190

Méthodes combinatoires, problèmes de dénombrement

I. Quelques outils de dénombrement [BiA]

1. Ensembles finis

Def. 1 : Un ensemble E est dit fini et de cardinal n, soit s'il est vide et dans ce cas $n=0$, soit, si $n>0$, s'il existe une bijection de E sur $[\![1,n]\!]$. On note $\mathrm{Card}(E) = |E| = n$.

Rem 2 : Si A est fini, $f : A \to B$ est bijective, alors B est fini et $|B| = |A|$

a) Réunion d'ensembles

Prop 3 : Soient A, B deux ensembles finis. Alors $A \cup B$ et $A \cap B$ sont finis et $|A \cup B| = |A| + |B| - |A \cap B|$.

Prop 4 : Soit $(E_i)_{1\leq i\leq n}$ une famille d'ensembles finis deux à deux disjoints. Alors $\left|\bigcup_{i=1}^{n} E_i\right| = \sum_{i=1}^{n} |E_i|$.

Formule du crible : Soit $(E_i)_{1\leq i\leq n}$ une famille d'ensembles finis. Alors

$$\left|\bigcup_{i=1}^{n} E_i\right| = \sum_{i=1}^{n} |E_i| - \sum_{i<j} |E_i \cap E_j| + \sum_{i<j<k} |E_i \cap E_j \cap E_k| + \dots + (-1)^{n}\left|\bigcap_{i=1}^{n} E_i\right|$$

b) Produit d'ensembles

Def. 5 : Soient $A_1 \dots A_p$ des ensembles finis. Le produit cartésien $A_1 \times \dots \times A_p$ est l'ensemble des p-uplets $(x_1 \dots x_p)$, $x_k \in A_k$ pour $k \in [\![1,p]\!]$.

Th. 6 : $|A_1 \times \dots \times A_p| = \prod_{1\leq k\leq p} |A_k|$.

Appl 7 : Si $|A| = n$ et $|B| = p$, $|\{f : A \to B\}| = p^n$. C'est aussi le nombre de p-tirages ordonnés avec remise dans un ensemble de n boules.

· Si $|X| = n$, le nombre de parties de X est 2^n.

2. Arrangements, permutations et combinaisons

Def. 8 : Soit $(p,n) \in \mathbb{N}^2$, $1 \leq p \leq n$ et E un ensemble de cardinal n. Un arrangement p à p de E est une injection de $[\![1,p]\!]$ dans E.

Th. 9 : Le nombre d'arrangements p à p de E est $A_n^p = \frac{n!}{(n-p)!}$

Appl 10 : Le nombre de p-tirages ordonnés sans remise dans un ensemble de n boules est A_n^p

Def. 11 : Pour $n \geq 1$, on appelle permutation d'un ensemble E à n éléments tout arrangement de E n à n (c'est-à-dire une bijection de E dans E).

Rem 12 : Le nombre de permutations de E, $|E| = n$, est $n!$

Def. 13 : Soit $(n,p) \in \mathbb{N}^2$, $0 \leq p \leq n$ et E de cardinal n. Une combinaison p à p de E est une partie de E à p éléments

Th. 14 : Le nombre de combinaisons p à p d'un ensemble à n éléments est $\binom{n}{p} = \frac{n!}{p!(n-p)!}$. C'est aussi le nombre de p-tirages non ordonnés sans remise dans un ensemble de n boules.

Prop 15 : · $\binom{n}{p} = \binom{n}{n-p}$ · $\binom{n}{p} = \binom{n-1}{p} + \binom{n-1}{p-1}$ (formule de Pascal)

· $\binom{n}{p} = \frac{n}{p}\binom{n-1}{p-1} = \frac{n}{n-p}\binom{n-1}{p} = \frac{n-p+1}{p}\binom{n}{p-1}$

Formule du binôme de Newton : $(a,b) \in \mathbb{C}^2$, $n \in \mathbb{N}$:

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

Appl 16 : Soit Π la matrice de Pascal d'ordre $n+1$, de coefficients $\Pi_{i,j} = \binom{i-1}{j-1}$ si $j \leq i$, 0 sinon. Alors Π^{-1} est la matrice triangulaire inférieure de terme général $(-1)^{i-j}\binom{i-1}{j-1}$.

- Nombre de surjections de $[\![1,n]\!]$ dans $[\![1,p]\!]$ $(p\leq n)$

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

- Nombre de dérangements (permutations sans point fixe)

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

- Nombre de p-combinaisons avec répétition d'un ensemble à n éléments : $\binom{n+p-1}{n}$.

3. Autres principes

- Lemme des bergers : Soient A, B deux ensembles finis, $\varphi : A \to B$. Si $\forall x \in B$ $|\varphi^{-1}(x)| = n$, alors $|A| = n \cdot |B|$.

Ex 17 : Soit p premier impair. Il y a $\frac{p+1}{2}$ carrés dans $\mathbb{F}_p$.

Applications en théorie des groupes : [COM]

Relation orbite-stabilisateur : Soient X un G-ensemble, $x \in X$. (X et G finis)

Alors $|G| = |Stab_G(x)| \cdot |Orb(x)|$

Cor : formule des classes : si $X = \bigsqcup_{i=1}^{n} Orb(x_i)$, $|X| = \sum_{i=1}^{n} \frac{|G|}{|Stab_G(x_i)|}$

Appl 18 : Soient $n \in \mathbb{N}$ et q une puissance d'un nombre premier.

On note $D_n(q) = \{M \in M_n(\mathbb{F}_q),\ M \text{ diagonalisable}\}$.

Alors $|D_n(q)| = \sum_{n_1+\dots+n_q=n} \frac{|GL_n(\mathbb{F}_q)|}{\prod_{i=1}^{q} |GL_{n_i}(\mathbb{F}_q)|}$ avec par convention $|GL_0(\mathbb{F}_q)| = 1$ (DVPT 1)

- $|\mathbb{P}_n(\mathbb{F}_q)| = \frac{q^{n+1}-1}{q-1} = 1+q+\dots+q^n$

- Principe du double-comptage : Soient A, B deux ensembles finis et P une propriété sur $A \times B$. Alors :

$$|\{(x,y) \in A\times B \,/\, (x,y) \text{ vérifie } P\}| = \sum_{x\in A} |\{y \in B \mid (x,y) \text{ vérifie } P\}| = \sum_{y \in B} |\{x \in A \mid (x,y) \text{ vérifie } P\}|$$

Appl : Formule de Burnside [COM] : Soit X un G-ensemble (G, X finis) alors le nombre d'orbites est :

$$k = \frac{1}{|G|} \sum_{g \in G} |Fix(g)| \quad \text{où } Fix(g) = \{x \in X \mid g \cdot x = x\}$$

Ex 19 : Avec 4 perles bleues, 3 blanches et 2 rouges, on peut faire 76 colliers différents.

4. Utilisation du dénombrement

Prop 20 : Si $|A| = |B|$, $f : A \to B$ est bijective $\Leftrightarrow$ f est injective $\Leftrightarrow$ f est surjective.

- Principe des tiroirs : Si $|A| > |B|$, il n'existe pas d'injection de A sur B.

Appl 21 : Soit $x > 0$ un irrationnel. Pour tout $N \in \mathbb{N}^*$ il existe $(p,q) \in \mathbb{N}^2$, $1 \leq q \leq N$ tel que $\left|x - \frac{p}{q}\right| < \frac{1}{qN}$. [Gou An]

- Quelques cardinaux de groupes classiques [PER]

Soient $n \geq 2$ et q une puissance d'un nombre premier :

1) $|GL(n, \mathbb{F}_q)| = \prod_{i=0}^{n-1} (q^n - q^i)$

2) $|SL(n, \mathbb{F}_q)| = |PGL(n, \mathbb{F}_q)| = \frac{|GL(n, \mathbb{F}_q)|}{q-1} = q^{n-1} \cdot \prod_{i=0}^{n-2} (q^n - q^i)$

3) $|PSL(n, \mathbb{F}_q)| = \frac{|PSL(n, \mathbb{F}_q)|}{pgcd(n, q-1)}$

Appl 24 : On a les isomorphismes suivants :

- $GL(2, \mathbb{F}_2) = SL(2, \mathbb{F}_2) = PSL(2, \mathbb{F}_2) \simeq \mathfrak{S}_3$
- $PGL(2, \mathbb{F}_3) \simeq \mathfrak{S}_4$, $PSL(2, \mathbb{F}_3) \simeq A_4$

- Th. de l'amitié : On considère un groupe de $n > 2$ personnes tel que pour tout couple d'individus (u,v), il existe un unique ami commun à u et v (la relation d'amitié est supposée symétrique et irréflexive). Alors il existe une personne qui est l'amie de toutes les autres. [DVMT 2]

II. Utilisation des séries formelles / séries entières

Déf. 22. Etant donnée une suite $(a_n)_{n\in\mathbb{N}}$ de réels on définit sa série génératrice comme étant la série formelle $\sum_{n\in\mathbb{N}} a_n X^n \in \mathbb{R}[[X]]$ (ou la série entière $\sum_{n\in\mathbb{N}} a_n x^n$).

Quelques exemples d'utilisation :

- Nombre d'involutions (permutation σ telle que $\sigma^2 = id$) de $[\![1,n]\!]$.

$$U_n = \sum_{p+2q=n} \frac{n!}{2^q p! q!} \quad [BiA]$$

- Nombres de Catalan : C_n est le nombre de parenthésages possibles d'un produit de $n+1$ facteurs, et le nombre d'arbres binaires à n nœuds.

$$C_n = \frac{1}{n+1}\binom{2n}{n} \quad [S-P,\ COR]$$

- Nombres de Bell : B_n est le nombre de partitions de $[\![1,n]\!]$.

$$B_n = \frac{1}{e}\sum_{k\geq 0} \frac{k^n}{k!} \quad [X\text{-ENS Alg 1}]$$

- Partition d'un entier en parts fixées. Soient $a_1 \dots a_k$ premiers entre eux dans leur ensemble. On note V_n le nombre de k-uplets $(x_1 \dots x_k) \in \mathbb{N}^k$ tels que $\sum_{i=1}^{k} a_i x_i = n$. Alors $V_n \sim \frac{1}{a_1 \dots a_k} \cdot \frac{n^{k-1}}{(k-1)!}$. [X-ENS An 2]

III. Fonctions multiplicatives [PER]

1. Indicatrice d'Euler

Déf 23 : $n \geq 1$: $\varphi(n)$ est le nombre d'entiers x, $1 \leq x \leq n$ et n premier avec n.

Prop 24. $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$

Prop 25. Si $m \wedge n = 1$, $\varphi(mn) = \varphi(m)\cdot\varphi(n)$

Cor. 26 Si $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ avec les p_i premiers distincts, $\alpha_i \in \mathbb{N}^*$, $\varphi(n) = n\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_r}\right)$.

Prop 27 : $n = \sum_{d|n} \varphi(d)$

Appl 28 : Si K est un corps fini, K^* est cyclique.

2. Fonction de Möbius

Déf. 29. On définit $\mu : \mathbb{N}^* \to \{0, \pm 1\}$ par $\mu(1) = 1$, $\mu(n) = 0$ si n a un facteur carré, et $\mu(p_1 \dots p_r) = (-1)^r$ si $p_1 \dots p_r$ sont premiers distincts.

Prop. 30 : Si $m \wedge n = 1$, $\mu(mn) = \mu(m)\cdot\mu(n)$.

Prop 31. Pour $n \geq 2$, $\sum_{d|n} \mu(d) = 0$.

Formule d'inversion de Möbius : Soit $f : \mathbb{N}^* \to A$ où A désigne un groupe abélien noté additivement. On pose $g(n) = \sum_{d|n} f(d)$.

Alors $f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) \cdot g(d)$

Cor. 32 $\varphi(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) \cdot d$

Appl. 33 : Soit $I(n,q)$ le nombre de polynômes irréductibles de degré n sur $\mathbb{F}_q$. Alors : $I(n,q) = \frac{1}{n}\sum_{d|n} \mu\left(\frac{n}{d}\right) q^d$.

Références :

[BIA] : DE BIASI : Mathématiques pour le CAPES et l'Agrégation interne

[COM] : COMBES : Algèbre et géométrie

[S-P] : SAUX-PICART : Cours de Calcul formel : Algorithmes fondamentaux

[COR] CORMEN : Algorithmique

[PER] : PERRIN : Cours d'Algèbre

[GOU AN] : GOURDON, Analyse

Autres développements possibles : Calcul de $I(n,q)$, partition d'un entier en parts fixées, nombres de Bell.