190

Méthodes combinatoires, problèmes de dénombrement.

Soient n, p et k trois entiers naturels, et E et F deux ensembles.

I- Éléments d'analyse combinatoire

A- Les ensembles finis, briques élémentaires de la combinatoire

[Go] 299 293 **Thm/Def 1** : ▸ On dit que E et F sont *équipotents* s'il existe une bijection de E dans F.

▸ On dit que E est *fini* s'il existe $m \in \mathbb{N}$ tel que E et $[\![1,m]\!]$ sont équipotents. L'entier m est unique, on l'appelle *cardinal* de E, et on le note $\#E$ ou $\mathrm{card}(E)$, voire $|E|$.

Dans la suite, on suppose que $\#E = n$ et $\#F = p$.

Thm 2 : ▸ E et F sont équipotents *si, et seulement si* $\#E = \#F$.

▸ $E = \emptyset \iff \#E = 0$.

[Go] 300 **Prop 3** : Si $F \subseteq E$, alors $\#F \leq \#E$, avec égalité *si, et seulement si* $F = E$.

[Go] 300 **Cor 4** (principe des tiroirs) : Si $\#E > \#F$, alors pour toute application $f : E \to F$, il existe un élément de F admettant au moins 2 antécédents. (Contraposée : s'il existe $f : E \to F$ injective, alors $\#E \leq \#F$.)

[Go] 299 **Appli 5** : Soient $(G, \times)$ un groupe et H une partie finie non vide G. Si H est stable par $\times$, alors H est un sous-groupe de G.

B- Principe additif - obtention de formules par partion

[Go] 300 **Prop 6** (principe additif) : Si $E \cap F = \emptyset$, alors $\#E \sqcup F = \#E + \#F$.

Cor 7 (lemme des bergers) : S'il existe $f : E \to F$ telle que chaque élément de F admet exactement $k \geq 1$ antécédents par f, alors $\#E = k\#F$.

[Go] 300 **Cor 8** : Si $F \subseteq E$, alors $\#E \setminus F = \#E - \#F$

[Go] 301 **Thm 9** (formule du crible) : ▸ $\#E \cup F = \#E + \#F - \#E \cap F$

▸ Plus généralement, si $(E_1, \dots, E_m)$ est une famille d'ensembles finis, alors :

$$\# \bigcup_{k=1}^{m} E = \sum_{k=1}^{m} (-1)^{k+1} \sum_{\substack{I \subseteq [\![1,m]\!] \\ \#I = k}} \# \bigcap_{i \in I} E_i$$

Rq 10 : Une méthode très répandue pour obtenir des formules explicites ou des relations de récurrence est de partitionner un ensemble selon un critère bien choisi. On peut par exemple démontrer le principe des tiroirs en écrivant $E = \bigsqcup_{y \in F} f^{-1}(\{y\})$. Voir le paragraphe D pour d'autres exemples.

C- Principe multiplicatif - listes et arrangements

Prop 11 (principe multiplicatif) : $\#E \times F = \#E \times \#F$. [Go] 301

Cor 12 : $\# E^F = \#E^{\#F}$. [Go] 302

Cor 13 : $\#\mathcal{P}(E) = 2^{\#E}$. [Go] 302

Def 14 : ▸ Une k-liste de E est un élément de E^k. [Go] 301

▸ Un *k-arrangement* de E est une k-liste de E dont les composantes sont distinctes.

▸ On appelle *arrangement de k parmi n*, et on note A_k^n le nombre de k-arrangements d'un ensemble à n éléments.

Prop 15 : $A_k^n = \dfrac{n!}{(n-k)!}$ si $0 \leq k \leq n$, et $A_k^n = 0$ sinon. [Go] 301

Ex 16 : ▸ A_n^p est le nombre d'injections de E dans F. [Go] 302

▸ A_k^n est le nombre de tirages successifs sans remise de k boules parmi n.

D- Combinaisons - coefficient binomial

Def 17 : ▸ On appelle *k-combinaison* de E une partie de E de cardinal k. [Go] 302

▸ On appelle *combinaison de k parmi n* ou plus simplement *k parmi n*, et on note C_k^n ou $\binom{n}{k}$, le nombre de k-combinaisons d'un ensemble à n éléments.

Prop 18 : $k!\binom{n}{k} = A_k^n$, et donc $\binom{n}{k} = \dfrac{n!}{k!(n-k)!}$ si $0 \leq k \leq n$, et $\binom{n}{k} = 0$ sinon. [Go] 302

Prop 19 : ▸ $\binom{n}{k} = \binom{n}{n-k}$ ▸ $\binom{n}{0} = \binom{n}{n} = 1$ ▸ $\binom{n}{1} = \binom{n}{n-1} = n$ [Go] 303

▸ Formule de Pascal : $\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$

▸ Formule des colonnes : $\binom{n+1}{p+1} = \sum_{k=p}^{n} \binom{k}{p}$

Ex 20 : Formules obtenues par partition d'un ensemble

[Rb] 53 ▸ Notons D_n le nombre dérangements d'un ensemble à n éléments. Par convention, $D_0 = 1$. On a : $n! = \sum_{k=0}^{n} \binom{n}{k} D_k$

▸ Notons $S_{n,p}$ le nombre de surjections d'un ensemble de cardinal n sur un ensemble de cardinal p. On a $p^n = \sum_{k=0}^{p} \binom{p}{k} S_{n,k}$.

[Go] 303-306 ▸ $\Gamma_n^p = \#\{(\alpha_1, \dots, \alpha_p) \in \mathbb{N}^p \mid \alpha_1 + \dots + \alpha_p = n\} = \binom{n+p-1}{p-1} = \binom{n+p-1}{n}$. C'est le nombre de manières de choisir sans ordre p éléments (non nécessairement distincts) parmi n éléments (on parle de combinaison avec répétition).

[P] 74 ▸ $\varphi(n) = \sum_{d \mid n} \varphi(d)$ où $\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times = \#\{z \in \mathbb{U}_n \mid \mathbb{U}_n = \langle z \rangle\}$

[Go] 304 Prop 21 ▸ Formule du binôme : $\forall (a,b) \in \mathbb{R}^2$, $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$

[Go] 305 ▸ Formule du multinôme : $\forall (a_1, \dots, a_p) \in \mathbb{R}^p$, $(a_1 + \dots + a_p)^n = \sum_{\substack{(i_1,\dots,i_p) \in \mathbb{N}^p \\ i_1 + \dots + i_p = n}} \frac{n!}{i_1! \cdots i_p!} a_1^{i_1} \cdots a_p^{i_p}$

[Go] 304 ▸ Formule de VANDERMONDE : $\sum_{i=0}^{n} \binom{n}{i}\binom{p}{k-i} = \binom{n+p}{k}$

Appli 22 : Construction des lois hypergéométrique et multinomiale

[Rb] 51 Thm 23 (formule d'inversion de PASCAL) : Soient $(f_n)_{n\in\mathbb{N}}$ et $(g_n)_{n\in\mathbb{N}}$ deux suites réelles telles que $\forall n \in \mathbb{N}$, $f_n = \sum_{k=0}^{n} \binom{n}{k} g_k$. Alors $\forall n \in \mathbb{N}$, $g_n = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} f_k$.

Appli 24 : $S_{n,p} = \sum_{k=0}^{p} (-1)^{p-k} \binom{p}{k} k^n$.

E - Série génératrice d'une suite de nombres

Def 25 : Soient K un corps de caractéristique 0, et $(a_n)_{n\in\mathbb{N}} \in K^{\mathbb{N}}$. On appelle *série génératrice* de $(a_n)_{n\in\mathbb{N}}$ la série formelle $\sum_{n=0}^{+\infty} a_n X^n \in K[[X]]$.

Rq 26 : L'unicité du développement en série formelle permet d'établir des formules ou des relations entre certaines suites.

[Go] 312 Ex 27 : ▸ $\sum_{n=0}^{+\infty} \frac{D_n}{n!} X^n = \frac{e^{-X}}{1-X} = \left(\sum_{n=0}^{+\infty} \frac{(-1)^n}{n!} X^n\right)\left(\sum_{n=0}^{+\infty} X^n\right) = \sum_{n=0}^{+\infty} \left(\sum_{k=0}^{n} \frac{(-1)^k}{k!}\right) X^n$ donc $D_n = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}$

▸ On retrouve la formule de VANDERMONDE en remarquant que $(1+X)^n(1+X)^p = (1+X)^{n+p}$

▸ Supposons que $10 \mid n$. Notons A le nombre de parties de $[\![1,n]\!]$ dont la somme est divisible par 5. Notons a_p le nombre de parties de $[\![1,n]\!]$ dont la somme vaut p, de sorte que $A = \sum_{k=0}^{N/5} a_{5k}$ où $N = \frac{n(n+1)}{2}$. On a $\sum_{k=0}^{N} a_k X^k = \prod_{k=1}^{n} (1+X^k) =: P(X)$. On a : [3b7b]

$$A = \sum_{k=0}^{N/5} a_{5k} = \frac{1}{5} \sum_{k=1}^{4} P(\zeta_5^k) = \frac{1}{5} \sum_{k=1}^{4} \Big[\underbrace{(1+\zeta_5)\cdots(1+\zeta_5^4)}_{=(-1)^5-1}\Big]^{\frac{n}{5}} = \frac{1}{5} \cdot 4 \cdot 2^{\frac{n}{5}}$$

Ex 28 : On note B_n le nombre de partitions d'un ensemble à n éléments avec la convention $B_0 = 1$ (ce sont les nombres de BELL). [B] 266 [FGN] 12

1▸ $B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_{n-k}$ [Go] 314

2▸ Posons $S : t \mapsto \sum_{n=0}^{+\infty} \frac{B_n}{n!} t^n$. Cette série entière admet un rayon de convergence $R > 0$, et $\forall t \in]-R, R[$, $S'(t) = \exp(t) \times S(t)$.

3▸ Formule de DOBLINSKI : $B_n = \frac{1}{e} \sum_{p=0}^{+\infty} \frac{p^n}{p!}$

DEV 1

II - Le dénombrement à travers les mathématiques

A - Utilisation de la théorie des groupes

Soit $(G, \cdot)$ un groupe fini. Supposons que G agit sur E.

Thm 29 (de LAGRANGE) : Pour tout sous-groupe H de G, $\#G = (G:H)\#H$. [Rb] 2

Prop 30 : Si φ est un morphisme de G dans un groupe (quelconque), alors [Rb] 5

$$\#G = \#\mathrm{Ker}(\varphi)\,\#\mathrm{Im}(\varphi)$$

Appli 31 : Si $m \wedge n = 1$, alors le morphisme trivial est le seul morphisme de groupes entre $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z}$.

Thm 32 (relation orbite-stabilisateur) : $\forall x \in E$, $\#G = \#\mathrm{Orb}(x)\,\#\mathrm{Stab}(x)$. [Rb] 21

Prop 33 (équation aux classes) : L'action de G sur E partionne E en orbites. [Rb] 21

Étant donné $(x_1, \dots, x_r) \in E^r$ un système complet de représentants, on a :

$$\#E = \sum_{k=1}^{r} \#\mathrm{Orb}(x_k) = \sum_{k=1}^{r} \#G / \#\mathrm{Stab}(x_i)$$

[Rb] 23 **Appli 34** : Soit p un nombre premier. Le centre d'un groupe de cardinal une puissance de p n'est pas trivial. Corollaire : tout groupe d'ordre p^2 est abélien

[Rb] 35 **Thm 35** (formule de BURNSIDE) : Le nombre d'orbites distinctes de l'action de G sur E est $\frac{1}{\#G}\sum_{g\in G}\#\mathrm{Fix}(g)$ où $\mathrm{Fix}(g)=\{x\in E \mid g\cdot x = x\}$.

[C] 132 **Appli 36** : Espérance et variance de F_n dans Prop 45.

B- Autour des corps finis

Soient $p\geq 3$ un nombre premier et $r\in\mathbb{N}^*$, posons $q=p^r$. On pose $\varphi : \mathbb{F}_q^\times \longrightarrow \mathbb{F}_q^\times$, $x\longmapsto x^2$ et $\psi : \mathbb{F}_q^\times \longrightarrow \mathbb{F}_q^\times$, $x \longmapsto x^{\frac{q-1}{2}}$.

Prop 37 : $\mathrm{Im}(\psi)=\mathrm{Ker}(\varphi)=\{\pm 1\}$ et $\mathrm{Ker}(\psi)=\mathrm{Im}(\varphi)=\{x^2 : x\in\mathbb{F}_q^\times\}$.

Cor 38 (critère d'EULER) : $x\in\mathbb{F}_q^\times$ est un carré si et seulement si $x^{\frac{q-1}{2}}=1$

Cor 39 : Il y a $\frac{q-1}{2}$ carrés inversibles dans $\mathbb{F}_q$ (et $\frac{q+1}{2}$ carrés).

Soient p et q deux nombres premiers impairs.

[Rb] ~428 **Def 40** : Pour $x\in\mathbb{F}_p$, on définit le symbole de LEGENDRE de x en p :

$$\left(\frac{x}{p}\right)=\begin{cases}1 & \text{si } x \text{ est un carré dans } \mathbb{F}_p^\times\\ 0 & \text{si } x=0\\ -1 & \text{sinon}\end{cases}$$

Pour $x\in\mathbb{Z}$, on pose $\left(\frac{x}{p}\right)=\left(\frac{x \bmod p}{p}\right)$.

[Rb] 431 - 434 **Lemme 41** : Pour $a\in\mathbb{F}_q^\times$,

1. $\left(\frac{a}{q}\right) \bmod q = a^{\frac{q-1}{2}}$
2. $\#\{x\in\mathbb{F}_q^\times \mid ax^2=1\} = 1+\left(\frac{a}{q}\right)$

[C] 301 **Thm 42** (loi de réciprocité quadratique) : $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ DEV 2

C- Probabilités discrètes, permutations aléatoires

Notons $\mathbb{P}$ la probabilité uniforme sur $(E,\mathcal{P}(E))$.

Prop 43 : $\forall A\in\mathcal{P}(E)$, $\mathbb{P}(A)=\frac{\#A}{\#E}$

Ex 44 (marche aléatoire sur $\mathbb{Z}$) : À chaque instant, $\mathbb{P}(k\to k+1)=1-\mathbb{P}(k+1\to k)=p\in]0,1[$. La probabilité de revenir en 0 partant 0 en $2n$ étapes est la probabilité de faire n pas à droite et n à gauche, et donc vaut $[p(1-p)]^n\binom{2n}{n}$. [Go] 382-383

Dans ce qui suit, $E=\mathfrak{S}_n$.

Prop 45 : Notons F_n la variable aléatoire qui compte le nombre de points fixes d'une permutation choisie au hasard dans $\mathfrak{S}_n$. [W] 1

- $\mathbb{P}(F_n=0)=\frac{\#D_n}{\#\mathfrak{S}_n}=\sum_{k=0}^{n}\frac{(-1)^k}{k!}$
- $\forall r\in[\![0,n]\!]$, $\mathbb{P}(F_n=r)=\frac{1}{\#\mathfrak{S}_n}\binom{n}{r}D_{n-r}=\frac{1}{n!}\binom{n}{r}(n-r)!\sum_{k=0}^{n-r}\frac{(-1)^k}{k!}=\frac{1}{r!}\sum_{k=0}^{n-r}\frac{(-1)^k}{k!}$
$\xrightarrow[n\to+\infty]{}\frac{e^{-1}}{r!}$

En particulier, $F_n\xrightarrow{\mathcal{L}}\mathcal{P}(1)$.

Prop 46 : Notons X_k la variable aléatoire qui vaut 1 si k est un point fixe, et 0 sinon. Alors $F_n=X_1+\dots+X_n$, $X_k\sim\mathcal{B}(\frac{1}{n})$, $\mathbb{P}(X_k=X_j=1)=\frac{1}{n(n-1)}$, donc $\mathbb{E}[F_n]=\mathbb{V}[F_n]=1$.

RÉFÉRENCES

[Rb] Rombaldi Algèbre et géométrie (2e)
[Go] Gourdon Algèbre (3e)
[P] Perrin Cours d'Algèbre
[B] Bernis² 40 développements [DEV 1]
[FGN] Oraux X-ENS Algèbre 1 [DEV 1]
[C] Caldero Nouvelles Histoires Hédonistes I [DEV 2]
[W] Wikipédia Permutation aléatoire
[3b1b] 3blue1brown (Youtube) "Olympic level counting"