I Outils de dénombrement

1) Ensembles finis

Définition 1. On appelle cardinal d'un ensemble E, noté $\mathrm{Card}(E)$ ou $|E|$, la classe des ensembles en bijection avec E. On dit que E est fini s'il est en bijection avec un ensemble $[\![1,n]\!]$, où $n \in \mathbb{N}^\star$. On notera $|E| = n$.

Remarque 2. *On doit adjoindre à cette définition le cas de l'ensemble vide, par définition fini, et de cardinal 0.*

Proposition 3. *Soient E et F deux sous-ensembles finis d'un ensemble S. Alors $E \cap F$ est fini, et on a $|E \cup F| = |E| + |F| - |E \cap F|$.*

Proposition 4. *Soit $(E_i)_{i\in[\![1,n]\!]}$ une famille de sous-ensembles disjoints et finis d'un ensemble S. Alors $\left|\bigcup_{i=1}^n E_i\right| = \sum_{i=1}^n |E_i|$.*

Proposition 5 (Formule du crible)**.** *Soit $(E_i)_{i\in[\![1,n]\!]}$ une famille de sous-ensembles finis d'un ensemble S. Alors :*

$$\left|\bigcup_{i=1}^n E_i\right| = \sum_{i=1}^n \sum_{1\leqslant i_1<\ldots<i_n\leqslant n} (-1)^{k-1} |E_{i_1} \cap \ldots \cap E_{i_k}|$$

Théorème 6. *Le produit cartésien de p ensembles finis $A_1, \ldots, A_p$ est fini, et de cardinal $\prod_{i=1}^p |A_i|$.*

Théorème 7. *Soient E et F deux ensembles finis. L'ensemble des fonctions de E vers F est de cardinal $|F|^{|E|}$.*

Application 8. *On a $|\mathcal{P}(E)| = 2^{|E|}$.*

Proposition 9 (Lemme des bergers)**.** *Soient E et F deux ensembles finis et $\varphi : E \to F$ une surjection telle que $|\varphi^{-1}(x)| = n$ pour tout $x \in F$. Alors $|E| = n|F|$.*

Proposition 10 (Principe des tiroirs)**.** *Soit E un ensemble de partition $E_1, \ldots, E_n$. Soient $x_1, \ldots, x_k \in E$. Alors un E_i contient $\lceil \frac{k}{n} \rceil$ éléments x_j.*

2) Arrangements et permutations

Soient E un ensemble de cardinal $n \in \mathbb{N}^\star$ et $p \leqslant n$.

Définition 11. Un p-arrangement de E est une injection $[\![1,p]\!] \hookrightarrow E$.

Théorème 12. *Le nombre de p-arrangement de E est $A_n^p = \frac{p!}{(n-p)!}$.*

Définition 13. Une permutation est un n-arrangement.

Application 14. *Comme E est fini, toute permutation est une bijection. Par composition, on peut associer toute permutation à une unique bijection $E \to E$, donc $|\mathfrak{S}(E)| = A_n^n = n!$*

3) Combinaisons

Soient E un ensemble de cardinal $n \in \mathbb{N}^\star$ et $p \leqslant n$.

Définition 15. Une p-combinaison de E est une partie de E à p éléments.

Proposition 16. *Le nombre de p-combinaisons de E est $\binom{n}{p} = \frac{n!}{p!(n-p)!}$.*

Proposition 17. *Pour $n \geqslant 1$ et $1 \leqslant p \leqslant n$, on a :*

- $\binom{n}{n-p} = \binom{n}{p}$
- $\binom{n-1}{p} + \binom{n-1}{p-1} = \binom{n}{p}$ *(Formule de Pascal)*
- $\binom{n}{p} = \frac{n}{p}\binom{n-1}{p-1} = \frac{n}{n-p}\binom{n-1}{p} = \frac{n-p+1}{p}\binom{n}{p-1}$

Proposition 18 (Binôme de Newton)**.** *Soient $a, b \in \mathbb{C}$ et $n \in \mathbb{N}$. Alors :*

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

Corollaire 19. *On retrouve de cardinal de $\mathcal{P}(E)$: $\sum_{k=0}^n \binom{n}{k} = 2^n$.*

Application 20. *Si $S_{n,k} = \sum_{\ell=1}^n \ell^k$, on a $1 + \sum_{k=0}^{p-1} \binom{p}{n} S_{n,k} = (n+1)^p$. On retrouve ainsi en particulier :*

$$S_{n,1} = \sum_{k=1}^n k = \frac{n(n+1)}{2} \quad \text{et} \quad S_{n,2} = \sum_{k=1}^n k^2 = \frac{n(n+1)(2n+1)}{6}$$

Application 21. *Le nombre σ_p^n de surjections d'un ensemble à n éléments dans un ensemble à p éléments est :*

$$\sigma_p^n = \sum_{k=0}^p (-1)^{p-k} \binom{p}{k} k^n$$

Application 22. *Le nombre d_n de dérangements (permutations sans point fixe) d'un ensemble à n éléments est :*

$$d_n = n! \sum_{k=0}^p \frac{(-1)^k}{k!}$$

II Dénombrement en algèbre

1) Théorie des groupes

Soit G un groupe et H un sous-groupe de G.

Définition 23. La classe à gauche de $g \in G$ est $gH = \{gh \,|\, h \in H\}$.

Proposition 24. *Pour tout $g \in G$, on a $|gH| = |H|$.*

Définition 25. L'indice $[G : H]$ de H dans G est le cardinal de G/H.

Théorème 26. *On a $|G| = |H| \times [G : H]$.*

Théorème 27 (Lagrange)**.** *Pour tout sous-groupe H de G, on a $|H| \mid |G|$.*

Application 28. *Tout groupe d'ordre premier est cyclique.*

Définition 29. Supposons que G opère sur X. Soient $x \in X$ et $g \in G$.

(i) L'orbite de x est : $O_x = \{g \cdot x \,|\, g \in G\}$.

(ii) Le stabilisateur de x est : $\mathrm{Stab}_x = \{g \in G \,|\, g \cdot x = x\}$.

(iii) Le fixateur de g est : $\mathrm{Fix}_g = \{x \in X \,|\, g \cdot x = x\}$.

Proposition 30. *Si G est fini, alors pour tout $x \in X$, $|G| = |\mathrm{Stab}_x||O_x|$.*

Théorème 31 (Équation aux classes)**.** *On suppose X et G finis. Soit θ une partie X contenant un unique représentant de chaque orbite. Alors :*

$$|X| = \sum_{x \in \theta} |O_x| = \sum_{x \in \theta} \frac{|G|}{|\,\mathrm{Stab}_x\,|}$$

Théorème 32 (Burnside)**.** *On suppose G et X finis. Soit Ω l'ensemble des orbites distinctes. Alors :*

$$|\Omega| = \frac{1}{|G|} \sum_{g \in G} |\,\mathrm{Fix}_g\,|$$

Application 33. *Le nombre de colliers de 5 perles différents que l'on peut réaliser avec deux couleurs est 8.*

2) Fonctions multiplicatives

Définition 34. On appelle indicatrice d'Euler de $n \geqslant 1$ l'entier :

$$\varphi(n) = \mathrm{Card}\left(\{k \in [\![1, n]\!] \,|\, k \wedge n = 1\}\right)$$

Corollaire 35. *Si $m \wedge n = 1$, alors $\varphi(mn) = \varphi(m)\varphi(n)$.*

Exemple 36. *Soient p premier, alors $\varphi(p) = p-1$ et $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$.*

Proposition 37. *(i) Pour $d|n$, $\mathbb{Z}/n\mathbb{Z}$ admet $\varphi(d)$ éléments d'ordre d.*
(ii) (Formule de Möbius) $n = \sum_{d|n} \varphi(n)$

Proposition 38. *Si on note μ_n l'ensemble des racines primitives n-ièmes de l'unité dans $\mathbb{C}$, on a $|\mu_n| = \varphi(n)$.*

Corollaire 39. *Le n-ième polynôme cyclotomique est de degré $\varphi(n)$.*

Définition 40. La fonction de Möbius $\mu : \mathbb{N}^\star \to \{0, 1, -1\}$ se définit par :

$$\mu(n) = \begin{cases} 1 & \text{si } n = 1 \\ (-1)^r & \text{si } n \text{ est sans facteur carré} \\ 0 & \text{sinon} \end{cases}$$

Proposition 41. *La fonction de Möbius est multiplicative sur $\mathbb{N}^\star$.*

Proposition 42. $\sum_{d|n} \mu(d) = 0$

Théorème 43. *Soient p premier, $\alpha, n \in \mathbb{N}^\star$ et $q = p^\alpha$. On note $\mathcal{P}_q(d)$ l'ensemble des polynômes unitaires irréductibles de degré d sur $\mathbb{F}_q$. Alors :*

$$X^{q^n} - X = \prod_{d|n} \prod_{P \in \mathcal{P}_q(d)} P(X)$$

Proposition 44 (Inversion de Möbius)**.** *On note μ la fonction de Möbius. Soit $g : \mathbb{N}^\star \to \mathbb{C}$. On pose $G(n) = \sum_{d|n} g(d)$. Alors :*

$$\forall\, n \in \mathbb{N}^\star,\ g(n) = \sum_{d|n} \mu(d) G\left(\frac{n}{d}\right)$$

Corollaire 45. *Si $I(q, d)$ désigne le cardinal de $\mathcal{P}_p(d)$, alors, pour tout $n \in \mathbb{N}^\star$, on a :*

$$I(q, n) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d \underset{+\infty}{\sim} \frac{q^n}{n}$$

III Dénombrement en analyse

1) Utilisation en probabilités

Soit Ω un ensemble fini. On considère l'espace probabilisé $(\Omega, \mathcal{P}(\Omega), \mathbb{P})$, où $\mathbb{P}$ est la loi uniforme sur Ω. Pour une partie A de Ω, on a alors $\mathbb{P}(A) = \frac{|A|}{|\Omega|}$. Ainsi, savoir dénombrer des ensembles permet de calculer des probabilités.

Exemple 46. *Dans un tirage avec remise, il y a n^p issues possibles.*

Exemple 47. *Dans un tirage sans remise, il y a A_n^p issues possibles.*

Exemple 48. *Une course de 20 chevaux a 1140 tiercés dans le désordre.*

Exemple 49. *Soit $n \leqslant 365$. En ne considérant pas les années bissextiles, la probabilité que deux personnes parmi n aient la même date d'anniversaire est $p_n = 1 - \frac{365!}{365^n \times (365-n)!}$.*

2) Séries génératrices

Définition 50. Soit $(u_n)_{n\in\mathbb{N}}$ une suite complexe. On définit sa série génératrice par $S(z) = \sum_{n\in\mathbb{N}} u_n z^n$.

Exemple 51. *La suite constante égale à 1 a pour série génératrice $S(z) = \frac{1}{1-z}$.*

Application 52 (Nombres de Catalan)**.** *On note C_n le nombre de parenthésages possibles d'un produit de $n+1$ facteurs. On a alors la relation $C_n = \sum_{k=1}^{n-1} C_k C_{n-k}$, et on obtient $C_n = \frac{1}{n+1}\binom{2n}{n}$.*

Application 53 (Nombres de Bell)**.** *Pour $n \in \mathbb{N}^\star$, on pose B_n le nombre de partitions de l'ensemble $[\![1, n]\!]$ avec la convention $B_0 = 1$, alors :*

$$\forall\, k \in \mathbb{N},\ B_k = \frac{1}{e} \sum_{n\geqslant 0} \frac{n^k}{n}$$

Développements

- Polynômes irréductibles unitaires sur $\mathbb{F}_q$ (43,44,45) [Tau08]
- Nombres de Bell (53) [FGN13a]

Références

[dB04] J. de Biasi. *Mathématiques pour le CAPES et l'agrégation interne.* Ellipses
[Per96] D. Perrin. *Cours d'Algèbre.* Ellipses
[FGN13a] S. Francinou, H. Gianella, et S. Nicolas. *Oraux X-ENS Algèbre 1.* Cassini
[Tau08] P. Tauvel. *Corps commutatifs et théorie de Galois.* Calvage et Mounet