. On note $G_{a,b}$ le sous-groupe de $(\mathbb{Z}, +)$ engendré par a et b. On note d le `p.g.c.d.` de a et b.

1. Justifier que $G_{a,b} = \{xa + yb \ ; \ x, y \in \mathbb{Z}\}$.

   C'est du cours. Tout sous-groupe contenant a et b contient les éléments $xa + yb$ pour x et y dans $\mathbb{Z}$. De plus, on vérifie que $\{xa + yb \ ; \ x, y \in \mathbb{Z}\}$ est un sous groupe de $\mathbb{Z}$ ($0 = 0a + 0b \in G_{a,b}$ et $(xa+yb) - (x'a+y'b) = (x-x')a + (y-y')b \in G_{a,b}$) donc c'est le sous-groupe engendré par a et b.

2. On suppose que $b > a$. Justifier que $G_{a,b} = G_{a,b-a}$.
   Les élements a et $b - a$ sont dans $G_{a,b}$ donc $G_{a,b-a} \subset G_{a,b}$. Réciproquement, $b = b - a + a$ donc $G_{a,b} \subset G_{a,b-a}$.

3. En déduire que $G_{a,b} = d\mathbb{Z}$ et qu'il existe deux entiers relatifs u et v tels que $ua + bv = d$.

   Par application successive de l'égalité, $G_{a,b} = G_{a,b-a}$, on obtient $G_{a,b} = G_{a,r}$ où r est le reste de la division euclidienne de b par a. L'algorithme d'Euclide assure alors que $G_{a,b} = G_{d,0}$ avec $d =$ `p.g.c.d.`(a, b) et par définition, $G_{d,0} = d\mathbb{Z}$.

   Par le théorème de Bezout ($\mathbb{Z}$ est un anneau principal, il existe deux entiers relatifs u et v tels que $ua + bv = d$.

4. On pose $a = da'$ et $b = db'$. Soient u et v deux entiers relatifs tels que $ua + bv = d$. Soient x et y dans $\mathbb{Z}$. Démontrer que :

$$xa + yb = d \Leftrightarrow \exists k \in \mathbb{Z} \ / \ \begin{cases} x = u - kb' \\ y = v + ka' \end{cases}$$

   Soient x et y dans $\mathbb{Z}$.

$$\begin{aligned} xa + yb = d &\Leftrightarrow xa + yb = ua + vb \\ &\Leftrightarrow a(x-u) = b(v-y) \\ &\Leftrightarrow a'(x-u) = b'(v-y) \end{aligned}$$

   Or `p.g.c.d.`$(a', b') = 1$, donc on peut utiliser le lemme de Gauss :

$$\begin{aligned} a'(x-u) = b'(v-y) &\Leftrightarrow \exists k \in \mathbb{Z} \ / \ \begin{cases} v - y = ka' \\ a'(x-u) = ka'b' \end{cases} \\ &\Leftrightarrow \exists k \in \mathbb{Z} \ / \ \begin{cases} x = u - kb' \\ y = v + ka' \end{cases} \end{aligned}$$

5. Soit $M_{a,b}$ le sous-monoïde de $(\mathbb{N}, +)$ engendré par a et b.

   (a) Justifier que $M_{a,b} = \{xa + yb \ ; \ x, y \in \mathbb{N}\}$.

   C'est du cours. On vérifie que $\{xa + yv \ ; \ x, y \in \mathbb{N}\}$ est un sous-monoïde de $(\mathbb{N}, +)$, il contient a et b. De plus tout sous-monoïde de $(\mathbb{N}, +)$ contenant a et b contient les sommes de la forme $xa + yv$, $x, y \in \mathbb{N}$.

(b) On suppose que a et b sont premiers entre eux. Démontrer qu'il existe un entier N tel que $\forall n \in \mathbb{N}, n > N \Rightarrow n \in M$.

Soit $n \in \mathbb{N}$. Il existe x, y dans $\mathbb{Z}$ tels que $n = xa + yb$ et alors pour tout entier k, $n = (x + kb)a + (y - ka)b$. On peut choisir k tel que $x + kb \in \{0, ..., b - 1\}$ alors $n - (b - 1)a \leq n - (x + kb)a = (y - ka)b$. Si $n > ab - b - a$, $-b < n - (b - 1)a \leq (y - ka)b$, donc $(y - ka)b$ est un entier relatif multiple de b et $> -b$, donc ≥ 0, et ainsi $(y - ka) \in \mathbb{N}$.

(c) Soit $F_{a,b}$ défini par :
$\forall n \in \mathbb{N}, n > F_{a,b} \Rightarrow n \in M_{a,b}$ et $F_{a,b} \notin M_{a,b}$. Exprimer $F_{a,b}$ en fonction de a et de b.

On vient de montrer que $\forall n \in \mathbb{N}, n > ab - (a + b) \Rightarrow n \in M$. Supposons que $ab - (a + b) \in M$. Alors, il existe x et y dans $\mathbb{N}$ tels que $ab - (a + b) = xa + yb$. Modulo b, $xa \equiv -a$ donc (puisque $\text{pgcd}(a, b) = 1$), $x \equiv -1$, et comme $x \in \mathbb{N}$, $x \geq b - 1$. Par symétrie $y \geq (a - 1)$ et $xa + yb \geq (a - 1)b + (b - 1)a = 2ab - (a + b) > ab - (a + b)$. Contradiction.
Donc $F_{a,b} = ab - a - b$

Soient a et b deux entiers naturels non nuls dont on note d le `p.g.c.d.`. Soit $M_{a,b}$ le sous-monoïde de $(\mathbb{N}, +)$ engendré par a et b.

5. Démontrer l'inclusion $M_{a,b} \subset d\mathbb{N}$.

$a \in d\mathbb{N}$ et $b \in d\mathbb{N}$, donc par définition du sous-monoïde engendré, $M =< a, b > \subset d\mathbb{N}$.

6. Démontrer qu'il existe un entier N tel que $\forall n \in \mathbb{N}, n > N \Rightarrow nd \in M_{a,b}$.
$M = d\tilde{M}$ où $\tilde{M}$ est le sous-monoïde engendré par a/d et b/d. En appliquant ce qui prècède à $\tilde{M}$, $N = F_{a/d,b/d}$ convient.

7. Exprimer en fonction de a, b et d l'entier $F_{a,b}$ défini par :
$\forall n \in \mathbb{N}, n > F_{a,b} \Rightarrow nd \in M_{a,b}$ et $dF_{a,b} \notin M_{a,b}$.

$F_{a,b} = F_{a/d,b/d} = ab/d^2 - a/d - b/d$.

Soit M un sous-monoïde de $(\mathbb{N}, +)$ tel que le seul entier naturel diviseur dans $\mathbb{N}$ de tous les éléments de M, est 1.

8. Démontrer qu'il existe un nombre fini d'éléments de M, soient $a_1, ..., a_n$ dont le `p.g.c.d.` est 1.

Soit $a \in M$ tel que $a \neq 0$. Si $a = 1$, $M = \mathbb{N} =< 1 >$. Sinon, soit p un diviseur premier de a. par hypothèse, il existe $b_p \in M$ non divisible par p. Alors $\{a, b_p \mid p \text{ diviseur premier de } a\}$ convient.

9. Démontrer que M est à engendrement fini.

Soit $L =< a, b_p, p$ diviseur premier de $a >$; c'est un sous-monoïde de M auquel on peut appliquer les résultats de 7) avec $d = 1$. Donc il existe N tel que pour tout $n > N$, $n \in L$. Ainsi, $M \setminus L$ est fini. Donc Donc $M =< M \setminus L, a, b_p \mid p \text{ diviseur premier de } a >$ est à engendrement fini.

10. Démontrer qu'il existe un entier naturel N $\forall n \in \mathbb{N}, n > N \Rightarrow n \in M$.
On peut raisonner par récurrence sur le cardinal r d'une partie génératrice du monoïde M. Soit $\{a_1, a_2, ..., a_r\}$ une partie génératrice de cardinal n de M. Soit d le p.g.c.d de $a_2, ..., a_r$. Alors a_1 et d sont premiers entre eux, donc pour $\forall n > F_{a_1,d}$, il existe u et v entiers naturels tels que $n = ua_1 + vd$. En utilisant la question 3, on peut supposer $0 \leq u < d$ et on a alors $vd > n - da_1$.

Par hypothèse de récurrence, il existe un entier N tel que $\forall v \in \mathbb{N}, v > N \Rightarrow v \in < \frac{a_2}{d}, ..., \frac{a_r}{d} >$. On en déduit que $\forall v \in \mathbb{N}, v > N \Rightarrow vd \in < a_2, ..., a_r >$.

Donc pour $n > \max(F_{a_1,d}, N + da_1)$, il existe u et v entiers naturels tels que $n = ua_1 + vd$, avec $vd \in < a_2, ..., a_r >$, i.e $n \in < a_1, a_2, ..., a_r >$.

On note F_M le plus petit entier tel que $\forall n \in \mathbb{N}, n > F_M \Rightarrow n \in M$.

11. On suppose que $X = \{a_1, a_2, ..., a_n\}$ est une partie génératrice minimale de cardinal n de M, numérotée de façon à avoir : $a_1 < a_2 < \cdots < a_n$. Pour $j \in \mathbb{N}$, on note L_j une liste de longueur a_n, numérotée à partir de 1, telle que :

$$L_j[i] := \begin{cases} 1, & \text{si } ja_n + i \in M, \\ 0, & \text{sinon.} \end{cases}$$

(a) Expliciter un algorithme qui permet de remplir la liste L_0.

On parcourt les indices entre 1 et a_n. On affecte des 0 aux indices de 1 à $(a_1 - 1)$, puis un 1 sur l'indice a_1. Puis on parcourt la liste en mettant un 1 en i, s'il y a déjà un 1 sur un $i - a_j$, pour un $a_j < i$ ou 0 sinon.

(b) Soit $j \in \mathbb{N}$. Ecrire un algorithme qui permet de créér L_{j+1} à partir de L_j.

On parcourt les indices entre 1 et a_n. Pour chaque indice, on regarde dans la liste L_j ou dans les termes précédents de la liste L_{j+1} s'il existe un k dans $\{1, 2, ..., n\}$ ayant attribué à $i - a_k$ la valeur 1. Dans ce cas, on met 1. Sinon on met 0.

(c) En déduire que tant que L_j contient au moins un 0, L_j est distinct de L_{j+1}.
On remarque que s'il y a un 1 à la place i dans L_j, il y en a aussi un à la place i dans L_{j+1} (on ajoute a_n). Donc le nombre de 1 croit avec j. De plus, le procédé de construction assure que si $L_j = L_{j+1}$, alors $L_{j+1} = L_{j+2}$. Or à partir d'un certain j, on sait que L_j ne contient que des 1. La suite des listes ne peut donc pas stationner avant.

(d) Quelle majoration obtient-on ainsi pour F_M ?

Puisqu'on ajoute au moins un 1 à chaque fois, la liste $L_{a_n - 1}$ ne contient que des 1.

(e) Expliciter un algorithme qui permet de calculer F_M. Estimer sa complexité au pire.

Au plus on remplit les a_n premières listes. Chacun des a_n indices d'une liste se voit attribuer un 1 ou un 0 selon n tests (un pour chaque a_i). la complexité au pire est ainsi majorée par $O(n(a_n)^2$.

(f) Un patissier vend de délicieux macarons dans des boîtes pré-emballées. Il y a trois formats de boîtes ; la petite boîte en contient 6, la boîte moyenne en contient 9 et le grande boîte en contient 20. Quelles sont les quantités possibles de macarons qui peuvent lui être achetées?
On ne peut pas acheter $1, 2, 3, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 22, 23, 25, 28, 31, 34$ ou 43 macarons. Toutes les autres quantités sont possibles.

Exercice 2.

Soit $\mathcal{C} = (n, \mathbb{P}, \mu_0)$ une chaîne de Markov, où l'espace d'états est $[\![1, n]\!]$, $\mathbb{P}$ est la matrice de transitions et $\mu_0 : [\![1, n]\!] \to [0, 1]$ la distribution initiale. On suppose la chaîne irréductible.

Pour tout entier i dans $[\![1, n]\!]$, on note d_i le `p.g.c.d.` des longueurs des cycles passant par i. On note d le `p.g.c.d.` des d_i pour tous les i dans $[\![1, n]\!]$.

1. Soit $i \in [\![1, n]\!]$. Démontrer que l'ensemble des longueurs des cycles passant par i est un sous-monoïde de $\mathbb{N}$.

   En concaténant deux cycles respectivement de longueur l_1,l_2 passant par i, on obtient un cycle passant par i de longueur $l_1 + l_2$. Le chemin vide est un cycle passant par i de longueur 0.

2. Démontrer que $d_i = d_j$, pour tous i, j dans $[\![1, n]\!]$.

   Soient $ch : i \to \cdots \to j$ un chemin de i vers j dont on note l la longueur, $ch' : j \to \cdots \to i$ un chemin de j vers i dont on note l' la longueur. Si cy est un cycle de longueur m passant par j, la concaténation $ch.cy.ch'$ est cycle de longueur $l + m + l'$ passant par i, donc d_i divise $l + m + l'$. Comme d_i divise $l + l'$ (puisque la concaténation $ch.ch'$ est un cycle de longueur $l + l'$ passant par i), d_i divise m. Ceci pour tout cycle passant par j, donc d_i divise d_j. Par symétrie $d_i = d_j$.

3. On suppose $d = 1$ ($\mathcal{C}$ est apériodique). Justifier qu'il existe N tel que : Pour tous $i, j \in [\![1, n]\!]$, pour tout $m \geq N$, il existe un chemin de longueur m de i vers j.

   La chaîne est apériodique, donc $d = 1$. Comme les d_i sont égaux pour tout i, $d_i = d = 1$. On applique la question 10 au monoïde défini par l'ensemble des longueurs des cycles passant par i.

4. Démontrer que la chaîne de Markov $\mathcal{C}$ est irréductible et apériodique si et seulement s'il existe N tel que pour $m \geq N$, tous les coefficients de $\mathbb{P}^m$ sont strictement positifs.

   Rappelons que le (i, j)-ème terme de la matrice $\mathbb{P}^m$ est la probabilité des chemins de longueur m de i vers j (pour tous sommets i, j).

   S'il existe N tel que pour $m \geq N$, tous les coefficients de $\mathbb{P}^m$ sont strictement positifs, alors :

   - Pour tous sommets i, j, il existe un chemin de longueur N de i vers j. Donc $\mathcal{C}$ est irréductible.
   - Pour tout sommet i, pour $m \geq N$, il existe un cycle de longueur m. Or $\texttt{p.g.c.d.}(N, N+1) = 1$, donc $d_i = 1$. Donc $d = \texttt{p.g.c.d.}(d_i, i) = 1$, i.e. $\mathcal{C}$ est apériodique.

   Réciproquement, supposons $\mathcal{C}$ irréductible et apériodique. Comme elle est irréductible, Pour tous sommets i, j, il existe un chemin de i vers j. On note la longueur $N_{i,j}$ d'un tel chemin. Comme elle est apériodique, pour tout sommet i, d_i =1 et il existe N_i (question 10) tel que pour $m \geq N_i$, il existe un cycle de longueur m passant par i.

   Posons $N = \max\{N_{i,j} + N_j \mid (i, j) \in [\![1, n]\!]^2\}$. Alors si $m \geq N$, Pour tous sommets i, j, il existe un chemin de i vers j de longueur $N_{i,j}$ et un cycle passant par j de longueur $m - N_{i,j}$ ($m - N_{i,j} \geq N_j$). En les concaténant, on obtient un chemin de i vers j de longueur m.

5. On ne suppose plus que $d = 1$. Démontrer qu'on peut établir une relation d'équivalence sur $[\![1, n]\!]$ ayant d classes d'équivalence $C_0, ..., C_{d-1}$ (l'indexation des classes est dans $\mathbb{Z}/d\mathbb{Z}$) telle que toute transition partant d'un état dans une classe C_i arrive dans la classe C_{i+1}.

Comme d divise toutes les longueurs de cycles, pour tous sommets i, j, Soient $ch : i \to \cdots \to j$ un chemin de i vers j dont on note l la longueur, $ch' : j \to \cdots \to i$ un chemin de j vers i dont on note l' la longueur. La concaténation $ch.ch'$ est cycle de longueur $l + l'$ passant par i, donc $d = d_i$ divise $l + l'$. Si on deux chemins de i vers j dont on note l_1, l_2 les longueurs respectives, d divise $l_1 + l'$ et $l_2 + l'$, donc $l_1 \equiv l_2[d]$.

La relation d'équivalence est :

$$i \sim j \Leftrightarrow \text{la longueur des chemins de } i \text{ vers } j \text{ est un multiple de } d$$

On choisit un sommet i_0. Pour $r \in [\![0, d-1]\!]$, on pose C_r est l'ensemble des sommets i tels que les longueurs des chemins de i_0 vers vers i sont congrues à r modulo d.

Quelle forme a la matrice $\mathbb{P}^d$?

$$\mathbb{P}^d = \begin{pmatrix} Q^d & 0 & 0 & \cdots & 0 \\ 0 & \ddots & 0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & Q^d & 0 \\ 0 & 0 & \cdots & 0 & Q^q \end{pmatrix} \text{ et } \mathbb{P} = \begin{pmatrix} 0 & Q & 0 & \cdots & 0 \\ 0 & 0 & Q & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & Q \\ Q & 0 & \cdots & \cdots & 0 \end{pmatrix}$$

où $Q = (p_{i,j})_{i \in C_0, j \in C_1}$.

Quel est le comportement asymptotique de la chaîne de Markov ?

Elle a un comportement périodique de période d.

Exercice 3. On munit $\mathbb{R}^n$ de la norme euclidienne notée $\| \ \|$ définie par le produit scalaire $< \ >$. Si $(e_1, ..., e_n)$ est une base orthonormée de $\mathbb{R}^n$, on a :

$$< \sum_{i=1}^n x_i e_i, \sum_{i=1}^n y_i e_i >= \sum_{i=1}^n x_i y_i \text{ et } \left\| \sum_{i=1}^n x_i e_i \right\|^2 =< \sum_{i=1}^n x_i e_i, \sum_{i=1}^n x_i e_i >= \sum_{i=1}^n x_i^2.$$

Cette définition est indépendante du choix de la base orthonormée (par définition de ce qu'est une base orthonormée!). On remarquera que la base canonique de $\mathbb{R}^n$ est une base orthonormée. Pour $P \in M_n(R)$, on rappelle l'équivalence des propriétés :

Ia) P est une matrice d'*isométrie*, i.e. $\forall v \in \mathbb{R}^n, \|Pv\| = \|v\|$,

Ib) P envoie une base orthonormée sur une base orthonormée,

Ic) ${}^tPP = Id$.

On définit sur l'algèbre des matrices $M_n(\mathbb{R})$ la norme matricielle associée à la norme euclidienne :

$$\forall M \in M_n(\mathbb{R}), |||M||| = \sup_{x \neq 0} \frac{\|Mx\|}{\|x\|}.$$

Une telle norme vérifie :

$$\forall M_1, M_2 \in M_n(\mathbb{R}), |||M_1 M_2||| \leq |||M_1||| |||M_2|||.$$

On rappelle que les matrices symétriques réelles sont diagonalisables sur une base orthonormée.

1. Soit M une matrice symétrique réelle de rayon spectral $\rho(M)$ (on rappelle que le rayon spectral de M est défini comme $|\lambda|$, λ étant la plus grande valeur propre en module de M.) Démontrer en utilisant une base orthonormée de vecteurs propres de M que la norme de M est le rayon spectral de M.

   Soient $(e_1, ..., e_n)$ une base orthonormée de vecteurs propres de M associés respectivement aux valeurs propres $\lambda_1, ..., \lambda_n$ numérotées telles que $\rho(M) = |\lambda_1| > |\lambda_2| \geq \cdots \geq |\lambda_n|$. Alors, pour tout $(x_1, x_2, \cdots, x_n)$ dans $\mathbb{R}^n$, $M(\sum_i x_i e_i) = \sum_i \lambda_i x_i e_i$ donc $\|M(\sum_i x_i e_i)\|^2 = (\sum_i \lambda_i^2 x_i^2 \leq \lambda_1^2 \|\sum_i x_i e_i\|^2$. On obtient ainsi $|||M||| \leq \rho(M)$. Or $\|M(e_1)\|^2 = \lambda_1^2 = \rho(M)^2$, $|||M||| = \rho(M)$.

2. Soit M une matrice stochastique, irréductible, apériodique et **symétrique**. On a vu en cours que le rayon spectral de M est 1, que la seule valeur propre de M de module 1 est simple et vaut 1. On note $1 = \lambda_1, ..., \lambda_n$ ses n valeurs propres réelles (comptées avec leurs multiplicités) numérotées telles que $1 = |\lambda_1| > |\lambda_2| \geq \cdots \geq |\lambda_n|$ et $\mathbf{1}$ le vecteur dont toutes les coordonnées sur la base canonique sont des 1.
   On note H l'hyperplan formé par les vecteurs dont la somme des coordonnées sur la base canonique vaut 0.

   (a) Démontrer que H est l'orthogonal du vecteur $\mathbf{1}$, c'est-à-dire l'ensemble $\{v \in \mathbb{R}^n \ ; \ < v, \mathbf{1} >= 0\}$.
   Si v est le vecteur de coordonnées $v_1, ..., v_n$ sur la base canonique, $< v, \mathbf{1} >= \sum v_i$; donc $\mathbf{1}^\perp = \{v \in \mathbb{R}^n \ ; \ < v, \mathbf{1} >= 0\} = H$.

   (b) En déduire l'existence d'une matrice d'isométrie P et d'une matrice symétrique Q dans $M_{n-1}(\mathbb{R})$ telle que :

$$M = {}^tP \begin{pmatrix} 1 & 0 \\ 0 & Q \end{pmatrix} P$$

   avec de plus $\rho(Q) = |\lambda_2|$.

   Soient $(e_1, ..., e_n)$ une base orthonormée de vecteurs propres de M associés respectivement aux valeurs propres $\lambda_1, ..., \lambda_n$ numérotées telles que $\rho(M) = |\lambda_1| > |\lambda_2| \geq \cdots \geq |\lambda_n|$. Alors e_1 est colinéaire à $\mathbf{1}$ et $(e_2, ..., e_n)$ est une base orthonormée de H. Soit P la matrice de passage de la base canonique à la base $(e_1, ..., e_n)$. La matrice P envoie une base orthonormée sur une base orthonormée donc est une matrice d'isométrie. Et on a :

$$M = {}^tP \begin{pmatrix} 1 & 0 \\ 0 & Q \end{pmatrix} P$$

   où Q est la matrice diagonale $\begin{pmatrix} \lambda_2 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \lambda_n \end{pmatrix}$. En particulier, Q est symétrique telle que $\rho(Q) = |\Lambda_2|$.

   (c) Retrouver ainsi que la suite $\{M^k\}_{k \in \mathbb{N}}$ converge vers une matrice L de rang 1 telle que :

$$|||M^k - L||| \leq |\lambda_2|^k.$$

.

$$\forall k \in \mathbb{N}, M^k = {}^tP \begin{pmatrix} 1 & 0 \\ 0 & Q^k \end{pmatrix} P$$

$$\text{Et, } Q^k = \begin{pmatrix} \lambda_2^k & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \lambda_n^k \end{pmatrix}.$$

Comme $1 > |\lambda_2| \geq \cdots \geq |\lambda_n|$, $\lim_{k\to\infty} Q^k = 0$ donc $\lim_{k\to\infty} M^k = {}^tP \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} P$.

Soit $L = {}^tP \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} P$, c'est bien une matrice de rang 1 (elle est semblable à une matrice de rang 1). De plus,

$$\forall k \in \mathbb{N}, M^k - L = {}^tP \begin{pmatrix} 1 & 0 \\ 0 & Q^k \end{pmatrix} P - {}^tP \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} P = {}^tP \begin{pmatrix} 0 & 0 \\ 0 & Q^k \end{pmatrix} P.$$

$\forall k \in \mathbb{N}, M^k - L$ est une matrice symétrique. Donc $\left\|\left|M^k - L\right|\right\| = \rho(M^k - L) = |\lambda_2|^k$.

(d) Justifier que L est stochastique et symétrique.

Le produit de deux matrices symétriques qui commutent est une matrice symétrique (Si M_1, M_2 sont symétriques et commutent, $({}^t(M_1M_2) = {}^t(M_2M_1) = {}^tM_1{}^tM_2 = M_1M_2)$ et lLe produit de deux matrices stochastiques est une matrice stochastique (vu en cours), donc
la matrice L est la limite d'une suite de matrices symétriques stochastiques. On vérifie qu'alors L est une matrice symétrique stochastique.
Quelle est alors la matrice L ?

La seule matrice symétrique et stochastique de rang 1 est la matrice $\begin{pmatrix} \frac{1}{n} & \cdots & \frac{1}{n} \\ \vdots & \ddots & \vdots \\ \frac{1}{n} & \cdots & \frac{1}{n} \end{pmatrix}$.

Exercice 4. Soit G un graphe fini non orienté. On note S son ensemble d'états, de cardinal n et A son ensemble d'arêtes de cardinal m. Pour chaque sommet $s \in S$. on note d_s le degré de s, c'est-à-dire le nombre d'arêtes (s,t) dans A. On suppose le graphe connexe.

Soit s_0 un sommet fixé dans G. On considère $\mathcal{C} = \{X_n\}_{n\in\mathbb{N}}$ la chaîne de Markov définie par :

- X_0 est une variable aléatoire prenant ses valeurs dans S. Si besoin, on pourra noter ν le vecteur tel que $\nu(s) = P(X_0 = s)$, pour tout s dans S. C'est la distribution initiale de la chaîne $\mathcal{C}$.
- Si $n \geqslant 1$, $P(X_n = t | X_{n-1} = s) = \frac{1}{d_s}$, pour tous s, t dans S tels que $(s,t) \in A$.

Soit λ définie sur S par $\lambda(s) = \frac{d_s}{2m}, \forall s \in S$.

3. Justifier que λ est une loi de probabilité sur S.
λ est bien à valeurs positives.

$$\sum_s \lambda(s) = \sum_s \frac{d_s}{2m} = \frac{1}{2m} \sum_s \sum_{\{t,(s,t)\in A\}} 1 = \frac{1}{2m} \sum_A 2 = 1$$

chaque arête fournit 2 : un 1 pour chacune de ses extrémités.

4. Justifier que $\mathcal{C}$ est une chaîne de Markov irréductible de période 1 ou 2.
$\mathcal{C}$ est une chaîne de Markov irréductible parce que le graphe est supposé connexe. La période est au plus 2 puisque chaque arête (s,t) définit un circuit de longueur 2 $s \to t \to s$.

5. Démontrer que la période est 2 si et seulement si le graphe G est biparti.

Supposons que la période est 2. Alors tous les chemins entre deux états, disons de s à t, sont soit tous de longueur paire, soient tous de longueurs impaires. On fixe alors s_o dans S. Soit I

(respectivement J l'ensemble des états t tels que les chemins de s_0 à t sont tous de longueur paire (respectivement tous de longueurs impaires). alors $(s,t) \in A$ et $s \in I$ impose $t \in J$ et $s \in J$ impose $t \in I$; le graphe est biparti.

Réciproquement, si le graphe est biparti, il existe une partition de S, $S = I \sqcup J$ telle que $(s,t) \in A$ et $s \in I$ impose $t \in J$ et $s \in J$ impose $t \in I$. Tout circuit est donc de longueur paire, ce qui impose que la période n'est pas 1, donc est 2.

6. Décrire la matrice de transition $\mathbb{P}$ de la chaîne de Markov $\mathcal{C}$.

Sur chaque ligne, il y a des zéros ou un nombre fixé, qui de plus n'est pas sur la diagonale. De plus le "motif" de la matrice est symétrique (si $a_{i,j} \neq 0$, $a_{j,i} \neq 0$).

7. Justifier que λ est une loi stationnaire pour $\mathcal{C}$.

$\sum_{(s,t)\in A} \lambda(s) p_{s,t} = \sum_{(s,t)\in A} \frac{d_s}{2m} \frac{1}{d_s} = \sum_{(s,t)\in A} \frac{1}{2m} = \frac{d_t}{2m} = \lambda(t)$.

8. Soit $\epsilon \in]0,1[$. On considère la chaîne de Markov $\mathcal{D}_\epsilon = \{Y_n\}_{n\in\mathbb{N}}$ définie par :

   - $Y_0 = X_0$.
   - Si $n \geqslant 1$, $P(Y_n = t | Y_{n-1} = s) = (1-\epsilon) P(X_n = t | X_{n-1} = s)$, pour tous s,t dans S tels que $(s,t) \in A$, et $P(Y_n = t | Y_{n-1} = t) = \epsilon$, pour tout t dans S.

   Démontrer que la chaîne de Markov $\mathcal{D}_\epsilon$ converge en loi vers la loi λ.

   La chaîne de Markov $\mathcal{D}_\epsilon$ est obtenue à partir de la chaîne $\mathcal{C}$ en ajoutant sur chaque sommet une boucle de probabilité ϵ et en pondérant les autres probabilités sortantes de $1-\epsilon$ uniformément. Le graphe sous-jacent est le même si ce n'est qu'on a ajouté des boucles sur chaque sommet. Cette chaîne est apériodique puisqu'il y a des circuits de longueur 1 et irréductible (puisque $\mathcal{C}$ l'est), donc elle converge en loi vers son unique distribution stationnaire. Or sa matrice de transition est $\epsilon Id + (1-\epsilon)\mathbb{P}$, donc λ, la distribution stationnaire de $\mathcal{C}$ reste stationnaire pour $\mathcal{D}_\epsilon$ (matriciellement, $\lambda\mathbb{P} = \lambda$ donc $\lambda(\epsilon Id + (1-\epsilon)\mathbb{P}) = \epsilon\lambda Id + (1-\epsilon)\lambda\mathbb{P} = \epsilon\lambda + (1-\epsilon)\lambda = \lambda$). Ainsi, elle converge en loi vers λ.

On suppose désormais le graphe *régulier*, c'est-à-dire que d_s est indépendant de s, $\forall s \in S$. On note d cette valeur commune.

7. Justifier que la matrice de transition $\mathbb{P}$ est symétrique.
   Dans le cas général (cf. question 6), la matrice a un motif symétrique (si $a_{i,j} \neq 0$, $a_{j,i} \neq 0$). Comme tous les coefficients non nuls ont la même valeur, la matrice est bien symétrique.

8. Pour tout $\epsilon \in]0,1[$, démontrer que la chaîne de Markov $\mathcal{D}_\epsilon$ converge en loi vers la loi uniforme sur S avec une convergence au moins géométrique.
   On sait (cf. question8) que la chaîne de Markov $\mathcal{D}_\epsilon$ converge en loi vers la loi λ, qui dans ce cas particulier est la loi uniforme. Comme la matrice est symétrique, on peut aussi déduire la convergence vers la loi uniforme de la question 2d et on obtient de plus la convergence géométrique.

9. Un exemple : Un mélange "idéal " d'un jeu de p cartes consiste en le tirage uniforme d'une permutation de $\mathcal{S}_p$. Une machine mélange un jeu de cartes en effectuant une suite finie d'opérations élementaires aléatoires sur le jeu de cartes. L'opération élémentaire consiste à choisir une carte de façon uniforme dans le jeu et, si ce n'est pas première, à l'échanger avec la première. On décrit ce procédé par une chaîne de Markov dont les états sont les permutations de $\mathcal{S}_p$ et les arêtes correspondent aux opérations élémentaires.

(a) Soit $\sigma \in \mathcal{S}_p$. Démontrer que les transitions issues de σ sont (σ, σ) et $(\sigma, \sigma(1,i))$ pour $i \in \{2, ..., p\}$.

$\sigma(1,i)(j) = \sigma(j)$ si $j \notin \{1, i\}$, $\sigma(1,i)(i) = \sigma(1)$, et $\sigma(1,i)(1) = \sigma(i)$.

(b) En déduire que la chaîne de Markov converge en loi vers la loi uniforme sur $\mathcal{S}_p$.

On applique ce qui précède au graphe G dont les sommets sont etiquetés par les permutations de $\mathcal{S}_p$, et les arêtes sont $(\sigma, \sigma(1,i))$, pour $\sigma \in \mathcal{S}_p$ et $i \in \{2, ..., p\}$. C'est bien un graphe non orienté puisque les transpositions sont d'ordre 2. Le degré en chaque sommet est $p-1$. Le graphe est connexe, parce que la famille de transpositions $(1,2), ..., (1,p)$ est génératrice (une décomposition d'une permutation σ comme produit de telles transpositions va définir un chemin de Id à σ dans le graphe. Le tirage de la première carte (de probabilité $1/p$ correspond à l'ajoût de $1/pId$ à $\frac{p-1}{p}$ la matrice de transition. On applique alors le résultat 8.

(c) Dans quelle mesure la machine fait-elle le travail attendu ? De façon asymptotique, c'est-à-dire si la machine effectue une infinité d'opérations, le mélange est uniforme. Plus pratiquement, un nombre suffisamment grand d'étapes va fournir un mélange suffisant, puisque proche du mélange uniforme. Il faut bien entendu quantifier cela, ce qui sort de l'application du cours, cf. Brémaud par exemple.

Question subsidiaire : Etudier le cas de la machine qui mélange les p cartes en effectuant une suite finie d'opérations élementaires aléatoires sur le jeu de cartes, lorsque l'opération élémentaire consiste à choisir une carte de façon uniforme dans le jeu et à la placer sur le dessus du paquet.

Ce n'est pas très différent, mais la famille génératrice utilisée est formée des cycles $(k, ..., 1)$, $k \in \{2, ..., n\}$.

10. Un autre exemple : m particules se déplacent sur un anneau formé de n cases, avec $n > m$. Une case contient au plus une particule. A chaque étape, une case est choisie de façon uniforme. Si la case est pleine, on passe à l'étape suivante. Sinon, la case se remplit par le déplacement d'une des deux particules les plus proches, le choix de la particule étant uniforme (avec probabilité 1/2).

(a) Décrire ce processus à l'aide d'une chaîne de Markov sur un graphe fini qu'on explicitera.

Le graphe fini a pour ensemble de sommets l'ensemble des configurations possibles (les positions des particules). Pour ne pas faire de dessins (je n'ai pas le temps, mais ce serait plus clair!), je représente l'anneau comme une ligne, les cases vides par des 0 et les cases pleines par des 1. Une arête est alors de la forme :

$$\left|0\right|\underbrace{1}_{\uparrow}\left|0\right|\cdots\left|1\right|0\left| \overset{1/n}{\rightarrow} \right|0\left|\underbrace{1}_{\uparrow}\right|0\left|\cdots\right|1\left|0\right|$$

$$\left|0\right|\underbrace{1}_{\uparrow}\left|1\right|\cdots\left|1\right|0\left| \overset{1/2n}{\leftarrow} \right|1\left|\underbrace{0}_{\uparrow}\right|1\left|\cdots\right|1\left|0\right| \overset{1/2n}{\rightarrow} \left|1\right|\underbrace{1}_{\uparrow}\left|0\right|\cdots\left|1\right|0\right|$$

(b) Ecrire la matrice de transition correspondante lorsque $n = 5$ et $m = 2$. Vous expliquerez comment vous numérotez les états. Vous avez parfaitement le droit de faire un programme ou d'utiliser un logiciel pour expliciter la matrice, néanmoins je veux voir le résultat sous forme d'une matrice (ici, il y a 10 états).

Les états sont :

11000 numéroté en 1, 10100 numéroté en 2, 10010 numéroté en 3, 10001numéroté en 4 , 01100 numéroté en 5, 01010 numéroté en 6, 01001 numéroté en 7, 00110 numéroté en 8 , 00101 numéroté en 9, 00011 numéroté en 10.

La matrice est alors :

$$\begin{pmatrix} 2/5 & 1/10 & 1/10 & 1/10 & 1/10 & 1/10 & 1/10 & 0 & 0 & 0 \\ 1/10 & 2/5 & 1/10 & 1/10 & 1/10 & 0 & 0 & 1/10 & 1/10 & 0 \\ 1/10 & 1/10 & 2/5 & 1/10 & 0 & 1/10 & 0 & 1/10 & 0 & 1/10 \\ 1/10 & 1/10 & 1/10 & 2/5 & 0 & 0 & 1/10 & 0 & 1/10 & 1/10 \\ 1/10 & 1/10 & 0 & 0 & 2/5 & 1/10 & 1/10 & 1/10 & 1/10 & 0 \\ 1/10 & 0 & 1/10 & 0 & 1/10 & 2/5 & 1/10 & 1/10 & 0 & 1/10 \\ 1/10 & 0 & 0 & 0 & 1/10 & 1/10 & 2/5 & 0 & 1/10 & 1/10 \\ 0 & 1/10 & 1/10 & 0 & 1/10 & 1/10 & 0 & 2/5 & 1/10 & 1/10 \\ 0 & 1/10 & 0 & 1/10 & 1/10 & 0 & 1/10 & 1/10 & 2/5 & 1/10 \\ 0 & 0 & 1/10 & 1/10 & 5 & 1/10 & 1/10 & 1/10 & 1/10 & 2/5 \end{pmatrix}.$$

(c) Déterminer la limite lorsque k tend vers $+\infty$ de la probabilité qu'une case particulière soit occupée par une particule après k étapes.

Le graphe est connexe et symétrique et apériodique, donc il y a convergence en loi vers la loi uniforme.