DS 3 de mathématiques

Durée : 4 heures. Tout appareil électronique est interdit. Une attention particulière sera portée à la qualité de la rédaction et à la rigueur du raisonnement.

Les trois problèmes sont indépendants. Au sein d'un problème, les différentes parties sont essentiellement indépendantes ; cependant, certaines définitions ou résultats pourront avoir été donnés dans une partie précédente.

1 Formule d'inversion de Möbius

Dans ce problème, on étudie différents aspects de la formule d'inversion de Möbius.

On montre dans un premier temps qu'une telle formule existe dans un ensemble ordonné fini quelconque ; puis on en donne des applications aux ordres donnés par l'inclusion dans $\mathcal{P}(E)$ ou par la divisibilité dans $\mathbb{N}$.

1.1 Cadre théorique

Soit $(P, \leq)$ un ensemble ordonné fini.

- On note $P^{2,\leq} = \{(x, y) \in P^2 \mid x \leq y\}$.
- Si $(x, y) \in P^{2,\leq}$, on appelle distance de x à y et on note $d(x, y)$ le plus grand entier naturel n tel que
$$\exists (x_0, \dots, x_n) \in P^{n+1} : x = x_0 < x_1 < x_2 < \dots < x_n = y.$$
- Une fonction $\mu : P^{2,\leq} \to \mathbb{Z}$ est la fonction de Möbius de $(P, \leq)$ si elle vérifie :
$$\forall (x, z) \in P^{2,\leq}, \sum_{x \leq y \leq z} \mu(x, y) = \delta_{x,z},$$
où $\delta_{x,z} = 1$ si $x = z$ et 0 sinon.

0. Soit $(x, y) \in P^{2,\leq}$. Montrer que $d(x, y)$ est bien définie et que
$$d(x, y) = 0 \iff x = y.$$

1. En raisonnant par récurrence sur la distance entre deux éléments $x \leq y$, montrer l'existence et l'unicité de la fonction de Möbius de $(P, \leq)$.

On la notera μ dans la suite. On admet qu'on a de même :

$$\forall (x,z) \in P^{2,\leq}, \sum_{x \leq y \leq z} \mu(y,z) = \delta_{x,z}.$$

2. Soient f, g deux applications de P dans $\mathbb{R}$. Montrer l'équivalence entre

   i) $\forall y \in P, g(y) = \sum_{x \leq y} f(x)$; ii) $\forall y \in P, f(y) = \sum_{x \leq y} g(x)\mu(x,y)$.

On admet qu'on a aussi l'équivalence entre :

i) $\forall x \in P, g(x) = \sum_{x \leq y} f(y)$; ii) $\forall x \in P, f(x) = \sum_{x \leq y} g(y)\mu(x,y)$.

On appelle *formules d'inversion de Möbius* ces équivalences.

1.2 Principe d'inclusion-exclusion

Dans cette partie, $n \in \mathbb{N}^*$, $E = [\![1,n]\!]$ et $P = \mathcal{P}(E)$, ordonné par la relation d'inclusion.

3. Soit $(A,B) \in P^{2,\leq}$. Que vaut la distance de A à B ?

4. On définit μ sur $P^{2,\leq}$ par

   $$\forall (A,B) \in P^{2,\leq}, \mu(A,B) = (-1)^{|B|-|A|}.$$

   Montrer que μ est la fonction de Möbius de P.

Ainsi, si $f, g : \mathcal{P}(E) \to \mathbb{R}$, on a les équivalences suivantes :

- $\forall B \in \mathcal{P}(E), g(B) = \sum_{A \subset B} f(A) \iff \forall B \in \mathcal{P}(E), f(B) = \sum_{A \subset B} g(A)(-1)^{|B|-|A|}$
- $\forall A \in \mathcal{P}(E), g(A) = \sum_{A \subset B} f(B) \iff \forall A \in \mathcal{P}(E), f(A) = \sum_{A \subset B} g(B)(-1)^{|B|-|A|}$.

C'est la formulation générale du *principe d'inclusion-exclusion.*

5. **Première application.** En déduire la formule d'inversion de Pascal : si $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$ sont deux suites réelles telles que $\forall n \in \mathbb{N}, v_n = \sum_{k=0}^{n} \binom{n}{k} u_k$, alors

   $$\forall n \in \mathbb{N}, u_n = \sum_{k=0}^{n} \binom{n}{k} (-1)^{n-k} v_k.$$

6. **Deuxième application.** Soit F un ensemble fini, soient $A_1, \dots, A_n$ des parties de F. On définit $f : \mathcal{P}(E) \to \mathbb{N}$ par
$$\forall I \in \mathcal{P}(E), f(I) = \Big|\Big(\bigcap_{i\in I} A_i\Big) \bigcap \Big(\bigcap_{j\in \overline{I}} \overline{A_j}\Big)\Big|.$$
   (a) On définit $g : \mathcal{P}(E) \to \mathbb{N}$ par
$$\forall I \in \mathcal{P}(E), g(I) = \sum_{I\subset J} f(J).$$
   Simplifier l'expression de $g(I)$.

   (b) En déduire la formule du crible :
$$\Big|\bigcap_{i=1}^{n} \overline{A_i}\Big| = \sum_{J\subset [\![1,n]\!]} (-1)^{|J|}\Big|\bigcap_{j\in J} A_j\Big|.$$

1.3 Inversion de Möbius dans $\mathbb{N}^*$

Dans cette partie, $N \in \mathbb{N}^*$ et $P = [\![1, N]\!]$, ordonné par la relation de divisibilité.

On définit $\tilde{\mu} : \mathbb{N}^* \to \mathbb{Z}$ par
$$\forall n \in \mathbb{N}^*, \tilde{\mu}(n) = \begin{cases} 0 & \text{s'il existe un nombre premier } p \text{ tel que } p^2 \text{ divise } n \\ (-1)^r & \text{si } n \text{ est le produit de } r \text{ nombres premiers distincts.} \end{cases}$$
En particulier, $\tilde{\mu}(1) = 1$.

7. Montrer que $\forall n > 1, \sum_{\substack{d\mid n\\ d>0}} \tilde{\mu}(d) = 0$.

On en déduit aisément que la fonction de Möbius μ de P est définie par
$$\forall (d, n) \in P^{2,\leq}, \mu(d, n) = \tilde{\mu}(\frac{n}{d}).$$

8. **Une application.** Pour tous $d \in [\![1, N]\!]$, on définit
$$H_d^N = \{(u, v) \in [\![1, N]\!]^2 \mid u \wedge v = d\}.$$
   (a) Montrer que
$$\forall d \in [\![1, N]\!], \lfloor \frac{N}{d} \rfloor^2 = \sum_{\substack{1\leq n\leq N\\ d\mid n}} |H_n^N|.$$
   (b) En déduire que
$$|H_1^N| = \sum_{n=1}^{N} \tilde{\mu}(n)\lfloor \frac{N}{n} \rfloor^2.$$

2 Théorème d'Erdős-Ginzburg-Ziv

Pour tout $n \geq 2$, on note $\mathcal{P}(n)$ l'assertion suivante :

$$\forall (x_1, \dots, x_{2n-1}) \in \mathbb{N}^{2n-1}, \exists I \subset [\![1, 2n-1]\!] : |I| = n \text{ et } \sum_{i \in I} x_i \equiv 0\,[n].$$

Autrement dit, $\mathcal{P}(n)$ affirme que parmi $2n-1$ entiers naturels, on peut en choisir n dont la somme est divisible par n.

On cherche à montrer $\mathcal{P}(n)$, pour tout $n \geq 2$.

2.1 Généralités et structure de la démonstration

1. Montrer $\mathcal{P}(2)$.
2. Montrer $\mathcal{P}(3)$.
3. On fixe $n \geq 2$. Montrer que si on remplace $2n-1$ par $2n-2$ dans $\mathcal{P}(n)$, l'assertion ainsi obtenue est fausse.
4. Montrer que si $n, m \geq 2$ sont tels que $\mathcal{P}(n)$ et $\mathcal{P}(m)$ sont vraies, alors $\mathcal{P}(nm)$ est vraie.
5. En déduire qu'il est suffisant de montrer $\mathcal{P}(p)$, pour tout nombre premier p, pour en déduire $\mathcal{P}(n)$, pour tout entier $n \geq 2$.

2.2 Démonstration de $\mathcal{P}(p)$, p premier

On fixe un nombre premier p et on cherche à démontrer $\mathcal{P}(p)$. Soient $x_1, \dots, x_{2p-1}$ des entiers naturels. Pour tout $I \subset [\![1, 2p-1]\!]$, de cardinal p, on note $S_I = \sum_{i \in I} x_i$. On note enfin

$$S = \sum_{\substack{I \subset [\![1,2p-1]\!] \\ |I| = p}} S_I^{p-1}.$$

6. Montrer que pour tout $k \in [\![1, p-1]\!]$, p divise $\binom{2p-k-1}{p-k}$.
7. En déduire que p divise S. *On admettra la formule du multinôme : si* $I = \{i_1, \dots, i_p\}$,

$$S_I^{p-1} = \sum_{\substack{0 \leq \alpha_1, \dots, \alpha_p \leq p-1 \\ \alpha_1 + \dots + \alpha_p = p-1}} \binom{p-1}{\alpha_1, \dots, \alpha_p} x_{i_1}^{\alpha_1} \dots x_{i_p}^{\alpha_p},$$

où $\binom{p-1}{\alpha_1, \dots, \alpha_p} = \dfrac{(p-1)!}{\alpha_1! \dots \alpha_p!}$.

8. On suppose par l'absurde que $\mathcal{P}(p)$ est faux. Aboutir à une contradiction et conclure.

3 Théorème de l'amitié

Soit E un ensemble fini de cardinal N, $\mathcal{R}$ une relation sur E symétrique et anti-réflexive, c'est-à-dire : $\forall x \in E, \mathrm{non}(x \,\mathcal{R}\, x)$. Si $x \in E$, on note

$$N(x) = \{y \in E \mid x \,\mathcal{R}\, y\} \text{ et } d(x) = |N(x)|.$$

On considère (A) et (B) les propriétés suivantes :

$$\begin{array}{ll} (A) & \forall x, y \in E, (x \neq y) \implies |N(x) \cap N(y)| = 1. \\ (B) & \exists x \in E, d(x) = N - 1. \end{array}$$

Le théorème de l'amitié – démontré en 1966 par Erdős, Rényi et Sós – affirme que $(A) \implies (B)$. De façon imagée, si dans un groupe de personnes deux quelconques ont exactement un ami en commun, alors il existe une personne amie avec tout le monde.

Pour bien apprécier les définitions qui suivent, on pourra représenter la situation sous la forme d'un graphe dont les sommets sont les éléments de E, deux sommets x et y étant reliés par une arête ssi $x \,\mathcal{R}\, y$. Les illustrations graphiques pour appuyer un argument combinatoire seront valorisées.

- Deux éléments x et y de E sont adjacents si $x \,\mathcal{R}\, y$.
- Si $(E, \mathcal{R})$ vérifie la propriété (A) et si $x \neq y$ sont deux éléments de E, on note $x \vee y$ l'unique élément adjacent à x et y.

On a donc $N(x) \cap N(y) = \{x \vee y\}$.

- Soit $n \geq 2$. Un chemin de longueur n est un $(n+1)$-uplet $(x_0, \dots, x_n)$ d'éléments de E tel que, pour tout $i \in [\![0, n-1]\!]$, x_i et x_{i+1} sont adjacents.
- Une boucle de longueur n est un chemin $(x_0, \dots, x_n)$ de longueur n tel que $x_0 = x_n$.
- Un n-cycle est une boucle $(x_0, \dots, x_n)$ de longueur n telle que $x_0, \dots, x_{n-1}$ sont deux à deux distincts.

3.1 Tous les $d(x)$ sont égaux.

0. On suppose que $N = 5$ et que $(E, \mathcal{R})$ vérifie les propriétés (A) et (B). Représenter graphiquement un exemple de cette situation.

On revient au cas général. On suppose que $(E, \mathcal{R})$ vérifie la propriété (A) et on cherche à montrer qu'il vérifie la propriété (B).

1. Montrer qu'il n'existe pas de 4-cycle dans E.

2. Soient x et y distincts et non adjacents dans E. On note

   - $z = x \vee y$; $u = x \vee z$; $v = y \vee z$.
   - Si $u_1, \ldots, u_s$ sont les éléments (distincts) adjacents à x et différents de z et u, on note $v_i = u_i \vee y$, pour tout $i \in [\![1, s]\!]$.

   Représenter graphiquement la situation et montrer brièvement que les éléments x, y, z, u, v, $u_1, \ldots, u_s$ et $v_1, \ldots, v_s$ sont deux à deux distincts.

3. En déduire que si x et y sont non adjacents, alors $d(x) = d(y)$.

On suppose désormais – par l'absurde – que $(E, \mathcal{R})$ ne vérifie pas la propriété (B).

4. Montrer que $\forall x, y \in E, d(x) = d(y)$.

On note m l'entier tel que $\forall x \in E, d(x) = m$.

5. Montrer que $N = 1 + m + m(m-2) = m(m-1) + 1$.

3.2 Conclusion arithmético-combinatoire

Le cas $N = 3$ étant trivial, on suppose $m - 1 \geq 2$. On fixe un nombre premier p divisant $m - 1$. On note $\mathcal{B}_p$ l'ensemble des boucles de longueur p et on cherche à obtenir une contradiction sur le cardinal de $\mathcal{B}_p$.

6. Montrer que $|\mathcal{B}_p| \equiv 0\,[p]$.

On note :

- $\mathcal{C}_{p-2}$ l'ensemble des chemins de longueur $p-2$
- $\mathcal{B}_{p-2}$ l'ensembles des boucles de longueur $p-2$
- $K = |\mathcal{C}_{p-2}|$, $K_1 = |\mathcal{B}_{p-2}|$ et $K_2 = |\mathcal{C}_{p-2} - \mathcal{B}_{p-2}|$.

7. Montrer que $K_1 + K_2 = K = Nm^{p-2}$.

8. Montrer que $|\mathcal{B}_p| = mK_1 + K_2$.

9. En déduire que $|\mathcal{B}_p| \equiv 1\,[p]$ et conclure.