Vincent Pilaud
Kholles de mathématiques
MP*1/MP*2 - Lycée du Parc - Lyon

1, 2 et 3 juin 2005

Mathématiques discrètes

Table des matières

1 Géométrie

1.1 Théorème de Helly

Exercice. [Théorème de Radon]

Soit A un ensemble de $d+2$ points de $\mathbb{R}^d$. Montrer qu'il existe une partition $\{A_1, A_2\}$ de A telle que $\mathrm{Conv}(A_1) \cap \mathrm{Conv}(A_2) \neq \emptyset$.

Exercice. [Théorème de Helly - intersection finie]

Soient $n \geq d+1$ et $C_1, \ldots, C_n$ des convexes de $\mathbb{R}^d$. On suppose que pour tout $(i_1, \ldots, i_{d+1}) \in \{1, \ldots, n\}^{d+1}$, l'intersection des convexes $C_{i_1}, \ldots, C_{i_{d+1}}$ est non vide. Montrer qu'alors l'intersection de tous les convexes $C_1, \ldots, C_n$ est non vide.

Exercice. [Théorème de Helly - intersection de compacts]

Soit $\mathcal{C}$ une famille de compacts convexes tels que l'intersection de $d+1$ de ces éléments soit toujours non vide. Montrer que l'intersection de tous les compacts convexes de $\mathcal{C}$ est non vide.

Exercice. [Contre-exemple]

Montrer qu'une famille infinie de convexes non compacts de $\mathbb{R}^d$, telle que l'intersection de $d+1$ de ces éléments soit toujours non vide n'est pas nécessairement d'intersection non vide.

Exercice. [Application]

Montrer qu'il existe une constante optimale $r(d)$ (que l'on calculera) telle que toute famille finie de points deux à deux distants d'au plus 1 soit incluse dans une boule de rayon $r(d)$.

Exercice. [Théorème de Jung]

Soit X un compact de $\mathbb{R}^d$ et δ sont diamètre (ie. $\delta = \sup\{d(x,y) \mid x, y \in X\}$). Montrer que X est contenu dans une boule unique de rayon minimum r. Montrer de plus que

$$r \leq \delta \sqrt{\frac{d}{2(d+1)}},$$

cette inégalité étant la meilleure possible.

2 Théorie des graphes

2.1 Planarité des graphes

On rappelle qu'un **graphe** G est un couple (V, E) où V est l'ensemble des **sommets** de G et $E \subset \binom{V}{2}$ est l'ensemble des **arêtes** de G. Un **plongement** $\tilde{G} = (\tilde{V}, \tilde{E})$ de G dans le plan $\mathbb{R}^2$ est la donnée d'une famille $\tilde{V} = \{p_v\}_{v \in V}$ de points du plan indéxée par les éléments de V et d'une famille $\tilde{E} = \{\gamma_e\}_{e \in E}$ d'arcs ouverts (ie. image de l'intervalle ouvert $]0; 1[$ par une application injective continue de $[0; 1]$ dans $\mathbb{R}^2$) du plan indéxée par les éléments de E telles que

1. $p_v \neq p_{v'}$ pour $v \neq v'$,
2. les extrémités de l'arc γ_e associé à l'arête $e = \{v; v'\}$ sont les points p_v et $p_{v'}$,
3. γ_e évite tout point de $\tilde{V}$.

On dit que le graphe G est **planaire** lorsqu'il existe un plongement $\tilde{G} = (\tilde{V}, \tilde{E})$ de G tel que les arcs de $\tilde{E}$ sont deux à deux disjoints.

Le but de ce qui suit est d'étudier la planarité des graphes.

Exercice. [Formule d'Euler]

Montrer rapidement que pour tout graphe plongé dans le plan, on a la formule :

$$f - a + s = 2,$$

où f désigne le nombre de faces du plongement du graphe, a le nombre d'arêtes et s le nombre de sommets du graphe.

Exercice. [Combinatoire des graphes planaires simples]

En étudiant les relations d'incidence faces/arêtes, et en utilisant la formule d'Euler, montrer que le nombre d'arêtes et le nombre de sommets d'un graphe planaire simple sont liés par l'inégalité :

$$a \leq 3n - 6.$$

Exercice. [Graphes non planaires]

On note K_n le **graphe complet** à n sommets :

$$K_n = (\{1, 2, \ldots, n\}, \{\{i, j\} \mid i < j \in \{1, \ldots, n\}\}),$$

et $K_{n \times m}$ le **graphe bipartite complet** à n et m sommets :

$$K_{n \times m} = (\{A_1 \ldots, A_n\} \cup \{B_1, \ldots, B_m\}, \{\{A_i, B_j\} \mid i \in \{1, \ldots, n\}, j \in \{1, \ldots, m\}\}).$$

Montrer que K_5 n'est pas planaire. Avec des arguments similaires, montrer que $K_{3\times3}$ n'est pas planaire.

Remarque. [Théorème de Kuratowski]

En fait, les graphes non planaires sont essentiellement représentés par les graphes K_5 et $K_{3\times3}$. En effet, on peut montrer (théorème de Kuratowski) que tout graphe non planaire admet soit le graphe K_5, soit le graphe $K_{3\times3}$ comme sous-graphe.

Plus généralement, étant donné une surface de genre g, on peut trouver un système de représentants de graphes qui ne se plongent pas dans cette surface de sorte que tout graphe ne se plongeant pas dans cette surface contienne au moins l'un des représentants comme sous-graphe.

Soit G un graphe. Pour tout plongement $\tilde{G} = (\tilde{V}, \tilde{E})$ de ce graphe, on appelle **nombre de croisements** de $\tilde{G}$ le nombre

$$\mathfrak{C}(\tilde{G}) = \sum_{\{e,e'\} \in \binom{E}{2}} \phi(\{e, e'\}),$$

où $\phi(\{e, e'\})$ désigne le nombre de points d'intersection des arcs γ_e et $\gamma_{e'}$. Le **nombre de croisements** de G (noté $\mathfrak{C}(G)$) est le minimum des $\mathfrak{C}(\tilde{G})$ lorsque $\tilde{G}$ décrit l'ensemble des plongements de G dans le plan.

Exercice. [Nombre de croisements de K_5]

Quel est le nombre de croisements de K_5 ?

Exercice. [Minoration du nombre de croisements]

1. Soit G un graphe avec n sommets et m arêtes, et $\tilde{G}$ un plongement de G. En utilisant l'inégalité de combinatoire des graphes planaires simples sur un graphe bien choisi, montrer que $\mathfrak{C}(\tilde{G}) - m + 3n \geq 0$.

2. On considère un plongement $\tilde{G}$ de G qui réalise le nombre chromatique de G, c'est-à-dire tel que $\mathfrak{C}(G) = \mathfrak{C}(\tilde{G})$. Pour un réel p compris entre 0 et 1, on considére un échantillon aléatoire R de V obtenu en tirant de manière indépendante chaque sommet de V avec la probabilité p, et on note $\tilde{G}_R$ le sous-graphe de $\tilde{G}$ correspondant. On note $n(R)$ (resp. $m(R)$, resp. $\mathfrak{C}(R)$) la variable aléatoire correspondant au nombre de sommets (resp. d'arêtes, resp. de croisements) obtenus avec cet échantillon du graphe.

Calculer les espérances de $n(R)$, $m(R)$ et $\mathfrak{C}(R)$.

Montrer que pour tout $p \in [0; 1]$, on a $p^4\mathfrak{C}(G) - p^2m + 3pn \geq 0$.

En déduire que si $m \geq 4n$, alors

$$\mathfrak{C}(G) \geq \frac{m^3}{64n^2}.$$

2.2 Coloriabilité des graphes

Un graphe $G = (V, E)$ est dit **k-coloriable** si il existe une partition de V en au plus k parts telles que les extrémités de toute arête de E soient toujours séparées par cette partition. À titre d'exemple, on peut noter qu'un graphe ne peut être coloriable que si il est sans boucle. On appelle **nombre chromatique** du graphe G l'entier $\chi(G)$ tel que G est $\chi(G)$-coloriable, mais pas $(\chi(G) - 1)$-coloriable.

Le but de ce qui suit est de majorer le nombre chromatique d'un graphe planaire.

Exercice. [Nombre chromatique d'un graphe k-régulier]

Soit G un graphe k-régulier à n sommets. Montrer que le nombre chromatique de G vérifie $\chi(G) \geq \frac{n}{n-k}$.

Exercice. [Théorème du sommet de degré 5]

En utilisant la formule d'Euler, montrer que tout graphe planaire simple contient un sommet de degré inférieur ou égal à 5.

Exercice. [6-coloriabilité des graphes planaires simples]

Montrer que tout graphe planaire simple est 6-coloriable.

Exercice. [5-coloriabilité des graphes planaires simples]

En utilisant le théorème du sommet de degré 5 et le fait que K_5 n'est pas planaire, montrer que tout graphe planaire simple est 5-coloriable.

Exercice. [Art-Galery problem]

On considère une galerie d'art (modélisée par un polygone simple P) que l'on doit surveiller en plaçant un minimum de caméras (chaque caméra étant un point dont l'angle de vision est de 2π. En considérant un 3-coloriage d'une triangulation de P, montrer que l'on peut surveiller la galerie avec $\lfloor \frac{n}{3} \rfloor$ caméras (où n est le nombre de sommets de P). Montrer par ailleurs que cette borne est optimale.

2.3 Complexité des graphes bipartites

Exercice.

Montrer que pour tous $a \geq b$ entiers naturels, $(a-b+1)^b \leq b!\binom{a}{b} \leq a^b$.

Exercice. [Inégalité de Hölder]

Le but de l'exercice est de montrer l'inégalité de Hölder, à savoir que si p et q sont deux exposants conjugués (ie. $\frac{1}{p} + \frac{1}{q} = 1$) et si f et g sont deux fonctions mesurables, alors

$$\int |fg| d\mu \leq \left(\int |f|^p d\mu \right)^{\frac{1}{p}} \left(\int |g|^q d\mu \right)^{\frac{1}{q}}.$$

Soit $\alpha \in [0;1]$. Montrer que pour tout $x \in \mathbb{R}^+$, $x^\alpha - \alpha x \leq 1 - \alpha$.

En déduire que pour $u, v \geq 0$, on a

$$u^\alpha v^{1-\alpha} \leq \alpha u + (1-\alpha) v.$$

Appliquer ce résultat à $\alpha = \frac{1}{p}$, $u = \frac{|f|^p}{\int |f|^p d\mu}$ et $v = \frac{|g|^q}{\int |g|^q d\mu}$ et en déduire le résultat en intégrant.

Remarque.

On admettra à partir de ce résultat que pour tout couple (p,q) d'exposants conjugués et toute familles sommables $(a_i)_{i \in I}$ et $(b_i)_{i \in I}$, on a l'inégalité

$$\sum_{i \in I} |a_i b_i| \leq \left(\sum_{i \in I} |a_i|^p \right)^{\frac{1}{p}} \left(\sum_{i \in I} |b_i|^q \right)^{\frac{1}{q}}.$$

Exercice. [Lemme de T. Kõvàri, V. Sós et P. Turàn]

Soit $A \subset M \times N$ un graphe bipartite inclus dans les ensembles M et N de cardinaux respectifs m et n. On suppose qu'il existe des constantes s et t telles que A ne contienne aucun sous-graphe bipartite complet $K_{s \times t}$ (ie le graphe

$$K_{s \times t} = (\{m_1 \ldots, m_s\} \cup \{n_1, \ldots, n_t\}, \{\{m_i, n_j\} \mid i \in \{1, \ldots, s\}, j \in \{1, \ldots, t\}\})).$$

Le but de ce qui suit est de montrer que

$$|A| = O(\min\{mn^{1-1/s} + n, nm^{1-1/t} + m\}).$$

On note $d_1, \ldots, d_n$ les degrés respectifs des sommets de N.

En considérant les sous-graphes $K_{s \times 1}$ du graphe A, montrer que

$$\sum_{i=1}^{n} \binom{d_i}{s} \leq (t-1)\binom{m}{s}.$$

En déduire que

$$\sum_{d_i \geq s} (d_i - s + 1)^s \leq (t-1) m^s.$$

En remarquant que $|A| = \sum_{i=1}^n d_i$ et en appliquant l'inégalité de Hölder, montrer que

$$|A| \leq (s-1)n + n^{1-1/s}(t-1)^{1/s} m.$$

Conclure.

2.4 Spectre d'adjacence d'un graphe

On considère un graphe $G = (V, E)$ fini et on indexe les sommets de G par les entiers de 1 à $n = |V|$. On appelle **matrice d'adjacence** de G la matrice $A = [a_{ij}]_{i,j\in\{1,\dots,n\}}$ où les coefficients a_{ij} sont définis par

$$a_{ij} = \begin{cases} 1 \text{ si } \{v_i, v_j\} \in E \\ 0 \text{ sinon} \end{cases}$$

Montrer que cette matrice est diagonalisable dans une base orthonormée. On note $\mu_1 \geq \dots \geq \mu_n$ ses valeurs propres en prenant en compte les multiplicités.

Le but de ce qui suit est d'étudier les relations entre les propriétés du graphes et celles du spectre de cette matrice.

Exercice. [Spectre d'adjacence d'un graphe k-régulier]

Soit $G = (V, E)$ un graphe et v un sommet de G. Le **degré** de v est défini par

$$\deg(v) = |\{w \in V \mid \{v; w\} \in E\}.$$

On dit que le graphe G est **k-régulier** si le degré de tout sommet de G est k.

Montrer que le vecteur $\begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$ est vecteur propre de la matrice d'adjacence A de G associé à la valeur propre k.

Montrer que $\forall i \in \{1, \dots, n\}, |\mu_i| \leq k$.

Montrer que la valeur propre $\mu_1 = k$ est de multiplicité 1 si et seulement si le graphe est connexe. (on pourra compléter ce résultat en montrant que la multiplicité de μ_1 est le nombre de composantes connexes du graphe G).

Exercice. [Spectre d'adjacence d'un graphe k-régulier bipartite]

On rappelle qu'on dit d'un graphe $G = (V, E)$ qu'il est **bipartite** si il existe une partition V_1, V_2 de V qui sépare les extrémités de toute arête de E.

On considère un graphe G connexe k-régulier et on note A sa matrice d'adjacence. Montrer l'équivalence des trois propositions suivantes :

1. G est bipartite,
2. le spectre d'adjacence de G est symétrique par rapport à 0,
3. $\mu_n = -k$.

Exercice. [Exemples]

On note K_n (resp. C_n) le **graphe complet** (resp. le **cycle**) à n sommets. Calculer la matrice d'adjacence de K_n (resp. C_n) et vérifier la proposition précédente.

Exercice. [Sommes spectrales]

Soit $G = (V, E)$ un graphe fini simple sans boucle dont le spectre d'adjacence est $\mu_1 \geq \dots \geq \mu_n$. Montrer que

$$\sum_{i=1}^{n} \mu_i = 0, \quad \sum_{i=1}^{n} \mu_i^2 = 2|E|, \quad \sum_{i=1}^{n} \mu_i^3 = 6|T|,$$

où T désigne l'ensemble des triangles formés par le graphe G.

Exercice. [Généralisation - graphes infinis]

Soit $G = (V, E)$ un graphe qui n'est pas nécessairement fini. Pour tout $(x, y) \in V^2$, on note

$$a_{xy} = \begin{cases} 1 \text{ si } \{x, y\} \in E \\ 0 \text{ sinon} \end{cases}$$

Par ailleurs, on note

$$\ell^2(V) = \{f : V \to \mathbb{C} \mid \sum_{x \in V} |f(x)|^2 < +\infty\}.$$

On dit que le graphe G est de **degré borné** si il existe $N \in \mathbb{N}$ tel que le degré de chaque sommet de G soit borné par N (ie. tel que $\forall x \in V, \sum_{y \in V} a_{xy} \leq N$).

Montrer que dans ce cas, pour toute fonction $f \in \ell^2(V)$, on a

$$\|Af\|_2 = \left(\sum_{x \in V} |(Af)(x)|^2\right)^{\frac{1}{2}} \leq N.\|f\|_2 = N.\left(\sum_{x \in V} |f(x)|^2\right)^{\frac{1}{2}},$$

c'est-à-dire que A est un opérateur borné de $\ell^2(V)$. Quelle est la norme de cet opérateur ?

Exercice. [Nombre d'indépendance et nombre chromatique]

On appelle **nombre d'indépendance** d'un graphe $G = (V, E)$ le nombre

$$\iota(G) = \max\{|F| \mid F \subset V, \forall x, y \in F, \{x; y\} \notin E\}.$$

On dit que G est k**-coloriable** si il existe une partition de V en au plus k parts qui sépare les extrémités de toute arête de E. On appelle **nombre chromatique** du graphe G l'entier $\chi(G)$ tel que G est $\chi(G)$-coloriable, mais pas $(\chi(G) - 1)$-coloriable.

Montrer que pour un graphe fini sans boucle à n sommets, on a l'inégalité

$$n \leq \iota(G)\chi(G)$$

Exercice. [Nombre chromatique d'un graphe fini, connexe, k-régulier]

On considère un graphe G fini, connexe, k-régulier, avec n sommets. On note $\mu_1 > \ldots \geq \mu_n$ son spectre d'adjacence. Le but de l'exercice est de montrer que le nombre chromatique de G vérifie

$$\chi(G) \geq \frac{k}{\max\{|\mu_2|, |\mu_n|\}}.$$

Soit $F \subset V$ telle que $|F| = \iota(G)$. On considère la fonction f définie par

$$\forall x \in V, \quad f(x) = \begin{cases} |V \setminus F| \text{ si } x \in F \\ -|F| \text{ si } x \in V \setminus F \end{cases}$$

Montrer que $\|f\|_2^2 \leq \iota(G)n^2$.

Montrer que pour tout $x \in F$, $(Af)(x) = -k\iota(G)$ et en déduire que $\|Af\|_2^2 \geq k^2\iota(G)^3$.

En remarquant que $\sum_{x \in V} f(x) = 0$ (ie. que le vecteur propre f est orthogonal aux fonctions constantes), montrer que $\|Af\|_2 \leq \max\{|\mu_2|, |\mu_n|\}\|f\|_2$.

Déduire des questions précédentes que

$$\iota(G) \leq \frac{n}{k} \max\{|\mu_2|, |\mu_n|\}$$

et conclure à l'aide de l'exercice précédent.

2.5 Théorie algébrique des graphes

Soit $G = (V, E)$ un graphe et e une arête de G. On notera $G - e$ le graphe dont l'ensemble des sommets est V et l'ensemble des arêtes est $E \setminus \{e\}$ et G/e le graphe dont l'ensemble des sommets est V/e et l'ensemble des arêtes est l'ensemble des paires de sommets hérités des arêtes de E (en fait, ceci revient à écraser l'arête e).

Exercice. [Polynôme chromatique]
Soit $G = (V, E)$ un graphe et $k \in \mathbb{N}$. Une **k-coloration** de G est une partition $V = V_1 \sqcup \ldots \sqcup V_k$ qui sépare les extrémités de toute arête de E. On note $\chi_G(k)$ le nombre de k-colorations de G.

1. Montrer que pour tout graphe G et toute arête e de G, on a

$$\chi_G(k) = \chi_{G-e}(k) - \chi_{G/e}(k).$$

En déduire que χ_G est un polynôme en k. Ce polynôme est le **polynôme chromatique** de G.

2. Calculer le polynôme chromatique d'un arbre à n sommets, du cycle à n sommets, du graphe complet à n sommets,...

Exercice. [Polynôme de Tutte]
Soit $G = (V, E)$ un graphe et $e \in E$. On dit que e est une **boucle** si ses deux extrémités sont identiques et un **isthme** $|\kappa(G-e)| = |\kappa(G)|+1$ (où $\kappa(G)$ est le nombre de composantes connexes de G). On appelle **polynôme de Tutte** le polynôme $T_G(X, Y) \in \mathbb{C}[X, Y]$ défini par induction :

- $T_{(\{v\},\emptyset)}(X, Y) = 1$,
- $T_G(X, Y) = XT_{G/e}(X, Y)$ si $e \in E$ est un isthme,
- $T_G(X, Y) = YT_{G-e}(X, Y)$ si $e \in E$ est une boucle,
- $T_G(X, Y) = T_{G/e}(X, Y) + T_{G-e}(X, Y)$ si $e \in E$ n'est ni un isthme, ni une boucle.

Remarque.
On ne demande pas de démontrer la bonne définition de ce polynôme. En fait, la question suivante nous permet de nous affranchir de cette preuve pénible.

1. Soit $F \subset E$. On note par abus $\kappa(F) = \kappa((V, F))$ le nombre de composantes connexes du graphe restreint à F. On note par $rg(F) = |V| - \kappa(F)$ et $n(F) = |F| - rg(F) = |F| - |V| + \kappa(F)$. Montrer que

$$\forall G = (V, E), \quad T_G(X, Y) = \sum_{F \subset E} (X-1)^{rg(E)-rg(F)}(Y-1)^{n(F)}.$$

2. Interpréter les nombres $T_G(1, 1)$, $T_G(2, 1)$, $T_G(1, 2)$ et $T_G(2, 2)$.

3. Calculer le polynôme de Tutte d'un arbre à n sommets, du cycle à n sommets, du graphe complet à n sommets,...

Remarque. [Évaluation du polynôme de Tutte]
En fait, l'évaluation du polynôme de Tutte est NP-dur, sauf aux points $(1, 1)$, $(-1, -1)$, $(0, -1)$, $(-1, 0)$, $(i, -i)$, $(-i, i)$, (j, j^2), (j^2, j) où elle est polynômiale.

Exercice. [Polynôme chromatique et polynôme de Tutte]
Montrer que

$$\chi_G(k) = (-1)^{|V|-1}kT_G(1-k, 0).$$

2.6 Graphes de Cayley

Soit G un groupe et S une partie finie, non vide et symétrique de G. Le **graphe de Cayley** $\mathcal{C}(G,S)$ est le graphe (V,E) avec

$$V = G \qquad E = \{\{x,y\} \mid x,y \in G,\ xy^{-1} \in S\}.$$

Exercice. [Exemples]
Quel est le graphe de Cayley $\mathcal{C}(\mathbb{Z}^2, \{(0,1),(0,-1),(1,0),(-1,0)\})$?
Comment exprimer le graphe complet K_n comme un graphe de Cayley ? Et le cycle C_n ?

Exercice. [Relation entre les propriétés de S et celles de $\mathcal{C}(G,S)$]
Soit $k = |S|$. Montrer que :

1. $\mathcal{C}(G,S)$ est k-régulier et simple,
2. $\mathcal{C}(G,S)$ est sans boucle si et seulement si $1 \notin S$,
3. $\mathcal{C}(G,S)$ est connexe si et seulement si S engendre G,
4. si il existe un morphisme $\lambda : G \to \{1,-1\}$ tel que $\lambda(S) = \{-1\}$, alors $\mathcal{C}(G,S)$ est bipartite. La réciproque est vraie lorsque $\mathcal{C}(G,S)$ est connexe.

3 Théorie des nombres

3.1 Réciprocité quadratique

Exercice. [Quelques rappels sur les corps finis]
Montrer que la cardinalité d'un corps fini $\mathbb{K}$ est nécessairement de la forme $q = p^\alpha$ où p est un nombre premier et α un entier non nul. p est appelée **caractéristique** du corps $\mathbb{K}$.

Exercice. [Carrés en caractéristique 2]
Montrer que dans un corps de caractéristique 2, tout élément est un carré.

Exercice. [Carrés en caractéristique impaire - Symbole de Legendre - Réciprocité quadratique]
Soit $\mathbb{F}_p$ le corps fini à p éléments (avec $p > 2$). Étant donné $x \in \mathbb{F}_p$, le symbole de Legendre de x est défini par

$$\left(\frac{x}{p}\right) = \begin{cases} 0 & \text{si } x = 0 \\ 1 & \text{si } x \neq 0 \text{ est un carré dans } \mathbb{F}_p \\ -1 & \text{sinon} \end{cases}$$

Montrer que $\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}}$. En déduire que $\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right)$.

Montrer que $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. (On montrera que p^2-1 est divisible par 8. On en déduira l'existence d'une racine primitive huitième de l'unité ζ dans $\mathbb{F}_{p^2}$. On vérifiera que $\zeta + \zeta^{-1}$ est une racine carrée de 2 dans $\mathbb{F}_{p^2}$.On concluera en trouvant la condition nécessaire et suffisante pour que 2 soit un carré dans $\mathbb{F}_p$).

Dans la suite de l'exercice, on veut montrer que pour tous nombres premiers p et q,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Pour cela, on introduit la **somme de Gauss** de la manière suivante. Soit ω une racine primitive q-ième de l'unité dans $\overline{\mathbb{F}}_p$. On pose

$$S = \sum_{x \in \mathbb{F}_q} \left(\frac{x}{q}\right) \omega^x.$$

Montrer que $S^2 = (-1)^{\frac{q-1}{2}} q$, puis que $S^{p-1} = \left(\frac{p}{q}\right)$. Conclure.

3.2 Approximation diophantienne des nombres algébriques

Soit $k \subset K$ un corps. On dit qu'un nombre $\alpha \in K$ est **algébrique** sur k s'il existe un polynôme $P \in k[X]$ tel que $P(\alpha) = 0$. Dans le cas contraire, α est **transcendant** sur k.

Notons que si α est algébrique, l'ensemble des polynômes de $k[X]$ qui s'annulent sur α est un idéal de $k[X]$. Le générateur unitaire de cet idéal est appelé **polynôme minimal** de α sur k et le degré de ce polynôme est appelé **degré** de α sur k.

Exercice.[Approximation des nombres algébriques]
Soit α un nombre algébrique sur $\mathbb{Q}$ de degré d. Montrer qu'il existe une constante γ telle que pour tout rationnel $\frac{p}{q}$, on a

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{\gamma}{q^d}.$$

Autrement dit, un nombre algébrique s'approche mal par une suite de rationnels.

Exercice. [Un nombre transcendant]
Montrer que $\sum_{i\in\mathbb{N}} \frac{1}{10^{i!}}$ est transcendant.

4 Théorie des groupes

4.1 Théorème de Polya

Soit $\mathbb{X} = \{x_1, \ldots, x_n\}$ un ensemble d'objets, $\mathbb{A} = \{a_1, \ldots, a_m\}$ un ensemble de couleurs et G un sous-groupe de $\mathfrak{S}_n$. G agit sur $\mathbb{X}$ par

$$\begin{array}{ccc} G \times \mathbb{X} & \longrightarrow & \mathbb{X} \\ (g, x_i) & \longmapsto & g \cdot x_i = x_{g(i)} \end{array}$$

Un **coloriage** de $\mathbb{X}$ par $\mathbb{A}$ est une application $\phi : \mathbb{X} \to \mathbb{A}$. On note $\mathfrak{C}$ l'ensemble des coloriages de $\mathbb{X}$ par $\mathbb{A}$. Le groupe G agit sur $\mathfrak{C}$ par

$$\begin{array}{ccc} G \times \mathfrak{C} & \longrightarrow & \mathfrak{C} \\ (g, \phi) & \longmapsto & g \cdot \phi : x \mapsto \phi(g^{-1} \cdot x) \end{array}$$

Une orbite pour cette action est appelée **schéma de coloriage**.

Le but du problème est de montrer que le nombre S schémas est donné par

$$S = \frac{1}{|G|} \sum_{g\in G} |\mathbb{A}|^{\gamma(g)},$$

où $\gamma(g)$ désigne le nombre de cycles de g dans sa décomposition en cycles à supports disjoints.

Exercice. [Lemme de Burnside]
On considère un groupe G agissant sur un ensemble X.
Si $x \in X$, on appelle **orbite** de x l'ensemble $\omega(x) = \{g \cdot x \mid g \in G\}$. L'ensemble des orbites est noté Ω. Étant donné $x \in X$, on appelle **stabilisateur** de x l'ensemble $\mathrm{Stab}(x) = \{g \in G \mid g \cdot x = x\}$. Symétriquement, étant donné $g \in G$, l'**ensemble des points fixes** de g est défini par $\mathrm{Fix}(g) = \{x \in X \mid g \cdot x = x\}$.

Montrer rapidement que pour tout $x \in X$, on a $|G| = |\omega(x)||\mathrm{Stab}(x)|$.

En considérant le cardinal de l'ensemble $F = \{(g, x) \in G \times X \mid g \cdot x = x\}$, montrer la formule de Burnside :

$$|G||\Omega| = \sum_{g\in G} |\mathrm{Fix}(g)|.$$

Exercice. [Théorème de Polya]

On considère l'action de G sur l'ensemble des coloriages décrite plus haut.

Soit $g \in G$. Montrer qu'un coloriage φ est dans $\mathrm{Fix}(g)$ si et seulement si il est constant sur les orbites de $\langle g \rangle$ pour l'action de G sur $\mathbb{X}$. En déduire une bijection entre $\mathrm{Fix}(g)$ et l'ensemble des applications de $\{1, \ldots, \gamma(g)\}$ dans A. Montrer alors la formule de Polya.

Exercice. [Application]

Quel est le nombre de colliers différents à 6 perles que l'on peut faire avec 3 couleurs ?

5 Combinatoire

5.1 Séries génératrices

Une **classe combinatoire** est un ensemble $\mathcal{C}$ muni d'une application de **taille** $|.| : \mathcal{C} \to \mathbb{N}$ telle que l'image réciproque de tout entier par $|.|$ est finie. Notons que $\mathcal{C}$ est donc nécessairement fini ou dénombrable.

La **suite de dénombrement** de $(\mathcal{C}, |.|)$ est la suite $C_n = |\mathcal{C}_n| = |\{\gamma \in \mathcal{C} \mid |\gamma| = n\}|$.

La **série génératrice** de $\mathcal{C}$ est la série formelle définie par

$$C(z) = \sum_{n \in \mathbb{N}} C_n z^n = \sum_{\gamma \in \mathcal{C}} z^{|\gamma|}.$$

Exercice. [Exemples]

Quelle est la série génératrice de l'ensemble des mots sur l'alphabet $\{a, b, c, d\}$ lorsque l'application de taille est la longueur d'un mot ?

Quelle est la série génératrice de l'ensemble $\mathfrak{S}$ des permutations (sachant que si $\sigma \in \mathfrak{S}_n$, $|\sigma| = n$) ?

Quel est le nombre de façon de couvrir le segment $[1, n]$ avec des petits segments de longueur 1 ou 2 ?

Exercice. [Nombres de Catalan]

1. Un mot **bien parenthèsé** est un mot $v = v_1 \ldots v_{2l}$ sur l'alphabet $\{0, 1\}$ tel que

$$\sum_{i=1}^{2l} v_i = l \qquad \text{et} \qquad \forall i \leq 2l,\ \sum_{j=1}^{i} v_j \leq \frac{i}{2}.$$

Montrer que pour tout mot $w = w_1 \ldots w_{2l+1}$ sur l'alphabet $\{0, 1\}$ tel que $\sum_{i=1}^{2l+1} w_i = l$, il existe un unique i tel que $w_{i+1} \ldots w_{2l+1} w_1 \ldots w_i = v0$, où v est un mot de parenthèse.

En déduire que le nombre de mots de parenthèses de longueur $2l$ vaut

$$P_l = \frac{1}{l+1} \binom{2l}{l}.$$

On pourra aussi en déduire une méthode de tirage aléatoire d'un mot de parenthèses.

2. Soit A un ensemble de n points en position convexe. On appelle **triangulation** de ces points tout ensemble maximal d'arêtes disjointes (sauf éventuellement en leurs extrêmités). On note T_n le nombre de façon de trianguler n points en position convexe.

Montrer que la suite T_n vérifie la relation de récurrence suivante :

$$T_n = \sum_{k=0}^{n-1} T_k T_{n-k-1}.$$

Montrer que cette relation se traduit sur la série génératrice $T(z)$ associée par l'équation fonctionnelle :

$$T(z) = 1 + zT(z)^2,$$

et en déduire l'expression de $T(z)$, puis des coefficients T_n.

3. Montrer combinatoirement l'égalité entre P_n et T_n.

Exercice. [Série génératrice d'un langage rationnel]

Montrer que la série génératrice d'un langage reconnaisable est une fraction rationnelle.

Exercice. [Langage évitant un motif]

On considère un alphabet $\mathbb{A}$ à a lettres. Soit $M = m_0 \dots m_{l-1} \in \mathbb{A}^*$ un motif fixé de longueur l. On appelle **polynôme d'autocorrélation** de M le polynôme $P_M(z) = p_0 + p_1 z + \ldots + p_{l-1} z^{l-1}$ avec

$$p_i = \begin{cases} 1 \text{ si } \forall j, m_j = m_{i+j} \\ 0 \text{ sinon} \end{cases}$$

Soient $\mathbb{S}_M = \{w \in \mathbb{A}^* \mid M \notin w\}$ et $\mathbb{R}_M = \{w \in \mathbb{A}^* \mid w = vM, v \in \mathbb{S}_M\}$. On note $S(z)$ et $R(z)$ les séries génératrices associées à ces deux langages.

Montrer que

$$\begin{cases} \mathbb{S}_M + \mathbb{R}_M = \{\varepsilon\} + \mathbb{S}_M \times \mathbb{A} \\ \mathbb{S}_M \times \{M\} = \mathbb{R}_M \times \sum_{p_i=1} \{m_i + 1 \dots m_{l-1}\} \end{cases}$$

En déduire que

$$\begin{cases} S(z) + R(z) = 1 + azS(z) \\ S(z)z^l = R(z)P_M(z) \end{cases}$$

Montrer enfin que

$$S(z) = \frac{P_M(z)}{z^l + P_M(z)[1 - az]}.$$

Exercice. [Estimation asymptotique des coefficients du développement d'une fraction rationnelle]

On considère une fraction rationnelle $f(z) = \frac{g(z)}{h(z)}$ telle que $h(0) \neq 0$. On note $\Omega = \{\alpha \in \mathbb{C} \mid h(\alpha) = 0\}$ l'ensemble des **pôles** de f et $\mu(\alpha)$ la **multiplicité** d'un pôle (ie. la multiplicité de α en tant que racine de h). On note $[z^n]f(z)$ le n-ième coefficient de f dans sa décomposition en série entière.

Montrer que pour n assez grand (à préciser),

$$[z^n]f(z) = \sum_{\alpha \in \Omega} R_\alpha(n)\alpha^n,$$

où R_α est un polynôme qui ne dépend que de α et dont le degré est $\mu(\alpha) - 1$. En déduire que si l'un des pôles α est de module $|\alpha|$ inférieur au module de tout autre pôle (on dit que le pôle α est **dominant**), alors on a l'équivalent

$$[z^n]f(z) \simeq C|\alpha|^{-n} n^{\mu(\alpha)-1}.$$

Exercice. [Application : probabilités]

On s'intéresse aux mots sur l'alphabet $\mathbb{A} = \{0, 1\}$.

Donner une expression rationnelle non ambigüe du langage $\mathbb{L}$ des mots évitant le mot 00.

En déduire une expression de la série génératrice $L(z)$ du langage $\mathbb{L}$. (on pourra vérifier que cette expression correspond bien à la formule générale de l'exercice sur les langages évitant un motif).

On se propose alors de calculer trois probabilités intéressantes :

1. Donner la probabilité $\mathbb{P}(n)$ pour qu'un mot de longueur n sur l'alphabet $\mathbb{A}$ ne contienne pas le motif 00 (on pourra en donner un équivalent asymptotique en se référant à l'exercice précédent).

2. Montrer que l'espérance $\mathbb{E}$ de la première occurence du motif 00 s'exprime par $L(\frac{1}{2})$.

3. Calculer le nombre moyen d'occurences du motif dans un texte de longueur n.

5.2 Formule des équerres

On note $\preccurlyeq$ l'ordre sur $(\mathbb{N}^*)^2$ défini par $(a,b) \preccurlyeq (c,d) \Leftrightarrow a \leq c$ et $b \leq d$. On notera $(a,b) \prec (c,d)$ lorsque $(a,b) \preccurlyeq (c,d)$ et $(a,b) \neq (c,d)$.

Un **diagramme de ferrers** F est une partie de $(\mathbb{N}^*)^2$ tels que si $(c,d) \in F$ et $(a,b) \preccurlyeq (c,d)$, alors $(a,b) \in F$. La **taille** de F est son cardinal.

Si $(a,b) \in F$, on appelle **équerre** de (a,b) dans F l'ensemble

$$Eq_F(a,b) = \{(c,d) \in F \mid a = c \text{ et } b \leq d \text{ ou } a \leq c \text{ et } b = d\}.$$

On note $eq_F(a,b) = |Eq_F(a,b)|$.

Soit F un diagramme de Ferrers de taille n. Un **tableau de Young** de forme F est une application $\phi : F \to \{1,\dots,n\}$ telle que

$$\forall u \prec v \in F, \quad \phi(u) < \phi(v).$$

Le but du problème est de montrer que le nombre de tableaux de Young de forme F vaut

$$N_F = \frac{n!}{\prod_{u \in F} e_F(u)}.$$

Exercice. [Chemins dans un diagramme de Ferrers]

Soit F un diagramme de Ferrers. On dit qu'un élément $u \in F$ est **maximal** si $\forall v \in F, u \preccurlyeq v \Rightarrow u = v$. Un **chemin** dans F est une suite $u_1,\dots,u_m$ telle que u_m est maximal, et pour tout $1 \leq i < m$, $u_{i+1} \in Eq_F(u_i) \setminus \{u_i\}$. Le **poids** d'un chemin $U = u_1,\dots,u_m$ est défini par la formule

$$\omega_F(U) = \prod_{i=1}^{m-1} \frac{1}{eq_F(u_i) - 1},$$

le poids d'un chemin réduit à une seule case étant par convention égal à 1.

Remarque. Le poids d'un chemin est en fait la probabilité de l'emprunter en partant de la case u_1 et en choisissant à chaque étape aléatoirement une case de $Eq_F(u_i) \setminus \{u_i\}$ jusqu'à arriver sur une case maximale.

Étant donné un chemin $U = u_1,\dots u_m = (a_1,b_1),\dots,(a_m,b_m)$, on note $I(U) = \{a_i \mid i \in \{1,\dots,m\}\} \setminus \{a_m\}$ sa première projection et $J(U) = \{b_i \mid i \in \{1,\dots,m\}\} \setminus \{b_m\}$ sa seconde.

Ensuite, pour un élément $u = (a,b)$ maximal, et $I \subset \{1,2,\dots,a-1\}$ et $J \subset \{1,2,\dots,b-1\}$, on note $\gamma_F(u,I,J)$ l'ensemble des chemins U dans F dont l'extremité est u, la première projection est I et la seconde est J.

Montrer par récurrence que pour tout triplet (u,I,J) convenable ($u = (a,b)$, $I \subset \{1,2,\dots,a-1\}$ et $J \subset \{1,2,\dots,b-1\}$), on a

$$\sum_{U \in \gamma_F(u,I,J)} \omega_F(U) = \prod_{i \in I} \frac{1}{eq_F(i,b) - 1} \prod_{j \in J} \frac{1}{eq_F(a,j) - 1}.$$

En déduire que

$$\Omega_F(u) = \sum_{\substack{U \text{ chemin} \\ \text{d'extremité } u}} \omega_F(U) = \prod_{\substack{v \in F \\ u \in Eq_F(v)}} \left(1 + \frac{1}{eq_F(v)}\right).$$

Exercice. [Poids d'un tableau de Young]

On considère un tableau de Young (F, ϕ) tel que $|F| = n$. Soit $u \in F$ tel que $\phi(u) = n$. Cet élément est nécessairement maximal dans F (par définition des tableaux de Young). On définit le poids $\Lambda(F, \phi)$ du tableau (F, ϕ) de manière récursive :

$$\Lambda(\emptyset) = 1 \quad \text{et} \quad \Lambda(F, \phi) = \Omega_F(u).\Lambda(F \setminus \{u\}, \phi_{|F \setminus \{u\}}).$$

1. En utilisant l'exercice précédent, montrer par récurrence que

$$\Lambda(F, \phi) = \prod_{v \in F} eq_F(v).$$

2. Soit $v \in F$. Montrer que la somme des poids des chemins d'origine v vaut 1.

Remarque. On attend une preuve algébrique, même si le résultat est clair au vue de la remarque précédente sur le poids d'un chemin.

En déduire que la somme des poids de tous les chemins d'une forme F vaut n.

3. Montrer par récurrence que la somme des poids de tous les tableaux de forme F vaut $n!$. Conclure.

5.3 Mots

Exercice. [Formule d'inversion de Möbius]

1. On définit la **fonction de Möbius** $\mu : \mathbb{N}^* \longrightarrow \{0, 1, -1\}$ par $\mu(1) = 1$, $\mu(n) = 0$ si n possède un facteur carré, et $\mu(p_1 \dots p_r) = (-1)^r$ si $p_1, \dots, p_r$ sont des nombres premiers distincts.

Montrer que

$$\sum_{d|n} \mu(d) = \delta_{1,n},$$

où $\delta_{i,j}$ est le symbole de Kronecker (ie. $\delta_{i,j} = 1$ si $i = j$ et 0 sinon). On pourra montrer aussi que cette égalité caractérise la fonction de Möbius.

2. Soit $(G, +)$ un groupe abélien et $f : \mathbb{N}^* \longrightarrow A$. On pose

$$g(n) = \sum_{d|n} f(d).$$

En utilisant la première question, montrer que

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

Exercice. [Mots de Lyndon]

On considère un alphabet $\mathbb{A} = \{a_1, \dots, a_q\}$ de cardinal q. L'ordre $\prec_{\text{lex}}$ désigne l'ordre lexicographique strict sur $\mathbb{A}^*$. On dit qu'un mot $u \in \mathbb{A}^*$ est un **mot de Lyndon** si pour tous mots $v, w \in \mathbb{A}^\times$ tels que $u = vw$, on a $u \prec_{\text{lex}} w$.

1. Donner les mots de Lyndon de longueur 1, 2, 3 et 4.

2. Montrer qu'un mot de Lyndon est strictement plus petit que tous ses conjugués.

3. Montrer que tout mot qui n'est pas puissance d'un autre mot admet un unique conjugué qui est un mot de Lyndon.

4. On note $L_q(l)$ le nombre de mots de Lyndon sur l'alphabet $\mathbb{A}$ de longueur l. Montrer que

$$q^n = \sum_{d|n} dL_q(d).$$

5. En déduire, par l'exercice précédent, que

$$L_q(n) = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d}.$$

5.4 Suite de Thue-Morse

Soit $n \in \mathbb{N}$. On note $(b_i(n))_{i\in\mathbb{N}}$ la décomposition de n en base 2, c'est-à-dire que $\forall i \in \mathbb{N}, b_i(n) \in \{0,1\}$ et

$$n = \sum_{i\in\mathbb{N}} b_i(n) 2^i.$$

On pose

$$B(n) = \sum_{i\in\mathbb{N}} b_i(n) \quad \text{et} \quad S_n = (-1)^{B(n)}.$$

La suite $(S_n)_{n\in\mathbb{N}}$ est appelée **suite de Thue-Morse**.

Un **facteur** de **longueur** p d'une suite $(u_n)_{n\in\mathbb{N}} \in E^{\mathbb{N}}$ est une suite finie $(v_n)_{n\in\{0,\dots,p-1\}} \in E^p$ telle qu'il existe $N \in \mathbb{N}$ tel que $\forall k \in \{0,\dots,p-1\}$, $u_{N+k} = v_k$. L'entier N s'appelle alors **début d'occurence** de v dans u. On note $occ[v,u]$ l'ensemble des débuts d'occurence de v dans u et $R[v,u] = \min occ[v,u]$. On note

$$\rho_u(p) = \max_{v\in E^p} R[v,u] \quad \text{et} \quad F_u(p) = p + \rho_u(p).$$

On désigne enfin par $P_u(p)$ le nombre de facteurs de longueur p de la suite u.

Exercice. [Facteurs impossibles, congruence des débuts d'occurence]
Montrer que $S_{2n} = S_n$ et que $S_{2n+1} = -S_n$.
En déduire que si n est pair, alors $S_{n+1} = -S_n$.
Montrer qu'aucune des suites $(1,1,1)$, $(-1,-1,-1)$, $(1,-1,1,-1,1)$, $(-1,1,-1,1,-1)$ n'est facteur de la suite $(S_n)_{n\in\mathbb{N}}$.
Soit t un facteur de la suite de Thue-Morse de longueur au moins 4. Montrer que si m et n sont deux débuts d'occurence de t, alors $m \equiv n \mod 2$.

Exercice. [Expressions explicites des suites $(\rho_S(p))_{p\in\mathbb{N}}$, $(F_S(p))_{p\in\mathbb{N}}$ et $(P_S(p))_{p\in\mathbb{N}}$]
Montrer que

$$\forall p \geq 3, \quad \rho_S(p) = 2\rho_S\left(\lfloor \frac{p}{2} \rfloor + 1\right) + 1,$$

$$\forall p \geq 3, \quad F_S(p) \leq 2F_S\left(\lfloor \frac{p}{2} \rfloor + 1\right),$$

$$\forall p \geq 3, \quad P_S(2p) = P_S(p+2) + P_S(p) \quad \text{et} \quad P_S(2p+1) = 2P_S(p+1).$$

En déduire que

$$\forall p \geq 3, \quad \rho_S(p) = 3.2^{\ln_2(p-2)} - 1,$$

$$\forall p \geq 3, \quad F_S(p) \leq 8(p-2),$$
$$\forall p \geq 3, \quad P_S(p) \leq 4(p-1).$$

Exercice. [Un produit étrange]
Le but de l'exercice est de montrer que

$$\prod_{n=0}^{\infty} \left(\frac{2n+1}{2n+2}\right)^{S_n} = \frac{1}{\sqrt{2}}$$

On pose

$$P = \prod_{n=0}^{\infty} \left(\frac{2n+1}{2n+2}\right)^{S_n}, \quad Q = \prod_{n=1}^{\infty} \left(\frac{2n}{2n+1}\right)^{S_n} \quad \text{et} \quad R = \prod_{n=1}^{\infty} \left(\frac{n}{n+1}\right)^{S_n}.$$

Montrer que P, Q et R sont des produits convergents, puis que $PQ = \frac{1}{2}R$ et que $R = \frac{Q}{P}$. En déduire le résultat.

6 Dénombrabilité

Exercice. [Théorème de Cantor-Bernstein]
Soit X un ensemble, $Y \subset X$ et f une injection de X dans Y. On définit par récurrence les ensembles $(A_n)_{n\in\mathbb{N}}$ de la manière suivante : $A_0 = X \setminus Y$ et $A_{n+1} = f(A_n)$.

1. Montrer que les ensembles $(A_n)_{n\in\mathbb{N}}$ sont deux à deux disjoints.

2. Montrer que f réalise une bijection de $\bigcup_{n\in\mathbb{N}} A_n$ dans $\bigcup_{n\in\mathbb{N}^*} A_n$.

3. En déduire une bijection de X sur Y.

4. Démontrer le théorème de Cantor-Bernstein : si il existe une injection de A dans B et de B dans A, alors il existe une bijection de A dans B.

Exercice. [Parties d'un ensemble]
Soit A un ensemble infini.

1. Soit X une partie dénombrable de A telle que $A \setminus X$ infini. Montrer que A et $A \setminus X$ sont équipotents.

2. On veut montrer que A et $\mathcal{P}(A)$ ne peuvent pas être en bjection. En supposant qu'une telle bijection f existe, et en considérant l'ensemble $\{a \in A \mid a \notin f(a)\}$, montrer ce résultat.