190 : Méthodes combinatoires, problèmes de dénombrement.

Pandou

31 mai 2022

1 Dénombrement

1.1 Ensembles finis

Définition 1. *On dit qu'un ensemble X est fini s'il est vide ou s'il existe $n \geqslant 1$ tel que X est en bijection avec $[\![1, n]\!]$.*
Cet entier n ne dépend que de X est appelé cardinal de X, noté $\mathrm{Card}(X)$. Le cardinal de l'ensemble vide est 0.

Remarque 2 : Un ensemble qui n'est pas fini est dit infini.

Proposition 3. *Soit X et Y deux ensembles.*
- *Si Y est fini et s'il existe une injection de X vers Y, alors X est fini et $\mathrm{Card}(X) \leqslant \mathrm{Card}(Y)$.*
- *Si X est fini et s'il existe une surjection de X vers Y, alors Y est fini et, $\mathrm{Card}(X) \geqslant \mathrm{Card}(Y)$.*

On a égalité dans les inégalités précédentes si l'injection (ou la surjection) est une bijection.

Remarque 4 : L'approche combinatoire pour calculer le cardinal de X consister à mettre X en bijection avec un ensemble Y dont on connaît le cardinal.

Corollaire 5 (Principe des tiroirs)**.** *Soit X et Y deux ensembles finis tels que $\mathrm{Card}(Y) < \mathrm{Card}(X)$. Si $\varphi : X \longrightarrow Y$ est une application, alors il existe $y \in F$ tel que $\varphi^{-1}(y)$ est de cardinal au moins 2.*

Application 6 : Soit $A \subset [\![1, 2n]\!]$ contenant au moins $n+1$ éléments, alors il existe $a \neq B \in A$ tel que $a|b$.

Application 7 : Soit $\alpha \in \mathbb{R}$ et $n \in \mathbb{N}^*$, alors il existe $\dfrac{p}{q} \in \mathbb{Q}$ avec $1 \leqslant q \leqslant n$ tel que $\left|\alpha - \dfrac{p}{q}\right| < \dfrac{1}{qn}$.

Proposition 8. *Soit X un ensemble fini et A une partie de X, alors A est fini et $\mathrm{Card}(A) \leqslant \mathrm{Card}(X)$. On a égalité si, et seulement si, $A = X$.*

Remarque 9 : Pour des ensembles infinis, on peut avoir une partie stricte de X qui est en bijection avec X tout entier.

Proposition 10. *Soit X un ensemble et A, B deux parties finies de X.*
- *$A \cup B$ est fini et $\mathrm{Card}(A \cup B) = \mathrm{Card}(A) + \mathrm{Card}(B) - \mathrm{Card}(A \cap B)$. Si A et B sont disjoints, on a $\mathrm{Card}(A \sqcup B) = \mathrm{Card}(A) + \mathrm{Card}(B)$.*
- *$A \setminus B$ est fini et $\mathrm{Card}(A \setminus B) = \mathrm{Card}(A) - \mathrm{Card}(A \cap B)$. En particulier, si $B \subset A$, alors $\mathrm{Card}(A \setminus B) = \mathrm{Card}(A) - \mathrm{Card}(B)$.*

Proposition 11. *Soit X un ensemble et $A_1, ..., A_n$ des parties finies deux à deux disjoints, alors*

$$\mathrm{Card}\left(\bigcup_{i=1}^{n} A_i\right) = \sum_{i=1}^{n} \mathrm{Card}(A_i)$$

Remarque 12 : Si tous les (A_i) ont même cardinal et forment une partition de X, alors $\mathrm{Card}(X) = n\mathrm{Card}(A)$: c'est le lemme du berger.

Théorème 13 (Formule du crible)**.** *Soit X un ensemble et $A_1, ..., A_n$ des parties finies, alors*

$$\mathrm{Card}\left(\bigcup_{i=1}^{n} A_i\right) = \sum_{k=1}^{n} (-1)^{k-1} \sum_{1 \leqslant i_1 < ... < i_k \leqslant n} \mathrm{Card}\left(A_{i_1} \cap ... \cap A_{i_k}\right)$$

Application 14 : Soit D_n l'ensemble des permutations de $[\![1, n]\!]$ qui n'a aucun point fixe. Alors,

$$\mathrm{Card}(D_n) = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}$$

1.2 Listes et arrangements

Proposition 15. *Soit $E_1, ..., E_n$ des ensembles finis, alors $E_1 \times ... \times E_n$ est fini et on a*

$$\mathrm{Card}(E_1 \times ... \times E_n) = \mathrm{Card}(E_1) \times ... \times \mathrm{Card}(E_n)$$

En particulier, si X est fini, X^n est fini et $\mathrm{Card}(X^n) = \mathrm{Card}(X)^n$.

Définition 16. *Soit X un ensemble et $p \geqslant 1$. Une p-liste de X est un élément de X^p. On appelle un p-arrangement de X toute p-liste d'éléments de X tous distincts.*

Proposition 17. *Soit X un ensemble de cardinal n et $p \leqslant n$. Le nombre de p-arrangements de X est*

$$A_n^p = n(n-1)...(n-p+1) = \frac{n!}{(n-p)!}$$

Proposition 18. *Soit X et Y deux ensembles finis. L'ensemble des applications de X vers Y est fini et de cardinal* $\mathrm{Card}(Y)^{\mathrm{Card}(X)}$.

Application 19 : On note $p = \mathrm{Card}(X)$ et $n = \mathrm{Card}(Y)$, alors le nombre d'injections de X vers Y est A_n^p.

Proposition 20. *Soit X un ensemble fini, alors $\mathcal{P}(X)$ est fini et de cardinal* $2^{\mathrm{Card}(X)}$.

1.3 Combinaison

Définition 21. *Soit X un ensemble de cardinal n et $p \in \mathbb{N}$. Une p-combinaison de X est une partie de X de cardinal p. Le nombre de p-combinaisons de X est noté* $\binom{n}{p}$.

Proposition 22.

$$\binom{n}{p} = \begin{cases} \frac{n!}{p!(n-p)!} & si\ 0 \leqslant p \leqslant n \\ 0 & sinon \end{cases}$$

Application 23 : $\displaystyle\sum_{k=0}^{n} \binom{n}{k} = 2^n$.

Proposition 24. *On a les formules suivantes :*

1. $\binom{n}{p} = \binom{n}{n-p}$.
2. $\binom{n}{p} = \binom{n-1}{p-1} = \binom{n-1}{p}$.
3. $\binom{n}{p} = \frac{n}{p}\binom{n-1}{p-1}$.

Application 25 : $\displaystyle\binom{n+1}{p+1} = \sum_{k=p}^{n} \binom{n}{k}$.

Théorème 26 (Binôme de Newton)**.** *Soit a et b deux éléments d'une algèbre qui commutent, alors*

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

Application 27 : Soit f, g deux fonctions dérivables n fois, alors $(f \times g)^{(n)} = \displaystyle\sum_{k=0}^{n} f^{(k)} g^{(n-k)}$. En effet, on travaille dans l'anneau $\mathcal{L}\big(\mathcal{C}^\infty(\mathbb{R}^2, \mathbb{C})\big)$ avec $a = \partial_x$ et $b = \partial_y$.

Théorème-Définition 28. *Soit X un ensemble fini de cardinal $n \geqslant 1$ et $i_1, ..., i_p$ des entiers tels que $i_1 + ... + i_p = n$. Le nombre de partitions ordonnées $(A_1, ..., A_p)$ de X telles que* $\mathrm{Card}(A_k) = i_k$ *est appelé coefficient multinomial et vaut*

$$\binom{n}{i_1, ..., i_p} = \frac{n!}{i_1!...i_p!}$$

Théorème 29 (Multinôme)**.** *Soit $a_1, ..., a_p$ des éléments d'une algèbre qui commutent deux à deux, alors*

$$(a_1 + ... + a_p)^n = \sum_{i_1+...+i_p=n} \binom{n}{i_1, ..., i_p} a_1^{i_1} ... a_p^{i_p}$$

1.4 Séries génératrices

Remarque 30 : (Esprit de la méthode) Utiliser l'unicité des coefficients d'une série entière. Calculer cette série entière de deux façons différentes afin d'en déduire une formule sur les coefficients.
Il est parfois utile d'avoir établi une relation de récurrence sur les quantités qu'on cherche à évaluer. Mais voyons quelques exemples concrets dans la suite.

Exemple 31 : (Formule de Vandermonde) Grâce à $(1+x)^n(1+x)^m = (1+x)^{n+m}$, on en déduit que $\displaystyle\sum_{k=0}^{p} \binom{n}{k}\binom{m}{p-k} = \binom{n+m}{p}$.

Exemple 32 : (Nombres de Bell) Soit B_n le nombre de partitions de $[\![1, n]\!]$. On a $B_{n+1} = \displaystyle\sum_{k=0}^{n} \binom{n}{k} B_k$ avec $B_0 = 1$. En considérant $B(z) = \displaystyle\sum_{n=0}^{+\infty} \frac{B_n}{n!} z^n$, on en déduit que $B'(x) = B(x)\exp(x)$, d'où :

$$B_n = \frac{1}{e} \sum_{k=0}^{+\infty} \frac{k^n}{k!}$$

Exemple 33 : (Nombres de Catalan) On note C_n le nombre de mots binaires de longueur $2n$ qui contiennent autant de 0 que de 1, alors on a $C_n = \displaystyle\sum_{k=0}^{n-1} C_k C_{n-1-k}$. En

posant $C(z) = \sum_{n=0}^{+\infty} C_n z^n$, on trouve que $xC^2(x) - C(x) + 1 = 0$ et donc

$$C_n = \frac{1}{n+1}\binom{2n}{n}$$

Exemple 34 : (Partitions en parts fixées) Soit $\alpha_1, ..., \alpha_p$ des entiers premiers entre eux dans leur ensemble et S_n le nombre de solutions $(n_1, ..., n_p)$ entières de $n_1\alpha_1 + ... + n_p\alpha_p = n$. On note $S(z) = \sum_{n=0}^{+\infty} S_n z^n$, on trouve ensuite par exemple que

$$S_n \sim \frac{1}{\alpha_1 \dots \alpha_p} \frac{n^{p-1}}{(p-1)!}$$

Exemple 35 : (Partitions d'entiers) On pose $p(t) = \prod_{k=1}^{+\infty} \frac{1}{1-t^k}$. Si (p_n) est le nombre de partitions de l'entier n, alors on a $p(t) = 1 + \sum_{n\geqslant 1} p_n t^n$.

Une étude difficile de cette série entière permet d'obtenir des résultats non triviaux comme par exemple $p_n \sim \frac{1}{4n\sqrt{3}} e^{\pi\sqrt{\frac{2n}{3}}}$.

2 Utilisation en théorie des groupes

2.1 Actions de groupes et formule des classes

Théorème 36 (Lagrange). *Soit G un groupe fini, alors l'ordre de tout sous-groupe de G divise l'ordre de G.*

Définition 37. *On dit que G agit sur un ensemble X s'il existe un morphisme de groupes $\rho : G \longrightarrow \mathfrak{S}(X)$. On définit*

- *Si $x \in X$, le stabilisateur de x est $G_x = \{g \in G, g \cdot x\}$.*
- *Si $x \in X$, l'orbite de x est $G \cdot x = \{g \cdot x, g \in G\}$.*

Proposition 38. *Si G est fini, on a une bijection naturelle $G/G_x \longrightarrow G \cdot x$ pour n'importe quel x.*

Remarque 39 : En particulier, cette formule peut se révéler utile si l'action de G est transitive. Dans ce cas, on peut faire un choix astucieux de x pour obtenir des informations.

Corollaire 40 (Équations aux classes). *Si X et G sont finis et $\mathcal{X}$ est un système de représentants de X pour l'action de G, alors*

$$\mathrm{Card}(X) = \sum_{x\in\mathcal{X}} \frac{\mathrm{Card}(G)}{\mathrm{Card}(G_x)}$$

Application 41 : (Formule de Burnside) On note Fix_g l'ensemble des points de X fixes par g. Alors, on a

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

Application 42 : (Théorème de Cauchy) Soit G un groupe fini et p premier qui divise l'ordre de G, alors G admet un élément d'ordre p.

DEVELOPPEMENT 1

Lemme 43. *Soit $\varphi \in \mathrm{Aut}(\mathfrak{S}_n)$ qui envoie une transposition sur une transposition, alors φ est intérieur.*

Théorème 44. *Si $n \neq 6$, tous les automorphismes de $\mathfrak{S}_n$ sont intérieurs.*

Remarque 45 : Si $n = 6$, il existe un automorphisme qui n'est pas intérieur. Il suffit de trouver un sous-groupe de $\mathfrak{S}_6$ d'indice 6 qui n'est pas le stabilisateur d'un élément de $[\![1, 6]\!]$.

2.2 p-groupes

Définition 46. *Soit p un nombre premier, un p-groupe est un groupe dont l'ordre est une puissance de p.*

Proposition 47. *On note $X^G = \{x \in X, \forall g \in G, g \cdot x = x\}$. Alors, on a*

$$\mathrm{Card}(X) = \mathrm{Card}(X^G) \mod (p)$$

Corollaire 48. *Le centre d'un p-groupe est non trivial.*

Application 49 : Un groupe d'ordre p^2 est abélien.

2.3 Théorèmes de Sylow

Définition 50. *Soit G un groupe fini d'ordre $n = p^\alpha m$ avec $m \wedge p = 1$. Un p-sous-groupe de Sylow est un sous-groupe de G de cardinal p^α.*

Exemple 51 : Si $G = GL_n(\mathbb{F}_p)$, il est de cardinal $p^{\frac{n(n-1)}{2}} m$ et le sous-groupe des matrices unitriangulaires supérieures est un p-Sylow de G.

Lemme 52. *Soit G un groupe fini d'ordre $n = p^\alpha m$ avec $m \wedge p = 1$ et H un sous-groupe de G. Si S est un p-Sylow de G, alors il existe $a \in G$ tel que $aSa^{-1} \cap H$ est un p-Sylow de H.*

Théorème 53 (Sylow). *Soit G un groupe fini d'ordre $n = p^\alpha m$ avec $m \wedge p = 1$.*

1. *G admet au moins un p-Sylow.*
2. *Les p-Sylow sont conjugués.*
3. *Le nombre n_p de p-Sylow vérifie $n_p = 1 \mod (p)$.*

Application 54 : Un groupe d'ordre 63 ou 255 n'est pas simple.

3 Algèbre linéaire sur des corps finis

3.1 Groupes linéaires finis

Proposition 55. *Le centre de $GL_n(K)$ est l'ensemble des homothéties. Le centre de $SL_n(K)$ est l'ensemble des homothéties dont le rapport est une racine n-ième de l'unité dans K.*

Définition 56. *On définit les groupes projectifs (spécial) linéaire comme $GL_n(K)$ (resp. $SL_n(K)$) quotienté par leur centre.*

DEVELOPPEMENT 2

Proposition 57. *Les cardinaux des groupes linéaires sur $\mathbb{F}_q$ sont les suivants :*

1. $\mathrm{Card}\big(GL_n(\mathbb{F}_q)\big) = (q^n-1)(q^n-q)...(q^n-q^{n-1}) := g_n$.
2. $\mathrm{Card}\big(SL_n(\mathbb{F}_q)\big) = \mathrm{Card}\big(PGL_n(\mathbb{F}_q)\big) = \dfrac{g_n}{q-1}$.
3. $\mathrm{Card}\big(PSL_n(\mathbb{F}_q)\big) = \dfrac{g_n}{\mathrm{pgcd}(n,q-1)}$.

Lemme 58. *Le seul sous-groupe d'indice 2 de $\mathfrak{S}_n$ est $\mathfrak{A}_n$.*
On admettra dans la suite qu'un sous-groupe d'indice n de $\mathfrak{S}_n$ est isomorphe à $\mathfrak{S}_{n-1}$.

Théorème 59. *On a les isomorphismes exceptionnels suivants :*

1. $GL_2(\mathbb{F}_2) = SL_2(\mathbb{F}_2) = PSL_2(\mathbb{F}_2) \simeq \mathfrak{S}_3$.
2. $PGL_2(\mathbb{F}_3) \simeq \mathfrak{S}_4$ *et* $PSL_2(\mathbb{F}_2) \simeq \mathfrak{A}_4$.
3. $PGL_2(\mathbb{F}_4) = PSL_2(\mathbb{F}_4) \simeq \mathfrak{A}_5$.
4. $PGL_2(\mathbb{F}_5) \simeq \mathfrak{S}_5$ *et* $PSL_2(\mathbb{F}_5) \simeq \mathfrak{A}_5$.

Remarque 60 : Ainsi, $PGL_2(\mathbb{F}_5)$ montre que $\mathfrak{S}_6$ a un automorphisme non intérieur.

DEVELOPPEMENT 3

Théorème 61. *Soit $p \geqslant 3$ premier et $q = p^n$. Alors, $SO_2(\mathbb{F}_q)$ est cyclique, plus précisément, on a*

$$SO_2(\mathbb{F}_q) \simeq \begin{cases} \mathbb{Z}/(q-1)\mathbb{Z} & \text{si } -1 \text{ est un carré dans } \mathbb{F}_q^* \\ \mathbb{Z}/(q+1)\mathbb{Z} & \text{si } -1 \text{ n'est pas un carré dans } \mathbb{F}_q^* \end{cases}$$

Remarque 62 :

- Le groupe $O_2(\mathbb{F}_q)$ est isomorphe à un groupe diédral.
- Si $q = 2^n$, $O_2(\mathbb{F}_q) = SO_2(\mathbb{F}_q)$ est abélien et donc isomorphe à $(\mathbb{Z}/2\mathbb{Z})^n$.

3.2 Réduction

DEVELOPPEMENT 4

Lemme 63 (Décomposition de Fitting). *Soit $u \in \mathcal{L}(E)$, il existe un unique couple (F,G) de sous-espaces stables par u tels que*

1. $E = F \oplus G$.
2. $u_{|F}$ *est nilpotente.*
3. $u_{|G}$ *est inversible.*

Cela donne une bijection entre $\mathcal{L}(E)$ est l'ensemble des quadruplets (F,G,v,w) tels que $E = F \oplus G$, $v \in \mathcal{L}(F)$ nilpotent et $w \in GL(G)$.

Proposition 64. *Dans $M_n(\mathbb{F}_q)$, il y a $q^{n(n-1)}$ matrices nilpotentes.*

Lemme 65. *Soit $A \in M_n(\mathbb{F}_q)$, alors A est diagonalisable si, et seulement si, $A^q = A$.*

Application 66 : Le nombre de matrices diagonalisables de $M_n(\mathbb{F}_q)$ est

$$\sum_{n_1+\ldots+n_q=n} \frac{\mathrm{Card}\big(GL_n(\mathbb{F}_q)\big)}{\prod_{i=1}^{q} \mathrm{Card}\big(GL_{n_i}(\mathbb{F}_q)\big)}$$

Références :

- Caldero, Germoni, H2G2.
- Gourdon, Algèbre.
- Gourdon, Algèbre et probabilités.
- Perrin, Cours d'algèbre.