Agrégation Interne 2016/2017

Dénombrements

– I – Fonctions indicatrices d'ensembles

Ω est un ensemble non vide et $\mathcal{P}(\Omega)$ est l'ensemble de toutes les parties de Ω.

À toute partie A de Ω, on associe sa fonction indicatrice définie par :

$$\mathbf{1}_A : \begin{array}{ccc} \Omega & \to & \{0,1\} \\ x & \mapsto & \left\{ \begin{array}{l} 1 \text{ si } x \in A \\ 0 \text{ si } x \notin A \end{array} \right. \end{array}$$

Les fonctions indicatrices permettent de transformer des opérations ensemblistes en opérations algébriques sur des fonctions.

On note $\{0,1\}^{\Omega}$ l'ensemble des applications de Ω dans $\{0,1\}$.

1. Montrer que l'application qui associe à une partie A de Ω sa fonction indicatrice $\mathbf{1}_A$ réalise une bijection de $\mathcal{P}(\Omega)$ sur $\{0,1\}^{\Omega}$.
2. Montrer qu'il n'existe pas de bijection de Ω sur $\mathcal{P}(\Omega)$ (théorème de Cantor).
   Indication : on peut raisonner par l'absurde en considérant, pour φ bijective de Ω sur $P(\Omega)$, l'ensemble $A = \{x \in \Omega \mid x \notin \varphi(x)\}$.
   On en déduit en particulier que $\mathcal{P}(\mathbb{N})$ et $\{0,1\}^{\mathbb{N}}$ ne sont pas dénombrables.
3. Pour tout entier naturel non nul n, on définit les fonctions symétriques élémentaires $\sigma_{n,k} : \mathbb{R}^n \to \mathbb{R}$, l'entier k étant compris entre 0 et n, par :
$$\forall \alpha = (\alpha_1, \cdots, \alpha_n) \in \mathbb{R}^n,\ \sigma_{n,k}(\alpha) = \left\{ \begin{array}{l} 1 \text{ si } k = 0 \\ \displaystyle\sum_{1 \leq i_1 < \cdots < i_k \leq n} \alpha_{i_1}\alpha_{i_2}\cdots\alpha_{i_k} \text{ si } k \in \{1, \cdots, n\} \end{array} \right.$$
   Ces expressions sont qualifiées de symétriques, car pour toute permutation τ de $\{1, \cdots, n\}$, on a :
$$\sigma_{n,k}\left(\alpha_{\tau(1)}, \cdots, \alpha_{\tau(n)}\right) = \sigma_{n,k}(\alpha_1, \cdots, \alpha_n)$$
   (a) Soient $n \geq 2$ un entier et $\alpha = (\alpha_1, \cdots, \alpha_n) = (\alpha', \alpha_n) \in \mathbb{R}^n = \mathbb{R}^{n-1} \times \mathbb{R}$, où on a noté $\alpha' = (\alpha_1, \cdots, \alpha_{n-1}) \in \mathbb{R}^{n-1}$.
   Montrer que :
$$\left\{ \begin{array}{l} \sigma_{n,0}(\alpha) = \sigma_{n-1,0}(\alpha') = 1 \\ \sigma_{n,k}(\alpha) = \sigma_{n-1,k}(\alpha') + \alpha_n \sigma_{n-1,k-1}(\alpha')\ \ (1 \leq k \leq n-1) \\ \sigma_{n,n}(\alpha) = \alpha_n \sigma_{n-1,n-1}(\alpha') \end{array} \right.$$
   (b) Soit $P(X) = \displaystyle\prod_{k=1}^{n}(X - \alpha_k)$ un polynôme scindé unitaire de degré $n \geq 1$ dans $\mathbb{R}[X]$.
   Montrer que l'on a $P(X) = \displaystyle\sum_{k=0}^{n} a_k X^{n-k}$ avec :
$$\forall k \in \{0, 1, \cdots, n\},\ a_k = (-1)^k \sigma_{n,k}(\alpha_1, \cdots, \alpha_n)$$
4. Soit $(A_k)_{1 \leq k \leq n}$ une suite finie de parties de Ω. Montrer que :
   (a) $\mathbf{1}_{\bigcap\limits_{k=1}^{n} A_k} = \displaystyle\prod_{k=1}^{n} \mathbf{1}_{A_k}$;

(b) $\mathbf{1}_{\bigcup\limits_{k=1}^{n} A_k} = \sum\limits_{k=1}^{n} (-1)^{k-1} \sum\limits_{1\leq i_1<\cdots<i_k\leq n} \mathbf{1}_{A_{i_1}\cap A_{i_2}\cdots A_{i_k}}$ (formule de Poincaré) ;

(c) pour $A \in \mathcal{P}(\Omega)$, on a la partition $A = \bigcup\limits_{k=1}^{n} A_k$ si, et seulement si $\mathbf{1}_A = \sum\limits_{k=1}^{n} \mathbf{1}_{A_k}$;

(d) $\mathbf{1}_{\bigcup\limits_{k=1}^{n} A_k} \leq \sum\limits_{k=1}^{n} \mathbf{1}_{A_k} \leq \mathbf{1}_{\bigcap\limits_{k=1}^{n} A_k} + (n-1)$.

5. Soit $(\Omega, \mathcal{B}, \mathbb{P})$ un espace probabilisé.

(a) Montrer que, pour tous A, B dans $\mathcal{B}$, on a :

$$\mathbb{E}(\mathbf{1}_A) = \mathbb{P}(A), \ \operatorname{cov}(\mathbf{1}_A, \mathbf{1}_B) = \mathbb{P}(A\cap B) - \mathbb{P}(A)\,\mathbb{P}(B), \ \mathbb{V}(\mathbf{1}_A) = \mathbb{P}(A)(1-\mathbb{P}(A))$$

(b) Montrer que, pour tous A, B dans $\mathcal{B}$, on a :

$$|\mathbb{P}(A\cap B) - \mathbb{P}(A)\,\mathbb{P}(B)| \leq \frac{1}{4}$$

et :

$$|\mathbb{P}(B) - \mathbb{P}(A)| \leq \mathbb{P}(A \triangle B)$$

(c) Soit $(A_k)_{1\leq k\leq n}$ une suite d'éléments de $\mathcal{B}$.
En utilisant la formule de Poincaré pour les fonctions indicatrices, montrer que :

$$\mathbb{P}\left(\bigcup_{k=1}^{n} A_k\right) = \sum_{k=1}^{n} (-1)^{k-1} \sum_{1\leq i_1<\cdots<i_k\leq n} \mathbb{P}(A_{i_1}\cap\cdots\cap A_{i_k})$$

(formule de Poincaré).

(d) Soit $(A_k)_{1\leq k\leq n}$ une suite d'éléments de $\mathcal{B}$.
Montrer que :

$$\mathbb{P}\left(\bigcup_{k=1}^{n} A_k\right) \leq \sum_{k=1}^{n} \mathbb{P}(A_k) \leq \mathbb{P}\left(\bigcap_{k=1}^{n} A_k\right) + (n-1)$$

– II – Quelques classiques et moins classiques dénombrements

1. Soient E, F deux ensembles finis non vides et φ une application de E dans F.
Montrer que s'il existe un entier naturel non nul p tel que pour tout $y \in F$, $\varphi^{-1}\{y\}$ est de cardinal p, alors φ est surjective et $\operatorname{card}(E) = p\operatorname{card}(F)$ (principe des bergers).

2. On note, pour tout entier $n \geq 2$, $I_n = \{1, 2, \cdots, n\}$ et on appelle dérangement de I_n toute permutation σ de I_n n'ayant aucun point fixe (i. e. telle que $\sigma(i) \neq i$ pour tout $i \in I_n$).
Pour $p \in \mathbb{N}$, on note δ_p le nombre de dérangements de I_p. On a $\delta_1 = 0$ et, par convention, on pose $\delta_0 = 1$.

(a) Montrer que si $(f_n)_{n\in\mathbb{N}}$ et $(g_n)_{n\in\mathbb{N}}$ sont deux suites de réels telles que :

$$\forall n \in \mathbb{N}, \ f_n = \sum_{k=0}^{n} \binom{n}{k} g_k$$

on a alors :

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

(formule d'inversion de Pascal).
Indication : on peut utiliser la matrice de passage de la base canonique $\left(X^k\right)_{0\leq k\leq n}$ *de* $\mathbb{R}_n[X]$ *à la base* $\left((1+X)^k\right)_{0\leq k\leq n}$ *ou raisonner par récurrence sur* $n \geq 0$.

(b) Montrer que :

$$\forall n \in \mathbb{N},\ n! = \sum_{k=0}^{n} \binom{n}{k} \delta_k \tag{1}$$

(c) Montrer que :

$$\forall n \in \mathbb{N},\ \delta_n = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!} \tag{2}$$

Indication : on peut utiliser ou pas la formule d'inversion de Pascal.

(d) On considère n couples qui se présentent à un concours de danse, chaque danseur choisissant une partenaire au hasard (on suppose qu'on est dans le cadre de l'équiprobabilité).

i. Quelle est la probabilité p_n pour que personne ne danse avec son conjoint ?

ii. Calculer la limite de p_n quand n tend vers l'infini.

3. On se propose de montrer la formule (2) en utilisant la série génératrice $\sum \frac{\delta_n}{n!} z^n$ de la suite $\left(\frac{\delta_n}{n!}\right)_{n\in\mathbb{N}}$.

(a) Montrer que la série entière $\sum \frac{\delta_n}{n!} z^n$ est convergente pour $|z| < 1$. On note $f(z)$ sa somme.

(b) En utilisant (1), montrer que, pour $|z| < 1$, on a :

$$f(z) = \frac{e^{-z}}{1-z}$$

(c) En déduire que $\delta_n = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}$.

(d) Montrer que $\delta_n = E\left(\frac{n!}{e} + \frac{1}{2}\right)$ pour tout $n \geq 1$, où E est la fonction partie entière.

4. Pour tout couple (p, n) d'entiers naturels non nuls, on désigne par $u_{p,n}$ le nombre d'applications surjectives de l'ensemble $I_p = \{1, \cdots, p\}$ sur l'ensemble $I_n = \{1, \cdots, n\}$ (ou plus généralement d'un ensemble à p éléments sur un ensemble à n éléments) en convenant que $u_{p,0} = 0$ pour tout entier naturel non nul p.

(a) Montrer que :

$$\forall p \geq n \geq 1,\ n^p = \sum_{k=0}^{n} \binom{n}{k} u_{p,k}$$

(b) En utilisant la formule d'inversion de Pascal, en déduire que :

$$\forall p \geq n \geq 0,\ u_{p,n} = \sum_{k=0}^{n} \binom{n}{k} (-1)^{n-k} k^p$$

(c) Montrer que la série entière $\sum \frac{u_{p,n}}{n!} z^n$ (série génératrice de la suite $\left(\frac{u_{p,n}}{n!}\right)_{n\in\mathbb{N}}$) a un rayon de convergence infini.
On note $f_p(z)$ sa somme pour $p \geq 1$ fixé.

(d) Montrer que $f_p(z)\, e^z = \sum_{n\in\mathbb{N}} \frac{n^p}{n!} z^n$ pour tout nombre complexe z, puis en déduire que :

$$\forall p \geq n \geq 1,\ u_{p,n} = \sum_{k=0}^{n} \binom{n}{k} (-1)^{n-k} k^p$$

(e) Montrer que :

$$\forall n \geq 1,\ \sum_{k=0}^{n} \binom{n}{k} (-1)^{n-k} k^n = n!$$

(f) Montrer que :

$$\forall p \geq n \geq 2,\ u_{p,n} = n\left(u_{p-1,n-1} + u_{p-1,n}\right)$$

En déduire les valeurs de $u_{n+1,n}$ et $u_{n+2,n}$.

5. On note, pour $n \geq 1$, $I_n = \{1, 2, \cdots, n\}$ et on désigne par β_n le nombre de partitions de I_n (nombres de Bell). On convient que $\beta_0 = 1$.

(a) Calculer $\beta_1, \beta_2, \beta_3$.

(b) Montrer que :

$$\forall n \in \mathbb{N},\ \beta_{n+1} = \sum_{k=0}^{n} \binom{n}{k} \beta_k$$

(c) Montrer que :

$$\forall n \in \mathbb{N}^*,\ \sqrt{(n-1)!} \leq \beta_n \leq n!$$

(d) Montrer que la série entière $\sum \frac{\beta_n}{n!} z^n$ a un rayon de convergence infini. On note $f(z)$ sa somme.

(e) Montrer que, pour tout réel x, on a $f'(x) = e^x f(x)$, puis que $f(x) = e^{e^x - 1}$.

(f) En déduire que :

$$\forall n \in \mathbb{N},\ \beta_n = \frac{1}{e} \sum_{k=0}^{+\infty} \frac{k^n}{k!}$$

6. On se propose de calculer, pour tout entier $n \geq 2$, la probabilité r_n pour que deux entiers a, b compris entre 1 et n soient premiers entre eux.
Pour tout entier $n \geq 2$, on note :

$$A_n = \left\{(a, b) \in I_n^2 \mid a \wedge b = 1\right\}$$

φ désigne la fonction indicatrice d'Euler.

(a) En notant $A_n^+ = \{(a, b) \in A_n \mid a < b\}$, montrer que :

$$\operatorname{card}\left(A_n^+\right) = \sum_{k=2}^{n} \varphi(k)$$

(b) En déduire que :

$$\operatorname{card}(A_n) = 2 \sum_{k=1}^{n} \varphi(k) - 1$$

puis que la probabilité cherchée est :

$$r_n = \frac{1}{n^2} \left(2 \sum_{k=1}^{n} \varphi(k) - 1\right)$$

On peut montrer (ce qui est un peu délicat) que $\lim_{n \to +\infty} r_n = \frac{6}{\pi^2}$.

7. On utilise ici le théorème de Lagrange sur les sous-groupes d'un groupe fini pour dénombrer les racines n-èmes de l'unité dans un corps fini.
   $\mathbb{F}_q$ est un corps fini à q éléments ($q = p^r$, où $p \geq 2$ est un nombre premier et r est un entier naturel non nul) et, pour tout entier $n \geq 1$:
$$\mu_n(\mathbb{F}_q) = \{z \in \mathbb{F}_q \mid z^n = 1\}$$
   est l'ensemble des racines n-èmes de l'unité dans $\mathbb{F}_q$.
   (a) Montrer que $\mu_n(\mathbb{F}_q)$ est un sous-groupe du groupe multiplicatif $\left(\mathbb{F}_q^*, \cdot\right)$.
   (b) En désignant par δ le pgcd de n et $q-1$, montrer que $\mu_n(\mathbb{F}_q) = \mu_\delta(\mathbb{F}_q)$.
   (c) Montrer que :
$$\operatorname{card}(\mu_n(\mathbb{F}_q)) = n \wedge (q-1)$$

8. $\mathbb{F}_q$ est un corps fini à q éléments.
   Pour tout entier $m \geq 2$, on note :
$$P_m = \left\{x^m \mid x \in \mathbb{F}_q^*\right\}$$
   l'ensemble des puissances m-èmes dans $\mathbb{F}_q^*$.
   (a) Montrer que P_m est un sous-groupe de cardinal $\dfrac{q-1}{m \wedge (q-1)}$ du groupe multiplicatif $\left(\mathbb{F}_q^*, \cdot\right)$ et que :
$$P_m = \left\{x \in \mathbb{F}_q^* \mid x^{\frac{q-1}{m\wedge(q-1)}} = 1\right\}$$
   (b) Pour $q = 2^r$ et $m = 2$, montrer que $P_2 = \mathbb{F}_{2^r}^*$ (tout élément d'un corps à 2^r éléments est un carré).
   Pour la suite de cet exercice, on suppose que $q = p^r$ avec $p \geq 3$ et $m = 2$, c'est-à-dire qu'on s'intéresse aux carrés dans $\mathbb{F}_q$ pour q impair.
   (c) Montrer que :
      i. il y a $\dfrac{q-1}{2}$ carrés et $\dfrac{q-1}{2}$ non carrés dans $\mathbb{F}_q^*$;
      ii. $P_2 = \left\{x \in \mathbb{F}_q^* \mid x^{\frac{q-1}{2}} = 1\right\}$ et $\mathbb{F}_q^* \setminus P_2 = \left\{x \in \mathbb{F}_q^* \mid x^{\frac{q-1}{2}} = -1\right\}$ (les carrés de $\mathbb{F}_q^*$ sont les racines de $X^{\frac{q-1}{2}} - 1$ et les non carrés sont les racines de $X^{\frac{q-1}{2}} + 1$) ;
      iii. -1 est un carré dans $\mathbb{F}_q^*$ si, et seulement si, q est congru à 1 modulo 4 ;
      iv. le produit de deux non carrés de $\mathbb{F}_q^*$ est un carré, le produit d'un carré et d'un non carré est un non carré.
   (d) Soient a, b dans $\mathbb{F}_q^*$. Montrer que pour tout $c \in \mathbb{F}_q$, il existe x, y dans $\mathbb{F}_q$ tels que $c = ax^2 + by^2$ (prenant $a = b = 1$, on en déduit que tout élément de $\mathbb{F}_q$ est somme de deux carrés).
   (e) Déduire de **8(c)iii** qu'il existe une infinité de nombres premiers de la forme $4n + 1$.

9. $\mathbb{F}_p$ est un corps fini à p éléments pour $p \geq 2$ premier.
   (a) Déterminer le nombre de polynômes unitaires de degré 2 irréductibles dans $\mathbb{F}_p[X]$.
   (b) Donner tous les polynômes unitaires de degré 2 irréductibles dans $\mathbb{F}_2[X]$ et dans $\mathbb{F}_3[X]$.
   (c) À quelles conditions, portant sur les coefficients a, b dans $\mathbb{F}_p$, l'anneau $\dfrac{\mathbb{F}_p[X]}{(X^2 + 2aX + b)}$ est-il un corps ?

(d) Retrouver le résultat de la question **a.** en utilisant celui de la question **c.**

(e) Construire deux corps à 8 et 16 éléments respectivement.

10. $\mathbb{F}_q$ est un corps fini à q éléments et $GL_n(\mathbb{F}_q)$ est le groupe multiplicatif des matrices carrées inversibles d'ordre $n \geq 1$ à coefficients dans $\mathbb{F}_q$.
$SL_n(\mathbb{F}_q)$ est le sous-groupe de $GL_n(\mathbb{F}_q)$ formé des matrices de déterminant égal à 1.
Si E est un $\mathbb{F}_q$-espaces vectoriels de dimension $n \geq 1$, $GL(E)$ est le groupe des automorphismes de E.

(a) Montrer que l'on a :

$$\operatorname{card}(GL_n(\mathbb{F}_q)) = \prod_{k=1}^{n} \left(q^n - q^{k-1}\right) = q^{\frac{n(n-1)}{2}} \prod_{j=1}^{n} \left(q^j - 1\right)$$

et :

$$\operatorname{card}(SL_n(\mathbb{F}_q)) = q^{n-1} \prod_{k=1}^{n-1} \left(q^n - q^{k-1}\right) = q^{\frac{n(n-1)}{2}} \prod_{j=2}^{n} \left(q^j - 1\right)$$

(b) Soient E, F deux $\mathbb{F}_q$-espaces vectoriels de dimensions respectives $n \geq 1$ et $m \geq 1$.
Montrer que les espaces vectoriels E et F sont isomorphes si, et seulement si, les groupes $GL(E)$ et $GL(F)$ sont isomorphes.

(c) Quel est le cardinal du centre de $GL_n(\mathbb{F}_q)$, de $SL_n(\mathbb{F}_q)$?

11. Soit E un $\mathbb{F}_q$-espace vectoriel de dimension $n \geq 1$.
On se propose de dénombrer l'ensemble $DL(E)$ des automorphismes de E qui sont diagonalisables.
$GL(E)$ est le groupe des automorphismes de E.

(a) Montrer que :

$$DL(E) = \left\{u \in GL(E) \mid u^{q-1} = Id\right\}$$

(b) En notant $\mathbb{F}_q^* = \{\lambda_1, \cdots, \lambda_{q-1}\}$, montrer que :

$$\forall u \in DL(E),\ E = \bigoplus_{k=1}^{q-1} \ker(u - \lambda_k Id)$$

(c) En désignant par $\mathcal{F}$ l'ensemble des familles $(E_1, \cdots, E_{q-1})$ de sous-espaces vectoriels de E tels que $E = \bigoplus_{k=1}^{q-1} E_k$, montrer que l'application :

$$\begin{array}{rccc} \varphi : & DL(E) & \to & \mathcal{F} \\ & u & \mapsto & (\ker(u - \lambda_1 Id), \cdots, \ker(u - \lambda_{q-1} Id)) \end{array}$$

est bijective.
Il s'agit alors de dénombrer $\mathcal{F}$.

(d) Pour $(n_1, \cdots, n_{q-1}) \in \mathbb{N}^{q-1}$ tel que $\sum_{k=1}^{q-1} n_k = n$, on note :

$$\mathcal{F}_{(n_1, \cdots, n_{q-1})} = \{(E_1, \cdots, E_{q-1}) \in \mathcal{F} \mid \dim(E_k) = n_k,\ 1 \leq k \leq q-1\}$$

Montrer que pour tous $(E_1, \cdots, E_{q-1})$ et $(F_1, \cdots, F_{q-1})$ dans $\mathcal{F}_{(n_1, \cdots, n_{q-1})}$, il existe $u \in GL(E)$ telle que $u(E_k) = F_k$ pour tout k compris entre 1 et $q-1$.

(e) En notant, pour $(n_1, \cdots, n_{q-1}) \in \mathbb{N}^{q-1}$ tel que $\sum_{k=1}^{q-1} n_k = n$ et $(E_1, \cdots, E_{q-1})$ fixé dans $\mathcal{F}_{(n_1, \cdots, n_{q-1})}$:

$$\operatorname{Stab}(E_1, \cdots, E_{q-1}) = \{u \in GL(E) \mid u(E_k) = E_k \ 1 \leq k \leq q-1\}$$

montrer que :

$$\operatorname{card}(\operatorname{Stab}(E_1, \cdots, E_{q-1})) = \prod_{k=1}^{q-1} \operatorname{card}(GL(E_k))$$

et :

$$\operatorname{card}\left(\mathcal{F}_{(n_1, \cdots, n_{q-1})}\right) = \frac{\operatorname{card}(GL(E))}{\prod_{k=1}^{q-1} \operatorname{card}(GL(E_k))}$$

(f) Déduire de ce qui précède que :

$$\operatorname{card}(DL(E)) = \sum_{\substack{(n_1, \cdots, n_{q-1}) \in \mathbb{N}^{q-1} \\ n_1 + \cdots + n_{q-1} = n}} \frac{\operatorname{card}(GL_n(\mathbb{F}_q))}{\operatorname{card}(GL_{n_1}(\mathbb{F}_q)) \cdots \operatorname{card}\left(GL_{n_{q-1}}(\mathbb{F}_q)\right)}$$

avec la convention $\operatorname{card}(GL_0(\mathbb{F}_q)) = 1$.