190 MÉTHODES COMBINATOIRES, PROBLÈMES DE DÉNOMBREMENT.

I - MÉTHODES D'ANALYSE COMBINATOIRE

a) Lois fondamentales de la combinatoire

[G] **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 de cardinal $n \in \mathbb{N}$ si E et $\{1, \dots, n\}$ sont équipotents. L'entier n est unique, et est noté $\#E$ ou $|E|$.

[G] **Prop 2** : Si $E \subseteq F$, alors $|E| \leq |F|$, avec égalité si et seulement si $E = F$.

[G] **Corollaire 3** : [principe des tiroirs]
Si $|E| > |F|$, pour toute application $f : E \to F$, il existe un élément de F avec au moins deux antécédents par f.

[#] **Exemple 4** : Toute partie de $\{1, \dots, 9\}$ de cardinal 6 contient deux éléments dont la somme vaut 10.

[G] **Application 5** : Pour tout $x \in \mathbb{R}$, pour tout $n \in \mathbb{N}^*$, il existe $\frac{p}{q} \in \mathbb{Q}$ avec $1 \leq q \leq n$ tels que $|x - \frac{p}{q}| < \frac{1}{q \cdot n}$.

[W] **Application 6** : On peut placer jusqu'à 14 fous sur un échiquier sans capture immédiate.

[G] **Prop 7** : [règle de la somme]
Soient $E_1, \dots, E_r$ des ensembles deux à deux disjoints. Alors $|\bigsqcup_{i=1}^{r} E_i| = \sum_{i=1}^{r} |E_i|$.

Rq 8 : $|\cdot|$ est une mesure sur $(\mathbb{N}, \mathcal{P}(\mathbb{N}))$.

[G] **Prop 9** : [règle du produit]
Soient $E_1, \dots, E_r$ des ensembles. $|E_1 \times \dots \times E_r| = |E_1| \times \dots \times |E_r|$.

[#] **Cor 10** : $\# \mathcal{P}(E) = 2^{\#E}$.

[G] **Thm 11** : [formule du crible de Poincaré]
Soient $A_1, \dots, A_r$ des ensembles finis. $|\bigcup_{k=1}^{r} A_k| = \sum_{k=1}^{r} (-1)^{k-1} \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} |A_{i_1} \cap \dots \cap A_{i_k}|$

Corollaire 12 : [principe d'inclusion - exclusion] [#]
Soient $A_1, \dots, A_r$ des sous-ensembles de E fini.
$$|E \setminus \bigcup_{i=1}^{r} A_i| = |E| + \sum_{k=1}^{r} (-1)^k \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq r} |A_{i_1} \cap \dots \cap A_{i_k}|.$$

Exemple 13 : Il y a 26 entiers inférieurs à 100, qui ne sont des multiples ni de 2, 3 ou 5. [#]

Lemme 14 : [principe du double comptage] [AZ]
Soient R, C finis, $S \subseteq R \times C$. Si $(p, q) \in S$, on dit que p et q sont incidents. En notant r_p le nombre d'éléments incidents à $p \in R$ et c_q le nombre d'éléments incidents à $q \in C$, on a $\sum_{p \in R} r_p = |S| = \sum_{q \in C} c_q$.

Exemple 15 : $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$ [W]

Exemple 16 : Soit (V, E) un graphe simple. Alors $\sum_{v \in V} \deg(v) = 2|E|$. [AZ]

Application 17 : [formule de Burnside] [#]
Soient G un groupe fini, X un ensemble fini, X/G l'ensemble des orbites pour l'action de G sur X. Alors [CP]
$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |Fix(g)|.$$

b) Arrangements, permutations, combinaisons

Defs 18 : Soit E un ensemble fini, de cardinal n. [G]

- ▷ Une p-liste est un élément de E^p. Il y en a n^p en tout.
- ▷ Un p-arrangement est une p-liste de E, d'éléments distincts. Il y en a $P(n, p) = \frac{n!}{(n-p)!}$.
- ▷ Une p-combinaison est une partie de E de cardinal p. Il y en a $C(n, p) = \binom{n}{p} = \frac{n!}{(n-p)!\,p!}$.

Prop 19 : ▷ $\binom{n}{p} = \binom{n}{n-p}$ ▷ $\binom{n}{0} = \binom{n}{n} = 1$ ▷ $\binom{n}{1} = \binom{n}{n-1} = n$ [G]

- ▷ Formule de Pascal : $\binom{n}{p} = \binom{n-1}{p-1} + \binom{n-1}{p}$
- ▷ $\sum_{p=0}^{n} \binom{n}{p} = 2^n$ [H]

[#] Exemples 20 : ▷ [binôme de Newton] $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$.

▷ Il y a $120 = \frac{6!}{6}$ 6-cycles dans S_6.

[#] Application 21 : Soient A, B deux ensembles finis, $|A| = m$, $|B| = n$.

- Il y a n^m fonction de A dans B.
- Il y a $P(n,m) = \frac{n!}{(n-m)!}$ fonctions injectives de A dans B.
- (p.392) Il y a $n!\,S(m,n) := \sum_{k=0}^{n} (-1)^k \binom{n}{n-k}(n-k)^m$ fonctions surjectives de A dans B.

[G] Prop 22 : Soit E un ensemble de cardinal n, $i_1,\dots,i_p \in \mathbb{N}$ tels que $i_1+\dots+i_p = n$. Le nombre de partitions ordonnées $(A_1,\dots,A_p)$ de E telles que pour tout k, $|A_k| = i_k$ est

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

[#] Application 23 : Il y a $\frac{9!}{2!\,3!} = 30\,240$ permutations des lettres de MANAARIKI.

[G] Exemple 24 : [formule du multinôme] $(a_1+\dots+a_p)^n = \sum_{\substack{i_1,\dots,i_p\in\mathbb{N} \\ i_1+\dots+i_p=n}} \binom{n}{i_1,\dots,i_p} a_1^{i_1}\cdots a_p^{i_p}$.

[#] [G] Prop 25 : Le nombre de manières de choisir sans ordre p éléments (non nécessairement distincts) parmi n éléments (combinaison avec répétition) est $\binom{n+p-1}{n}$.

[#] Application 26 : Il y a $\binom{4+7-1}{7} = 120$ solutions dans $\mathbb{N}^4$ à $x_1+x_2+x_3+x_4=7$.

[#] Application 27 : Il y a $\binom{6+10-1}{10} = 3003$ distributions possibles de 10 billes dans 6 poches distinctes.

c) Les séries génératrices, outil crucial du dénombrement

Def 28 : Soit $(a_n)_n$ une suite réelle. On définit sa série génératrice par la série formelle $\sum_{n=0}^{+\infty} a_n X^n \in \mathbb{R}[X]$.

Rq 30 : L'unicité de l'écriture en série formelle et du développement de fonctions en séries entières permet de dénombrer des objets sous conditions.

Ex 29 : $(1+x)^n$ est la fonction associée à la série génératrice de la suite $\left(\binom{n}{k}\right)_{k\le n}$. [#]

$\frac{1}{1-x}$ est la fonction génératrice de la suite $(1, 1, \dots)$.

→ Plus d'exemples en annexe.

Exemple 31 : Notons D_n le nombre de dérangements d'un ensemble à n éléments, c'est-à-dire le nombre de permutations sans point fixe. [G]

Alors $\sum_{n=0}^{+\infty} \frac{D_n}{n!} X^n = \frac{e^{-X}}{1-X} = \left(\sum_{n=0}^{+\infty}\frac{(-1)^n}{n!}X^n\right)\left(\sum_{n=0}^{+\infty} X^n\right) = \sum_{n=0}^{+\infty}\left[\sum_{k=0}^{n} \frac{(-1)^k}{k!}\right]X^n$

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

Exemple 32 : 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). [BB]

▷ $B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_{n-k}$

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

▷ Formule de Dobinski : $B_n = \frac{1}{e}\sum_{p=0}^{+\infty}\frac{p^n}{p!}$.

DEV 1

Def 33 : Pour $n\in\mathbb{R}$, on pose $\binom{n}{r} := \frac{n(n-1)\dots(n-r+1)}{r!}$. [#]

En particulier, pour $n\in\mathbb{N}$, $\binom{-n}{r} = (-1)^r\binom{n+r-1}{r}$.

Prop 34 : $(1+x)^{-n} = \sum_{r=0}^{+\infty}\binom{-n}{r}x^r$. [#]

Application 35 : Il y a 125 façons de distribuer 24 oranges à 4 personnes, de manière à ce que chaque personne ait entre 3 et 8 oranges. [#]

C'est le coefficient devant x^{24} dans $(X^3+X^4+\dots+X^8)^4$.

II_ PROBLÈMES DE DÉNOMBREMENT EN ALGÈBRE

a) Utilisation des actions de groupes

Soit $(G,\cdot)$ un groupe fini, X un ensemble. On suppose que G agit sur X.

Prop 36 : Si φ est un morphisme de G dans un groupe, alors $|G| = |\mathrm{Ker}\,\varphi|\,|\mathrm{Im}\,\varphi|$. [R6]

[RG] Notations : On note $O_x = \{g\cdot x \mid g\in G\}$ l'orbite de x sous l'action par G, et $Stab(x) = \{g\in G \mid g\cdot x = x\}$ le stabilisateur de x.

[RG] Thm 37 : [relation orbite-stabilisateur]
$\forall x\in X,\ |G| = |Orb(x)|\cdot|Stab(x)|$.

[RG] Prop 38 : [équation aux classes]
L'action de G sur X partitionne X en orbites.
Étant donné $(x_1,\dots,x_r)\in E^r$ un système complet de représentants, on a
$$|X| = \sum_{i=1}^{r} |Orb(x_i)| = \sum_{i=1}^{r} \frac{|G|}{|Stab(x_i)|}$$

[RG] Application 39 : Soit p 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.

[CP] Application 40 : Dénombrement de matrices sur $\mathbb{F}_q$.
Soit $n\in\mathbb{N}$, $q = p^r$ où p premier, $r\geq 0$.

- $|GL_n(\mathbb{F}_q)| = \prod_{k=1}^{n-1}(q^n - q^k) = q^{\frac{n(n-1)}{2}}\prod_{k=1}^{n}(q^k - 1)$
- On note $D_n(\mathbb{F}_q)$ l'ensemble des matrices diagonalisables dans $M_n(\mathbb{F}_q)$.
$$|D_n(\mathbb{F}_q)| = \sum_{n_1+\dots+n_q = n} \frac{|GL_n(\mathbb{F}_q)|}{\prod_{i=1}^{q}|GL_{n_i}(\mathbb{F}_q)|}$$
- On note $N_d(\mathbb{F}_q)$ l'ensemble des matrices nilpotentes dans $M_d(\mathbb{F}_q)$.
$$|N_d(\mathbb{F}_q)| = q^{d(d-1)}.$$
DEV 2
- L'ensemble des matrices de $M_n(\mathbb{F}_q)$ admettant une décomposition LU est $(q-1)^n q^{n(n-1)}$.

b) Formule d'inversion de Möbius

Def 41 : La fonction de Möbius $\mu : \mathbb{N}^* \to \{-1,0,1\}$ est définie par [RG]
$$\mu(n) = \begin{cases} 1 & \text{si } n=1 \\ (-1)^r & \text{si } n = \prod_{i=1}^{r} p_i \quad (\text{i.e. si } n \text{ est sans facteur carré}) \\ 0 & \text{sinon} \end{cases}$$

Lemme 42 : Soit $n\in\mathbb{N}^*$, alors $\sum_{d\mid n}\mu(d)$ vaut 1 si $n=1$, 0 sinon. [RG]

Prop 43 : [formule d'inversion de Möbius] [FG]
Soient $f : \mathbb{N}^*\to\mathbb{R}$ multiplicative et $g : n\in\mathbb{N}^*\mapsto \sum_{d\mid n} f(d)$. Alors, pour tout $n\in\mathbb{N}^*$,
$$f(n) = \sum_{d\mid n}\mu\left(\frac{n}{d}\right)g(d).$$

Exemple 44 : On note φ l'indicatrice d'Euler : pour $n\in\mathbb{N}$, $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$. Alors pour tout $n\geq 0$, $\varphi(n) = \sum_{d\mid n}\mu(d)\frac{n}{d}$. [RG]

Prop 45 : On note $U_n(p)$ l'ensemble des polynômes irréductibles unitaires sur $\mathbb{F}_p[X]$ de degré n. [RG]

- $\forall d\mid n, \forall P\in U_d(p),\ P \mid X^{p^n} - X$.
- si P irréductible divise $X^{p^n}-X$, alors $\deg P \mid n$.

Prop 46 : Pour $n\geq 1$, on a $|U_n(p)| = \frac{1}{n}\sum_{d\mid n}\mu\left(\frac{n}{d}\right)p^d$. [RG]

Corollaire 47 : Pour tout $n\geq 1$, il existe un polynôme irréductible de degré n sur $\mathbb{F}_p$. [RG]

RÉFÉRENCES

[H] R. GRIMALDI, Discrete and Combinatorial Mathematics, 5th edition.
[AZ] M. AIGNER, G. ZIEGLER, Raisonnements divins.
[CP] P. CALDERO, M. PERONNIER, Carnet de voyage en Algébrie.
[G] T. GOURDON, Algèbre, 3e edition (!)
[RG] J.E. ROMBALDI, Algèbre et géométrie
[BB] BERNIS, BERNIS, Analyse pour l'oral de l'agrégation
[FG] FRANCINOU, GIANELLA. Exercices pour l'agrégation de mathématiques