190. Méthodes combinatoires, problèmes de dénombrement.

1 Généralités

1.1 Ensembles finis

Définition 1. Soit E un ensemble. On dit qu'il est fini de cardinal $p \in \mathbb{N}$ s'il est vide (auquel cas $p = 0$) ou s'il est en bijection avec $[\![1, p]\!]$. On note alors $p = \mathrm{Card}(E)$ ou $p = |E|$.

Proposition 2. Soient A, B deux ensembles finis. Alors $A \cup B, A \cap B$ sont finis et $\mathrm{Card}(A \cup B) = \mathrm{Card}(A) + \mathrm{Card}(B) - \mathrm{Card}(A \cap B)$.

Proposition 3 (Formule du crible)**.** Soient $E_1, \cdots, E_n$ des ensembles finis. Alors $\mathrm{Card}\left(\bigcup_{i=1}^{n} E_i\right) = \sum_{1 \le i \le n} \mathrm{Card}(E_i) - \sum_{1 \le i,j \le n} \mathrm{Card}(E_i \cap E_j) + \cdots + (-1)^n \mathrm{Card}\left(\bigcap_{i=1}^{n} E_i\right)$.

Proposition 4. Soient $A_1, \cdots, A_n$ des ensembles finis. Alors $A_1 \times \cdots \times A_n$ est fini, et $\mathrm{Card}(A_1 \times \cdots \times A_n) = \prod_{i=1}^{n} \mathrm{Card}(A_i)$.

Proposition 5. Soient A, B finis. Alors A^B est fini et $\mathrm{Card}(A^B) = \mathrm{Card}(A)^{\mathrm{Card}(B)}$.

Corollaire 6. Si A est fini, alors $\mathcal{P}(A)$ est fini et $\mathrm{Card}(\mathcal{P}(A)) = 2^{\mathrm{Card}(A)}$.

***Application* 7.** *Il y a 684 nombres à trois chiffres qui contiennent au moins l'un des chiffres 0, 3, 6 ou 9.*

***Application* 8.** *L'alphabet Braille contient 64 configurations différentes.*

1.2 Arrangements, permutations, combinaisons

Définition 9. Soient E un ensemble de cardinal n, $p \le n$ un entier naturel. On appelle arrangement p à p de E un p-uplet d'éléments distincts de E.

Proposition 10. Le nombre d'arrangements p à p distincts de E est $A_n^p = \dfrac{n!}{(n-p)!}$.

***Application* 11.** *Cela correspond au nombre de tirages possibles de p boules dans une urne contenant n boules, sans remise.*

Définition 12. On appelle permutation de E tout arrangement n à n de E.

Proposition 13. Il y a $n!$ permutations de E.

Définition 14. On appelle combinaison à p éléments de E toute partie de E de cardinal p. On note $\binom{n}{p}$ le nombre de combinaisons à p éléments de E.

Théorème 15. On a $\binom{n}{p} = \frac{n!}{p!(n-p)!}$.

***Application* 16.** *Dans une course de 20 chevaux, il y a 1140 tiercés dans le désordre et 6840 tiercés dans l'ordre.*

Proposition 17. On a aussi $\binom{n}{p} = \binom{n}{n-p}, \binom{n}{p} = \frac{n}{p}\binom{n-1}{p-1}$.

Proposition 18 (Pascal)**.** On a $\binom{n}{p} = \binom{n-1}{p-1} + \binom{n-1}{p}$.

Théorème 19 (Binôme de Newton)**.** Si A anneau et si $a, b \in A$ commutent, alors $\forall n \in \mathbb{N}, (a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$.

***Application* 20.** *La somme de deux éléments nilpotents d'un anneau commutatif est nilpotente.*

1.3 Autres principes de dénombrement

Proposition 21 (Lemme des bergers)**.** Soient A, B ensembles finis, $\varphi : A \to B, n \in \mathbb{N}$. Si pour tout $x \in B, \mathrm{Card}(\varphi^{-1}(x)) = n$ alors $\mathrm{Card}(A) = n\mathrm{Card}(B)$.

***Application* 22.** *Pour $p \ge 3, q = p^n$, il y a $\frac{q+1}{2}$ carrés dans $\mathbb{F}_q$.*

Proposition 23 (Principe des tiroirs)**.** Si $k > n$ et $\varphi : [\![1, k]\!] \to [\![1, n]\!]$, alors il existe $j \in [\![1, n]\!]$ ayant au moins deux antécédents par φ.

***Application* 24.** *La série $\sum_{n \ge 1} \dfrac{1}{n^2 \sin(n)^2}$ diverge.*

2 Méthodes combinatoires en théorie des groupes

2.1 Premiers résultats

Proposition 25. Soient G un groupe fini, H un sous-groupe de G. On définit une relation d'équivalence par $g \mathcal{R} g' \Leftrightarrow g^{-1}g' \in H$. Les classes d'équivalence sont les $gH, g \in G$. Elles sont toutes en bijection avec H.

Définition 26. On note G/H l'ensemble des classes d'équivalence.

Théorème 27 (Lagrange)**.** On a $|G| = |H| \cdot |G/H|$.

***Application* 28.** *L'ordre de tout élément de G divise $|G|$. Tout groupe d'ordre premier est cyclique.*

2.2 Actions de groupes

Soit $(G, \cdot)$ un groupe, soit X un ensemble.

Définition 29. On dit que G agit sur X (à gauche) s'il existe une application $\begin{cases} G \times X \to X \\ (g, x) \mapsto g \cdot x \end{cases}$ telle que :

(i). $\forall g, g' \in G, \forall x \in X, g \cdot (g' \cdot x) = (gg') \cdot x$

(ii). $\forall x \in X, e_G \cdot x = x$.

***Exemple* 30.** *Un groupe agit sur lui-même par :*
- *Translation à gauche : $g \cdot h = gh$.*
- *Translation à droite : $g \cdot h = hg^{-1}$.*
- *Conjugaison : $g \cdot h = ghg^{-1}$.*

Définition 31. On considère une action de G sur X.
- Soit $x \in X$, on appelle orbite de x l'ensemble $Gx = \{g \cdot x, g \in G\}$. On appelle stabilisateur de x l'ensemble $\mathrm{Stab}(x) = \{g \in G, g \cdot x = x\}$.
- L'action est dite transitive si elle ne possède qu'une seule orbite.

Théorème 32 (Formule des classes)**.** Soit G groupe fini qui agit sur un ensemble fini X. On a, pour tout $x \in X, |G| = |Gx| \cdot |\mathrm{Stab}(x)|$. Ainsi, si Ω partie de X qui rencontre chaque orbite en un seul point, $|X| = \sum_{x \in \Omega} \frac{|G|}{|\mathrm{Stab}(x)|}$.

***Application* 33** (Lemme de Cauchy)**.** *Si p est un nombre premier, un p-groupe possède un élément d'ordre p.*

***Application* 34** (Loi de réciprocité quadratique)**.** *Soient $p, q \geq 3$ des nombres premiers. On a $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.*

Définition 35. Si G agit sur X, pour $g \in G$, on appelle fixateur de g l'ensemble $\mathrm{Fix}(g) = \{x \in X, g \cdot x = x\}$.

Théorème 36 (Formule de Burnside)**.** Si G, X sont finis, le nombre d'orbites de l'action de G sur X est donné par $N = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)|$.

***Application* 37.** *On peut réaliser 76 colliers différents avec 4 perles rouges, 3 perles noires et 2 perles bleues.*

***Application* 38** (Fermat)**.** *Pour tous $a \in \mathbb{N}^*, p$ premier, on a $a^p \equiv a \mod p$.*

Définition 39. Soit p nombre premier, soit G un groupe d'ordre multiple de p. On appelle p-Sylow de G tout sous-groupe de G d'ordre égal à $\max\{k \in \mathbb{N}, p^k \mid |G|\}$.

Théorème 40 (Théorèmes de Sylow)**.** Soit G groupe d'ordre $p^k m$, p premier, $m \nmid p$.

(i). G possède un p-Sylow.

(ii). Tous les p-Sylow de G sont conjugués.

(iii). Si on note c_p le nombre de p-Sylow de G, on a $c_p \mid m$ et $c_p \equiv 1 \ [p]$.

***Application* 41.** *Il n'existe pas de groupe simple à 30 ou 42 éléments.*

3 Fonction indicatrice d'Euler

Définition 42. Pour tout $n \in \mathbb{N}^*$, on définit l'indicatrice d'Euler par $\varphi(n) = \mathrm{Card}((\mathbb{Z}/n\mathbb{Z})^\times)$.

Proposition 43. $\varphi(n)$ est aussi le nombre de générateurs du groupe $\mathbb{Z}/n\mathbb{Z}$, ainsi que le nombre d'entiers dans $[\![1, n]\!]$ premiers avec n.

Proposition 44. On a $\varphi(n) = \sum_{d|n} \varphi(d)$.

***Application* 45.** *Si K est un corps fini, K^* est cyclique.*

Proposition 46. φ est multiplicative : $\forall m, n \in \mathbb{N}^*, m \wedge n = 1 \Rightarrow \varphi(mn) = \varphi(m)\varphi(n)$.

Proposition 47. Si p premier, $\alpha \in \mathbb{N}^*, \varphi(p^\alpha = p^{\alpha-1}(p-1)$. Ainsi, si $n \in \mathbb{N}^*$ a pour décomposition en nombres premiers $n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$, on a $\varphi(n) = n \prod_{i=1}^{s} \left(1 - \frac{1}{p_i}\right)$.

4 Séries génératrices

Définition 48. Soit $(a_n)_{n \in \mathbb{N}} \in \mathbb{Z}^{\mathbb{N}}$. On appelle série génératrice de cette suite la série formelle $\sum_{n \in \mathbb{N}} a_n X^n$.

Remarque 49. On peut également considérer la série entière associée.

***Application* 50** (Rendu de monnaie)**.** *Soient $a_1, \cdots, a_k \in \mathbb{N}$ premiers entre eux dans leur ensemble. Pour $n \geq 1$, on note $u_n = \#\{(x_1, \cdots, x_k) \in \mathbb{N}^k, a_1 x_1 + \cdots + a_k x_k = n\}$. Alors $u_n \underset{n \to +\infty}{\sim} \frac{1}{a_1 a_2 \cdots a_k} \frac{n^{k-1}}{(k-1)!}$.*

***Application* 51** (Nombres de Catalan)**.** *Pour $n \in \mathbb{N}^*$, on considère un mot de n caractères et on note a_n le nombre de parenthésages possibles. On a, pour tout $n \in \mathbb{N}^*, a_{n+1} = \sum_{k=1}^{n} a_k a_{n-k}$. La série génératrice, vue comme série entière, a un rayon de convergence égal à $\frac{1}{4}$ et vaut, pour $t > 0, \frac{1}{2}(1 - \sqrt{1-4t})$. On en déduit $a_n = \frac{1}{n}\binom{2n-2}{n-1}$.*

Développements

— Loi de réciprocité quadratique.
— Problème du rendu de monnaie.

Références

[1] F. Combes, Algèbre et géométrie, Bréal.

[2] J. Delcourt, Théorie des groupes, Dunod.

[3] J. De Biasi, Mathématiques pour le CAPES et l'agrégation interne, Ellipses.

[4] I. Nourdin, Agrégation de mathématiques - Épreuve orale, Dunod.

[5] D. Perrin, Cours d'algèbre, Ellipses.