190 Méthodes combinatoires, problèmes de dénombrement.

Sauf mention contraire, les lettres capitales E, F, G... désigneront des ensembles *finis*. Le *cardinal* de E est noté $|E|$.

1 Outils de base, cardinaux usuels

1.1 Principes fondamentaux

Principe 1 (de récurrence)**.** Soit $\mathcal{H}(n)$ une proposition dépendant de l'entier $n \in \mathbf{N}$. Si les propositions $\mathcal{H}(0)$ et $\forall n \in \mathbf{N},\ \mathcal{H}(n) \implies \mathcal{H}(n+1)$ sont vraies alors $\mathcal{H}(n)$ est vraie pour tout $n \in \mathbf{N}$.

Exemple 2. $1+2+\cdots+n = \frac{n(n+1)}{2}$ et $1+q+\cdots+q^n = \frac{1-q^{n+1}}{1-q}$ pour tous $n \in \mathbf{N}^*$ et $q \neq 1$.

Principe 3 (d'égalité)**.** (Il existe $f\colon E \to F$ bijective) $\iff |E| = |F|$.

Remarque 4. Toute partie stricte de E est finie, de cardinal $< |E|$. Un ensemble fini ne peut pas être mis en bijection avec une partie stricte.

Exemple 5. Pour tout $n \in \mathbf{N}^*$, $|\mathfrak{A}_n| = |\mathfrak{S}_n \setminus \mathfrak{A}_n|$.

Exemple 6. Une *partition* de l'entier $n \in \mathbf{N}^*$ est une suite finie décroissante d'entiers (appelés *parts*) $(n_i)_{1\leqslant i\leqslant k} \in (\mathbf{N}^*)^k$ de somme n. Par exemple $9 = 4+2+2+1$. Le nombre de partitions de n en parts impaires est égal au nombre de partitions de n en parts distinctes.

Principe 7 (d'inclusion)**.** Si $E \cap F = \varnothing$ alors $|E \cup F| = |E| + |F|$.

Principe 8 (d'exclusion)**.** Si $F \subset E$ alors $|E \setminus F| = |E| - |F|$.

Principe 9 (d'inclusion–exclusion, formule du crible)**.**
$|E_1 \cup E_2| = |E_1| + |E_2| - |E_1 \cap E_2|$, et plus généralement

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

Principe 10 (de multiplication)**.** $|E \times F| = |E| \times |F|$ et $|F^E| = |F|^{|E|}$.

Exemple 11. L'ensemble $\mathcal{P}(E)$ des parties de E est fini : $|\mathcal{P}(E)| = 2^{|E|}$.

Principe 12 (des bergers)**.** Soit $f\colon E \to F$ surjective telle que F est fini et tout élément $y \in F$ admet un nombre constant $r \in \mathbf{N}$ d'antécédents par f. Alors E est fini, et $|E| = r|F|$.

Exemple 13. Soit p premier. Le nombre de carrés dans $\mathbf{F}_p$ est $\frac{p+1}{2}$.

Définition 14. Soit $n \coloneqq |E|$. Un *k-arrangement* de E est un k-uplet $(x_1, \ldots, x_k)$ d'éléments de E deux à deux distincts. L'ensemble $\mathcal{A}^k(E)$ des k-arrangements de E est fini et $|\mathcal{A}^k(E)| = n(n-1)\cdots(n-k+1)$, noté A_n^k. C'est aussi le nombre d'injections de E vers un ensemble à k éléments. En particulier $|\mathfrak{S}(E)| = |\mathfrak{S}_n| = A_n^n = n!$.

Définition 15. Soit $n \coloneqq |E|$. L'ensemble $\mathcal{P}_k(E)$ des parties de E à k éléments est fini et $|\mathcal{P}_k(E)| = \frac{n(n-1)\cdots(n-k+1)}{k!} =: \binom{n}{k}$ (lu « k parmi n »).

Exemple 16. Il y avait $\binom{41}{2} = 820$ paires de leçons d'algèbre en 2013.

Formule 17 (Triangle de Pascal)**.** $\forall (k,n) \in \mathbf{N}^2,\ \binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}$.

Principe 18 (de double décompte)**.** Soit $S \subset E \times F$. Avec pour $x \in E$, $F_x \coloneqq \{y \in F \mid (x,y) \in S\}$ et pour $y \in F$, $E_y \coloneqq \{x \in E \mid (x,y) \in S\}$,

$$|S| = \sum_{x\in E} |F_x| = \sum_{y\in F} |E_y|.$$

Exemple 19. En notant $d(x)$ le degré du sommet x dans le graphe non orienté $G = (V, E)$, alors $2|E| = \sum_{x\in V} d(x)$.

Principe 20 (des tiroirs de Dirichlet)**.** Si $f\colon E \to F$ avec $|F| < |E|$, alors f n'est pas injective.

Exemple 21. Parmi $n+1$ nombres dans $\{1, \ldots, 2n\}$, au moins deux sont premiers entre eux, et au moins deux sont tels que l'un divise l'autre.

Exemple 22 ([FGN, 2.15 p. 79])**.** Soit $\alpha \in \mathbf{R} \setminus \mathbf{Q}$. Il existe une infinité de couples $(p,q) \in \mathbf{Z} \times \mathbf{N}^*$ tels que $|\alpha - \frac{p}{q}| < \frac{1}{q^2}$.

1.2 Quelques résultats combinatoires en algèbre

Formules 23 (du binôme, du multinôme)**.** Soient A un anneau et $n \in \mathbf{N}$. Si $x, y \in A$ commutent, alors $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$. Plus généralement si $x_1, \dots, x_p \in A$ commutent deux à deux, alors

$$(x_1 + \cdots + x_p)^n = \sum_{\substack{k_1,\dots,k_p \in \mathbf{N} \\ k_1+\cdots+k_p=n}} \frac{n!}{k_1! \cdots k_p!} x_1^{k_1} \cdots x_p^{k_p}.$$

Formule 24 (d'inversion de Pascal)**.** Soient A un anneau commutatif et $x_0, \dots, x_n, y_0, \dots, y_n$ dans A tels que $y_k = \sum_{i=0}^{k} \binom{k}{i} x_i$ pour tout $0 \leqslant k \leqslant n$. Alors $x_k = \sum_{i=0}^{k} (-1)^{k-i} \binom{k}{i} y_i$ pour tout $0 \leqslant k \leqslant n$.

Proposition 25. Soient G un groupe fini agissant sur E et Ω un système de représentants des orbites sous cette action.

(i) *Formule des classes.* $|E| = \sum_{x \in \Omega} \frac{|G|}{|\mathrm{Stab}(x)|}$.

(ii) *Formule de Burnside.* Avec $E^g \coloneqq \{x \in E \mid g \cdot x = x\}$ pour $g \in G$,

$$|\Omega| = \frac{1}{|G|} \sum_{g \in G} |E^g|.$$

Exemple 26. Il y a 57 dés cubiques de faces rouges, jaunes ou bleues.

Théorème 27 ($3^{\text{ème}}$ théorème de Sylow)**.** Soient G un groupe fini d'ordre $n \coloneqq p^\alpha m$ où p est un diviseur premier de n ne divisant pas m. Le nombre n_p de p-Sylow de G vérifie $n_p \equiv 1\ [p]$ et $n_p \mid m$.

Théorème 28 (de Cauchy)**.** Soient G un groupe fini et p un diviseur premier de $|G|$. Le nombre de $g \in G$ tels que $g^p = 1$ est divisible par p.

Définition 29. On note $\varphi(n)$ le nombre d'entiers $0 \leqslant k < n$ premiers avec $n \in \mathbf{N}^*$. φ est appelée *fonction indicatrice d'Euler*.

Proposition 30. Tout groupe cyclique d'ordre n possède $\varphi(n)$ générateurs, et pour tout diviseur d de n, un unique sous-groupe d'ordre d, qui est également cyclique.

Proposition 31. $\forall n \in \mathbf{N}^*,\ n = \sum_{d \mid n} \varphi(d)$ et $\varphi(n) = n \prod_{\substack{p \in \mathbf{P} \\ p \mid n}} (1 - \frac{1}{p})$.

Proposition 32. Soit A un anneau intègre. Tout polynôme $P \in A[X]$ de degré $n \in \mathbf{N}$ admet au plus n racines dans A.

Proposition 33. Soit G un sous-groupe fini du groupe des inversibles d'un corps (commutatif). Alors G est cyclique.

Proposition 34. Soient $p \in \mathbf{P}$, $n \in \mathbf{N}^*$ et $m = \lfloor \log_p(n) \rfloor$. La valuation p-adique de $n!$ est $\nu_p(n!) = \sum_{k=0}^{m} \lfloor \frac{n}{p^k} \rfloor$.

2 Utilisation des séries génératrices [FS]

Définition 35. Une *classe combinatoire* est un ensemble $\mathcal{C}$ muni d'une *fonction de taille* $|\cdot| \colon \mathcal{C} \to \mathbf{N}$ telle que pour tout $n \in \mathbf{N}$, l'ensemble $\mathcal{C}_n \coloneqq \{c \in \mathcal{C} \mid |c| = n\}$ est fini, de cardinal noté C_n.

Définition 36. La série génératrice (ordinaire) de $\mathcal{C}$ est la série formelle notée $C(X)$ (lettre droite) et définie par

$$C(X) \coloneqq \sum_{c \in \mathcal{C}} X^{|c|} = \sum_{n=0}^{+\infty} C_n X^n.$$

Exemple 37. $\mathcal{N} \coloneqq \mathbf{N}$ (avec $|n| = n$ pour tout $n \in \mathbf{N}$) a pour série génératrice $N(X) = \sum_{k=1}^{+\infty} X^k = \frac{1}{1-X}$.

Proposition 38 (Constructions admissibles)**.** Soient $\mathcal{A}, \mathcal{B}$ deux classes combinatoires. Sont encore des classes combinatoires :

1. la *somme disjointe* notée $\mathcal{A} + \mathcal{B}$ (avec $|x| = |x|$ pour $x \in \mathcal{A} \cup B$), de série génératrice $A(X) + B(X)$,
2. le *produit cartésien* $\mathcal{A} \times \mathcal{B}$ (avec $|(a,b)| = |a| + |b|$ pour $(a,b) \in \mathcal{A} \times \mathcal{B}$), de série génératrice $A(X)B(X)$,
3. la *séquence* $\mathsf{Seq}(\mathcal{A}) \coloneqq \sum_{k=0}^{+\infty} \mathcal{A}^k$ (à condition que $\mathcal{A}_0 = \varnothing$, et avec $|(a_1, \dots, a_n)| = \sum_{k=1}^{n} |a_k|$ pour tous $n \in \mathbf{N}, (a_1, \dots, a_n) \in \mathcal{A}^n$), de série génératrice $\frac{1}{1-A(X)}$.

Exemple 39. L'ensemble des arbres binaires $\mathcal{T}$ est défini récursivement par $\mathcal{T} = \mathcal{E} + \mathcal{R} \times \mathcal{T}^2$ où l'arbre vide $\mathcal{E}$ a taille 0 ($E(X) = 1$) et l'arbre-racine $\mathcal{R}$ a taille 1 ($R(X) = X$). D'où $T(X) = 1 + XT(X)^2$.

Exemple 40. Les partitions d'entiers sont l'ensemble $\mathcal{P}$ des suites $p = (\ell_i) \in \mathbf{N}^{(\mathbf{N}^*)}$ donnant pour tout $i \in \mathbf{N}^*$, le nombre $\ell_i \in \mathbf{N}$ de parts égales à i : $|p| = \sum_{i \in \mathbf{N}^*} i\ell_i$. Ainsi $\mathcal{P} = \prod_{k=1}^{+\infty} \mathcal{B}^k$ où $\mathcal{B}$ est un « bâton » de taille 1 ($B(X) = X$), et $P(X) = \prod_{k=1}^{+\infty} \frac{1}{(1-X)^k}$. Le nombre de partitions de $n \in \mathbf{N}^*$ est le coefficient en X^n de $P(X)$.

Question 41. À chaque seconde, un singe appuie au hasard sur une touche du clavier. Combien de temps se passera-t-il en moyenne pour que le mot ABRACADABRA apparaisse à l'écran ? DÉV. 1

Formule 42 (d'inversion de Lagrange)**.** Soit $y = \sum_{n=1}^{+\infty} y_n X^n \in \mathbf{C}[[X]]$ satisfaisant $y = X\phi(y)$ avec $\phi \in \mathbf{C}[[X]]$ tel que $\phi(0) \neq 0$. Alors

$$\forall n \in \mathbf{N}^*,\ y_n = \frac{1}{n}\,[X^{n-1}]\phi(X)^n.$$

Exemple 43. En reprenant l'exemple 39, avec $S(X) \coloneqq T(X) - 1$, S satisfait $S = X\phi(S)$ où $\phi(X) = (1+X)^2$, donc le nombre T_n d'arbres binaires à $n \geqslant 1$ nœuds est

$$T_n = [X^n]S(X) = \frac{1}{n}\,[X^{n-1}](1+X)^{2n} = \frac{1}{n}\binom{2n}{n-1} = \frac{1}{n+1}\binom{2n}{n}$$

(ce nombre est appelé *n-ième nombre de Catalan*).

Question 44. Soient F un ensemble fini et $(X_n)_{n \in \mathbf{N}^*}$ une suite de v.a. i.i.d. selon $\mathcal{U}(F)$. À partir de quelle valeur de $n \in \mathbf{N}^*$, en moyenne,

1. $(X_1, \ldots, X_n)$ contient deux éléments identiques ? DÉV. 2
2. $(X_1, \ldots, X_n)$ contient une occurrence de chaque élément de F ?

3 Autres exemples de dénombrements

Exemple 45 (dérangements)**.** Le nombre d'éléments de $\mathfrak{S}_n$ sans point fixe est $n! \sum_{k=0}^{n} \frac{(-1)^k}{k!} \underset{n \to +\infty}{\sim} n!e^{-1}$.

Exemple 46. Le nombre de surjections d'un ensemble à n élements sur un ensemble à $0 \leqslant r \leqslant p$ éléments est $\sum_{k=0}^{r} (-1)^{r-k} \binom{r}{k} k^n$.

Dénombrements dans les corps finis

Soient K un corps fini de cardinal q.

Proposition 47. Le nombre de carrés dans K est $\frac{q+1}{2}$.

Proposition 48. $(q-1)|\mathsf{SL}_n(K)| = |\mathsf{GL}_n(K)| = \prod_{i=0}^{n-1}(q^n - q^i)$.

Définition 49. La *fonction de Möbius* μ est définie, pour $n \in \mathbf{N}^*$ et k le nombre de facteurs premiers de n, par

$$\mu(n) = \begin{cases} 0 & \text{si } n \text{ a un facteur carré,} \\ (-1)^k & \text{sinon.} \end{cases}$$

Formule 50 (d'inversion de Möbius)**.** Soient $f, g \colon \mathbf{N}^* \to \mathbf{C}$. Alors $\forall n \in \mathbf{N}^*, g(n) = \sum_{d|n} f(d) \Leftrightarrow \forall n \in \mathbf{N}^*, f(n) = \sum_{d|n} \mu(d) g(n/d)$. [FG, p. 93]

Proposition 51 ([FG, p. 190])**.** Le nombre $I(n,q)$ de polynômes unitaires irréductibles de degré n à coefficients dans K est

$$I(n,q) \coloneqq \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d} \underset{n \to +\infty}{\sim} \frac{q^n}{n}.$$

Proposition 52 ([Tos])**.** Soit $\mathfrak{N}(K^n)$ l'ensemble des endomorphismes nilpotents de K^n. Alors $|\mathfrak{N}(K^n)| = q^{n(n-1)}$. DÉV. 3

Références

[FG] Serge Francinou et Hervé Gianella : *Exercices de mathématiques pour l'agrégation : Algèbre 1.*

[FGN] Serge Francinou, Hervé Gianella et Serge Nicolas : *Oraux X–ENS : Analyse 1.*

[FS] Philippe Flajolet et Robert Sedgewick : *Analytic Combinatorics.*

[Tos] Nicolas Tosel : Quelques dénombrements dans $\mathcal{M}_n(\mathbf{F}_q)$. *In Revue de la Filière Mathématiques*, numéro 117–1.