Leçon 190 : Méthodes combinatoire, problèmes de dénombrement.

RM
2022-2023

1 Méthodes ensemblistes et dénombrement

1.1 Cardinal des ensembles finis

Définition 1 : On dit qu'un ensemble E est fini s'il est vide ou s'il existe $n \in \mathbb{N}^*$ tel qu'il existe une bijection de $\{1, 2, ..., n\}$ dans E. L'entier n ne dépends alors pas de la bijection et est appelé cardinal de E, noté $|E|$ ou $Card(E)$. Si E est vide son cardinal est égale à 0.

Remarque 2 : Un ensemble non fini est dit infini. Ils existent différentes sorte d'infini, comme celui de $\mathbb{N}$ et de $\mathbb{R}$.

Proposition 3 : Soient E et F deux ensembles.

- Si E est fini et s'il existe une bijection de E vers F, alors F est fini et $|F| = |E|$. E et F sont dit équipotents.
- Si F est fini et s'il existe une injection de E vers F, alors E est fini et $|E| \leq |F|$.
- Si E est fini et s'il existe une surjection de E vers F, alors F est fini et $|F| \leq |E|$.

Remarque 4 : On détermine parfois le cardinal d'un ensemble en construisant une bijection sur un autre ensemble plus simple dont on connait le cardinal (c'est une approche combinatoire).

Corollaire (Principe des tiroirs) 5 : Soient E et F deux ensembles finis avec $|E| > |F|$. Si φ est une application de E vers F, alors il existe $y \in F$ ayant au moins deux antécédents par φ dans E.

Exemple 6 : Si on choisit 6 nombres distincts dans $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$, il en existe deux dont la somme vaut 11.

Proposition 7 : Soit B un ensemble fini et A une partie de B. Alors A est fini et $|A| \leq |B|$. Si $|A| = |B|$, alors $A = B$.

Proposition 8 : Soient A et B deux ensembles finis.

On a $|A \cup B| = |A| + |B| - |A \cap B|$ ou $|A \cup B| = |A| + |B|$ si A et B sont disjoints.
On a $|A \setminus B| = |A| - |A \cap B|$ ou $|A \setminus B| = |A| - |B|$ si $B \subset A$.

Proposition 9 : Soient $A_1, ..., A_n$ des ensembles finis deux à deux disjoints. Alors $|\bigcup_{i=1}^{n} A_i| = \sum_{i=1}^{n} |A_i|$. Si $A_1, ..., A_n$ forment une partition d'un ensemble fini E, alors $|E| = \sum_{i=1}^{n} |A_i|$.

Remarque 10 : Lorsque tous les $|A_i|$ ont le même cardinal k, alors $|E| = nk$. Ce résultat porte le nom de lemme des bergers, qui vient du fait qu'un berger peut compter ses moutons s'il ne voit que leur pattes, en divisant le nombre de pattes par quatre.

Proposition (Formule du crible de Poincaré) 11 : Soient $A_1, ..., A_n$ des ensembles finis. Alors on a

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{\emptyset \neq I \subset [\![1\,;n]\!]} (-1)^{|I|+1} \left|\bigcap_{i \in I} A_i\right|.$$

1.2 Listes, arrangements et combinaison

Définition 12 : Soit E un ensemble fini avec $|E| = n$ et $p \in \mathbb{N}^*$.

- Listes : On appelle $p-liste$ de E tout éléments $(x_1, ..., x_p)$ de $\mathbb{E}^p$ avec $|E|^p$ le nombre $p-liste$. Les listes modélisent les tirages successifs avec remise.
- Arrangement : pour $p \leq n$, on appelle p-arrangement de E toute $p-liste$ de E d'éléments distincts, avec $A_n^p = n!/(n-p)!$ le nombre de p-arrangement. En particulier, si $p = n$, c'est alors une permutation de E avec $n!$ nombre de permutation. Les arrangements modélisent les tirages successifs sans remise.
- Combinaison : On appelle p-combinaison de E tout partie de E de cardinal p, avec $\binom{n}{p} = \frac{n!}{p!(n-p)!}$ si $p \leq n$ et 0 sinon le nombre de p-combinaison. Les combinaisons modélisent les tirages simultanés.

Exemple 13 : Dans un jeu de 52 cartes, le nombre de façon de tirer 10 cartes :

- Avec remise est de 52^{10}.
- Sans remise est de $A_{52}^{10} = 52 \times 51 \times ... \times 43$.
- Simultanément est de $\binom{52}{10}$.

Proposition 14 : Soient E et F deux ensemble finis.

i) L'ensemble des applications de E vers F, noté F^E, est fini, et on a $|F^E| = |F|^{|E|}$.

ii) En notant $p = |E|$ et $n = |F|$, et lorsque $p \leq n$, l'ensemble des applications injectives de E dans F est fini de cardinal A_n^p.

En notant $|E|$, l'ensemble des bijections de E vers E, appelées permutations de E et noté $\mathcal{S}_E$, est fini de cardinal $n!$.

Proposition 15 : Soit E un ensemble fini. Alors l'ensemble $P(E)$ des parties de E est fini et $|P(E)| = 2^{|E|}$.

Remarque 16 : On peut dénombrer $|P(E)|$ d'un autre manière, en remarquant que

$|P(E)| = \sum_{i=0}^{|E|} A_i$ où A_i sont les nombres de parties de E à i éléments. On trouve alors que $\sum_{k=0}^{n} \binom{n}{k} = 2^n$.

Proposition 17 : Soient n et p deux entiers naturels. Alors si $0 \leq p \leq n$, on a $\binom{n}{p} = \binom{n}{n-p}$. Si $n, p \geq 1$, alors $\binom{n}{p} = \binom{n-1}{p-1} + \binom{n-1}{p}$ (formule de Pascal).

Proposition (Formule du binôme) 18 : Soient a et b deux éléments d'une algèbre qui commutent. Alors on a

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

Remarque 19 : Le dénombrement est très utile pour les probabilités. En effet, sur un espace fini, la probabilité d'un événement s'obtient comme le rapport entre le nombre d'issues favorable et le nombre total d'issues possible.

Exemple (Paradoxe des anniversaires) 20 : Pour savoir la probabilité que parmi n individus, deux au moins ont la même date d'anniversaire, on calcul la probabilité que aucun n'est la même date d'anniversaire. Pour ça on calcul le nombre de cas ou chacun n'a pas la même date d'anniversaire que les autres (issue favorable) soit A_{365}^n, sur le nombre de cas totale (issue possible) soit 365^n.
On a donc $P_n = 1 - \frac{A_{365}^n}{365^n}$. On a $P_n > 1/2$ pour $n = 23$.

2 Dénombrement en théories des groupes et des corps

2.1 En théorie des groupes

E est un ensemble non vide et G un groupe.

Définition 21 : On dit que le groupe G opère à gauche sur l'ensemble E si on a une application $(g, x) \in G \times E \mapsto g.x \in E$ telle que : $\forall x \in E, 1.x = x$ et $\forall (g, g', x) \in G^2 \times E, g.(g'.x) = (gg').x$.

Exemple 22 : G agit sur lui même par translation à gauche $g.h = gh$ et par conjugaison $g.h = ghg^{-1}$ avec $(g, h) \in G^2$.
Le Groupe $\mathcal{S}(E)$ agit naturellement sur E par $\sigma.x = \sigma(x)$ où $(\sigma, x) \in \mathcal{S}(E) \times E$.

Définition 23 : Si G opère sur E, on appelle pour tout x dans E l'orbite de x le sous ensemble $O_x = \{g.x | g \in G\}$. Les orbites forment une partition de G.
On dit que l'action est transitive si pour tout $(x, y) \in E^2$, il existe $g \in G$ tel que $x = g.y$, autrement dit il y a une seule orbite. Si le g est unique, elle est dit simplement transitive.

Définition 24 : On dit que l'action est fidèle si le morphisme de groupe $\varphi : g \in G \mapsto (\varphi(g) : x \mapsto g.x) \in \mathcal{S}(E)$ est injectif, autrement dit si $g.x = x$, alors $g = 1$.

Théorème (Cayley) 25 : L'action de G sur lui même par translation à gauche est fidèle et G est isomorphe à un sous-groupe de $\mathcal{S}(G)$.

Définition 26 : Si G opère sur E, pour tout x dans E, on appelle le sous-ensemble $G_x = \{g \in G | g.x = x =\}$ le stabilisateur de x.

Théorème (Équations aux classes) 27 : Si G est un groupe fini opérant sur E, on a :
i) En prenant $x_1, ..., x_r$ un système de représantant des orbites, on a $|E| = \sum_{i=1}^{r} |O_{x_i}|$.
ii) On a $|G| = |O_x||Gx|$ pour tout x dans E.

Lemme (Formule de Burnside) 28 : Soit G un groupe agissant sur un ensemble E. On note r le nombre d'orbites. Alors

$$r = \frac{1}{|G|} \sum_{g \in G} |Fix(g)|.$$

où $Fix(g) = \{x \in E | g.x = x\}$.

Développement 29 : Le nombre de colorations distinctes du cube avec c couleurs est

$$\frac{c^2}{24}(c^4 + 3^2 + 12c + 8)$$

Dev 1

2.2 En théorie des corps

Proposition 30 : Le cardinal d'un corps fini K est une puissance d'un nombre premier.

Théorème 31 : Soit p un nombre premier et $n \in \mathbb{N}^*$. On pose $q = p^n$. Il existe un unique corps fini de cardinal q noté $\mathbb{F}_q$ à isomorphisme près, qui est le corps de décomposition du polynôme $X^n - X$ sur $\mathbb{F}_p$.

Proposition 32 : Le cardinaux des groupes linéaires sur $\mathbb{F}_q$ sont les suivants :
i) $|GL_n(\mathbb{F}_q)| = (q^n - 1)(q^n - q)...(q^n - q^{n-1})$.
ii) $|SL_n(\mathbb{F}_q)| = (q^n - 1)(q^n - q)...(q^n - q^{n-2})q^{n-1}$.
iii) $|PGL_n(\mathbb{F}_q)| = |SL_n(\mathbb{F}_q)|$.
iv) $|PSL_n(\mathbb{F}_q)| = |SL_n(\mathbb{F}_q)|/(n \wedge q - 1)$.

Définition 33 : Soit $q = p^n$ une puissance d'un nombre premier. On pose $\mathbb{F}_q^2 = \{x \in \mathbb{F}_q | \exists y \in \mathbb{F}_q, x = y^2\}$ et $\mathbb{F}_q^{*2} = \mathbb{F}_q^* \cap \mathbb{F}_q^2$.

Proposition 34 : Si $p = 2$, alors $\mathbb{F}_q^2 = \mathbb{F}_q$. Si $p > 2$, alors $\mathbb{F}_q^2 = (q+1)/2$ et $\mathbb{F}_q^{*2} = (q-1)/2$.

Proposition 35 : Si $p > 2$, alors on a $x \in \mathbb{F}_q^{*2} \Leftrightarrow x^{(q-1)/2} = 1$.

Corollaire 36 : Si $p > 2$, alors -1 est un carré dans $\mathbb{F}_q$ si et seulement si q est congrus à 1 modulo 4.

Application (Théorème des deux carré de Fermat) 37 : Soit Σ l'ensemble des entiers qui sont somme de deux carrés. Alors $n \in \mathbb{N}^*$ est dans Σ si et seulement si $v_p(n)$ est pair pour tout p premier tel que $p = 3[4]$.

3 Fonctions arithmétiques multiplicatives

Définition 38 : Une fonction arithmétique $f : \mathbb{N}^* \to \mathbb{C}$ est dite multiplicative si $f(1) = 1$ et pour tout $a, b > 0$ premiers entre eux, on a $f(ab) = f(a)f(b)$.

3.1 La fonction indicatrice d'Euler

Définition 39 : On appelle fonction indicatrice d'Euler la fonction qui associe à $n \in \mathbb{N}^*$, le nombre $\varphi(n)$ d'entiers compris entre 1 et n qui sont premiers avec n.

Remarque 40 : Pour $n \geq 2$, $\varphi(n)$ est le nombre de générateur de $(\mathbb{Z}/n\mathbb{Z}, +)$ ou le nombre d'éléments inversibles de $(\mathbb{Z}/n\mathbb{Z}, +, \times)$.

Exemple 41 : Si $p \geq 2$ premier, alors $\varphi(p) = p - 1$.

Proposition 42 : La fonction φ est une fonction arithmétique multiplicative.

Théorème 43 : Pour tout entier $n \geq 2$, on a $n = \sum_{d|n} \varphi(d)$.

Théorème 44 : Si $n \geq 2$ a pour décomposition en facteurs premiers $n = \prod_{i=1}^r p_i^{\alpha_i}$, on a alors :

$$\varphi(n) = \prod_{i=1}^r p_i^{\alpha_i - 1}(p_i - 1) = n \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right).$$

Exemple 45 : On a $\varphi(18) = \varphi(2 \times 3^2) = 3 \times 2 = 6$.

3.2 La fonction de Möbius

Définition 46 : Soit $n = \prod_{i=1}^r p_i^{\alpha_i}$ la décomposition en facteurs premiers d'un entier $n \geq 2$. On définit la fonction de möbius μ par :

$$\forall n \in \mathbb{N}^*, \mu(n) = \begin{cases} 1 \text{ si } n = 1 \\ (-1)^r \text{ si } n \text{ est sans facteur carré} \\ 0 \text{ sinon} \end{cases}.$$

Proposition 47 : La fonction μ est une fonction arithmétique multiplicative.

Lemme 48 : On a que $\forall n \in \mathbb{N}^*, \sum_{d|n} \mu(d) = \begin{cases} 1 \text{ si } n = 1 \\ 0 \text{ si } n \geq 2 \end{cases}$.

Proposition (Formule d'inversion de Möbius) 49 : Soient $g : \mathbb{N}^* \mapsto \mathbb{C}$. Alors pour $n \in \mathbb{N}^*$, on a pour $G(n) = \sum_{d|n} g(n/d)$

$$g(n) = \sum_{d|n} \mu(d) G(n/d).$$

Application 50 : Pour tout $n \in \mathbb{N}^*$, on a $\varphi(n) = \sum_{d|n} \mu(d) \frac{n}{d}$.

Application 51 : Soit p un nombre premier. Pour $n \in \mathbb{N}^*$, on note $\mathcal{P}_p(n)$ l'ensemble des polynômes unitaires irréductibles de degré n de $\mathbb{F}_p[X]$ et $I_p(n)$ le cardinal de $\mathcal{P}_p(n)$. Alors on a

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

Développement 52 : Pour $n \geq 1$, on note r_n la probabilité pour que deux entiers choisis aléatoirement dans $[\![1\,;n]\!]$ soient premiers entre eux. Alors $\lim_{n \to +\infty} r_n = \frac{6}{\pi^2}$.

Dev 2

Références :

1. Algèbre Gourdon
2. Algèbre et géometrie Rombaldi
3. Algèbre Perrin
4. Corps Tauvel
5. oraux X-ENS tome 1 algèbre