Algèbre 01 – Méthodes combinatoires. Problèmes de dénombrement

On note E et F des ensembles non vides. La notation $[1,k]$ désigne les entiers $1 \leq j \leq k$.

1. Quelques outils de dénombrement

1.1. Les principes fondamentaux.

Principe d'égalité. S'il existe une bijection de E sur F alors $\mathrm{Card}(E) = \mathrm{Card}(F)$.

Application. Définition de la dimension d'un espace vectoriel.

Application. Il y a autant de sous-ensembles de E de cardinal pair que de cardinal impair.

Application. Si $p \geq 3$ est premier alors il y a $\frac{p+1}{2}$ carrés dans $\mathbb{F}_p$. On en déduit :
- -1 carré de $\mathbb{F}_p \iff p \equiv 1 \pmod 4$
- $\mathrm{Card}(\mathcal{SO}_2(\mathbb{F}_p)) = \begin{cases} p-1 & \text{si } p \equiv 1 \pmod 4 \\ p+1 & \text{si } p \equiv 3 \pmod 4 \end{cases}$

Application.

$$\mathrm{Card}(GL(\mathbb{F}_q)) = (q^n-1)(q^n-q)\cdots(q^n-q^{n-1})$$

Théorème de récurrence. Soit $\mathcal{P}(n)$ une propriété dépendant de l'entier $n \geq 0$. Si $\mathcal{P}(n_0)$ est vraie et si l'implication "$\mathcal{P}(n) \Rightarrow \mathcal{P}(n+1)$" est vraie pour tout $n \geq n_0$ alors la propriété $\mathcal{P}(n)$ est vraie pour tout $n \geq n_0$.

Principe d'addition. Si $(E_1, \ldots, E_k)$ est une partition de E alors $\mathrm{Card}(E) = \sum_{i=1}^{k} \mathrm{Card}(E_i)$.

Formule du crible. *Si $A_1, \ldots, A_k$ sont finis alors*

$$\mathrm{Card}\left(\bigcup_{i=1}^{k} A_i\right) = \sum_{\emptyset \neq I \subset [1,k]} (-1)^{\mathrm{Card}(I)+1} \mathrm{Card}\left(\bigcap_{i \in I} A_i\right).$$

Application. Soit $n \geq 1$ et $p_1, \ldots, p_k$ les nombres premiers inférieurs à n. La probabilité pour que deux entiers de $\{1, \ldots, n\}$ soient premiers entre eux est

$$1 - \frac{1}{n^2} \sum_{\emptyset \neq I \subset [1,k]} (-1)^{\mathrm{Card}(I)+1} E\left(\frac{n}{\prod_{i \in I} p_i}\right)^2.$$

Principe de multiplication.

$$\mathrm{Card}(E \times F) = \mathrm{Card}(E) \times \mathrm{Card}(F)$$

Principe des tiroirs. Si $\mathrm{Card}(E) > \mathrm{Card}(F)$ alors il n'existe pas d'injection de E dans F.

1.2. Cardinaux de référence.

On pose $n = \mathrm{Card}(E)$.

Définition. Une *p-liste* de E est un élément $(x_1, \ldots, x_p)$ de E^p *i.e.* correspond à une application $[1,p] \to E$.

Proposition. *Le nombre de p-listes de E est n^p.*

Définition. Un *p-arrangement* de E est une p-liste $(x_1, \ldots, x_p) \in E^p$ d'éléments deux à deux distincts *i.e.* correspond à une application injective $[1,p] \to E$.

Proposition. *Le nombre de p-arrangements de E est le nombre noté A_n^p défini par $\mathrm{A}_n^p = 0$ pour $p > n$ et $\mathrm{A}_n^p = \frac{n!}{(n-p)!}$ pour $0 \leq p \leq n$.*

Définition. Une *permutation* de E est un n-arrangement de E *i.e.* correspond à une application bijective $[1,p] \to E$. On note $\mathcal{S}(E)$ l'ensemble des permutations de E.

Proposition. $\mathrm{Card}(\mathcal{S}(E)) = n!$

Définition. Une *p-combinaison* de E est une partie à p éléments de E.
On note C_n^p le nombre de p-combinaisons de E.

Proposition. *On a $\mathrm{C}_n^p = 0$ pour $p > n$ et*

$$\forall p \in [0,n]\ ,\ \mathrm{C}_n^p = \frac{n!}{p!(n-p)!} = \mathrm{C}_n^{n-p} = \mathrm{C}_{n+1}^{p+1} - \mathrm{C}_n^{p+1}.$$

Application. Si $p < n$, alors le nombre de surjection $[1,k] \to E$ est $\sum_{p=0}^{n} (-1)^p \mathrm{C}_n^p (n-p)^k$.

1.3. Quelques exemples.

Formule du binôme de Newton. *Soit A un anneau et $a, b \in A$ tels que $ab = ba$ alors, pour tout $n \geq 0$, on a* $(a+b)^n = \sum_{k=0}^{n} \mathrm{C}_n^k a^k b^{n-k}$.

Si P est une probabilité sur E alors les événements élémentaires sont équiprobables *i.e.* $P(A) = \frac{\mathrm{Card}(A)}{\mathrm{Card}(E)}$.

Exemple. On lance un dé équilibré, la probabilité que le nombre lu soit pair est de $\frac{1}{2}$ et qu'il soit ≥ 3 est de $\frac{2}{3}$.

Exemple. Un candidat est élu à un scrutin par a suffrages contre b pour son adversaire (et il n'y a ni nul, ni blanc). La probabilité qu'il ait gardé la majorité tout au long du dépouillement est de $\frac{a-b}{a+b}$.

Exemples d'algorithmes. Dans la méthode de Gauss, il y a $\frac{n^3}{2}$ additions, $\frac{n^3}{2}$ multiplications et $\frac{n^2}{2}$ divisions. Dans la méthode de Choleski, il y a $\frac{n^3}{6}$ additions, $\frac{n^3}{6}$ multiplications, $\frac{n^2}{2}$ divisions et n racines carrées.

2. Utilisation de fonctions multiplicatives

Définition. Une fonction $f : \mathbb{N}^* \to \mathbb{C}$ est dite *multiplicative* si $f(mn) = f(m)f(n)$ pour $m \wedge n = 1$.

Définition. On définit l'*indicatrice d'Euler* φ en posant, pour tout $n \geq 2$, $\varphi(n) = \mathrm{Card}\{k \in [1,n]; n \wedge k = 1\}$.

Proposition. *Soit $n \geq 1$, alors*
- $\varphi(n) = \mathrm{Card}\ \mathcal{U}(\mathbb{Z}/n\mathbb{Z}) = \mathrm{Card}\ \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$
- $n = \sum_{d|n} \varphi(d)$.
- *Si $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ alors $\varphi(n) = n(1-\frac{1}{p_1})\cdots(1-\frac{1}{p_1})$*

De plus $\limsup_{n \to +\infty} \frac{\varphi(n)}{n} = 1$ et $n^{1-\delta} = o(\varphi(n))$ pour tout $\delta > 0$.

Définition. La *fonction de Möbius* est définie sur $\mathbb{N}^*$ par $\mu(1) = 1$, $\mu(n) = 0$ si n a un facteur carré et $\mu(q_1 \cdots q_r) = (-1)^r$ si les q_j sont des premiers distincts.

Proposition (formule d'inversion)**.** *Soit f, g deux fonctions définies sur $\mathbb{N}^*$ et à valeurs dans un groupe additif G, on a alors équivalence entre*

(i) $f(n) = \sum_{d|n} g(d)$, $\forall n \geq 1$

(ii) $g(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) f(d) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right)$, $\forall n \geq 1$

Application. $\forall n \geq 2$, $\varphi(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) d$

Application. La probabilité pour que deux entiers de $[1, n]$ soient premiers entre eux est $\frac{1}{n^2} \sum_{d=1}^{n} \mu(d) E\left(\frac{n}{d}\right)^2$ et tend vers $\frac{6}{\pi^2}$ lorsque n tend vers l'infini.

Application. Soit p un nombre premier et $f \geq 1$, on note $q = p^f$ et $\Pi(n, q)$ le nombre de polynômes unitaires de degré n irréductibles sur $\mathbb{F}_q$ alors

$$\Pi(n, q) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d = \frac{q^n}{n} + O\left(\frac{q^{n/2}}{n}\right).$$

Application. Soit $n \geq 3$, il y a $\frac{1}{2}\varphi(n)$ polygônes réguliers (convexes ou croisés) à n côtés inscrits dans le cercle trigonométrique tels que 1 soit un sommet.

Proposition (formule d'inversion multiplicative)**.** *Soit f, g deux fonctions définies sur $\mathbb{N}^*$ et à valeurs dans un groupe multiplicatif G, on a alors équivalence entre*

(i) $f(n) = \prod_{d|n} g(d)$, $\forall n \geq 1$

(ii) $g(n) = \prod_{d|n} f(d)^{\mu\left(\frac{n}{d}\right)} = \prod_{d|n} f\left(\frac{n}{d}\right)^{\mu(d)}$, $\forall n \geq 1$

Application. Le produit des polynômes unitaires de degré n irréductibles sur $\mathbb{F}_q$ est

$$\prod_{d|n} (T^{q^d} - T)^{\mu(n/d)} = \prod_{d|n} (T^{q^{n/d}} - T)^{\mu(d)}.$$

3. Utilisation de la théorie des groupes

3.1. **Utilisation d'une partie génératrice en algèbre commutative.** Soit A un anneau d'entiers de corps de nombres, on rappelle que :
- A est un anneau de Dedekind
- le groupe des classes d'idéaux $\mathrm{C}(A)$ est le quotient du groupe abélien des idéaux fractionnaires par le sous-groupe des idéaux fractionnaires principaux
- $\mathrm{C}(A)$ est fini et toute classe non nulle "contient" des idéaux premiers

Lemme. *Soit $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ des idéaux premiers de A tels que $\mathfrak{p}_1 \cdots \mathfrak{p}_r = A\pi$ alors π est irréductible si et seulement s'il n'existe par de sous-produit strict $\mathfrak{p}_{i_1} \cdots \mathfrak{p}_{i_s}$ principal.*

Lemme. *Soit $\mathfrak{p}$ un idéal premier de A dont la classe $\overline{\mathfrak{p}}$ est d'ordre r dans $\mathrm{C}(A)$ alors on a $\mathfrak{p}^r = A\pi$ avec π irréductible dans A.*

Définition. On dit que A est un *anneau semi-factoriel* si la longueur des factorisations d'un élément ne dépend que de l'élément *i.e.* toute égalité du type $\pi_1 \ldots \pi_r = \tau_1 \ldots \tau_s$, où les π_i, τ_j sont irréductibles dans A, implique $r = s$.

Théorème de Carlitz. *A est semi-factoriel si et seulement si* $\mathrm{Card}(\mathrm{C}(A)) \leq 2$.

3.2. **Utilisation d'une partie génératrice en géométrie.** On rappelle que
- $\mathcal{SO}(3)$ est engendré par les demi-tours
- les demi-tours sont conjugués dans $\mathcal{SO}(3)$

Application. $\mathcal{SO}(3)$ est simple.

3.3. **Utilisation d'actions de groupes.** On suppose que G est un groupe agissant sur l'ensemble E, on note $\mathcal{O}_1, \ldots, \mathcal{O}_k$ les orbites pour cette action, $x_1, \ldots, x_k$ un système de représentants et $\mathrm{Fix}(g) = \{x \in E; g \cdot x = x\}$.

Équation aux classes.

$$\mathrm{Card}(E) = \sum_{i=1}^{k} \mathrm{Card}(\mathcal{O}_i) = \sum_{i=1}^{k} \frac{\mathrm{Card}(G)}{\mathrm{Card}(\mathrm{Stab}(x_i))}$$

Formule de Burnside-Frobenius.

$$k = \frac{1}{\mathrm{Card}(G)} \sum_{g \in G} \mathrm{Card}(\mathrm{Fix}(g))$$

Application (théorèmes de Sylow)**.** Si $\mathrm{Card}(G) = p^\alpha m$ avec p est premier ne divisant pas m alors

(i) G admet un p-sous-groupe de Sylow

(ii) tout les p-sous-groupes de Sylow sont conjugués

(iii) le nombre n_p de p-sous-groupes de Sylow divise m et est congru à 1 modulo p

Application (collier de perles)**.** Si on dispose d'un fil circulaire, de 4 perles bleues, de 3 perles blanches et de 2 perles rouges, combien de colliers différents peut-on faire avec ce matériel ?

Application (sous-groupes finis de $\mathcal{SO}(3)$)**.** Si G est un sous-groupe d'ordre $n \geq 2$ de $\mathcal{SO}(3)$ alors G est isomorphe à l'un des groupes $\mathbb{Z}/n\mathbb{Z}$, $D_{n/2}$, $\mathcal{A}_4$, $\mathcal{S}_4$ ou $\mathcal{A}_5$.

Développements

Théorèmes de Carlitz.

Sous-groupes finis de $SO(3)$.

Nombre de polynômes irréductibles unitaires de $\mathbb{F}_q[T]$.

Probabilité pour que deux entiers soient premiers entre eux.

Références

[1] M. Alessandri, *Thèmes de géométrie. Groupes en situation géométrique*, Dunod, 1999.

[2] F. Combes, *Algèbre et géométrie*, Bréal, 1998.

[3] S. Francinou et H. Gianella, *Exercices d'algèbre 1*, Masson, 1993.

[4] S. Francinou, H. Gianella et S. Nicolas, *Oraux X-ENS, algèbre 1*, Cassini, 2001.

[5] R. Lidl and H. Niederreiter, *Introduction to finite fields and their applications*, Cambridge University Press, 1997.

[6] D. Perrin, *Cours d'algèbre*, Ellipses, 1996.