190

Méthodes combinatoires, problèmes de dénombrement

I Méthodes de dénombrement élémentaires

1) Définitions et notations

Définition 1 : Pour A, D deux ensembles non-vides, on note A^D l'ensemble des fonctions de D vers A.

Exemple 2 : $\mathbb{R}^{\mathbb{N}}$ est l'ensemble des suites réelles

Définition 3 : Soit $f : D \to A$. On dit que f est :

- injective si $\forall x, y \in D,\ x \neq y \Rightarrow f(x) \neq f(y)$
- surjective si $\forall z \in A,\ \exists x \in D : f(x) = z$
- bijective si elle est injective et surjective.

Définition 4 : Un ensemble Ω est dit fini si :

- ou bien $\Omega = \emptyset$
- ou bien il existe $n \in \mathbb{N}^*$ et une bijection $\Omega \to \{1, \dots, n\}$.

L'entier n est unique et est appelé cardinal de Ω, noté $|\Omega|$.

Proposition 5 : Soient A et D ensembles finis

- Il existe une injection de D dans A ssi $|A| \geq |D|$
- Il existe une surjection de D dans A ssi $|A| \leq |D|$
- Il existe une bijection de D dans A ssi $|A| = |D|$

Corollaire 6 : Soit $f : A \to D$ avec A et D finis. Si $|A| = |D|$, alors : f est injective $\Leftrightarrow$ f est surjective $\Leftrightarrow$ f est bijective.

2) Principes de base du dénombrement

Définition 7 : Un ensemble Ω est dit dénombrable s'il existe une bijection entre Ω et $\mathbb{N}$.

Exemple 8 : $\mathbb{Z}$ et $\mathbb{Q}$ sont dénombrables.

Proposition 9 : Soient A et B finis. Alors $|A \times B| = |A| \times |B|$

Définition 10 : On dit que les ensembles $(A_i)_{i \in I}$ forment une partition de A si l'on a $A = \bigcup_{i \in I} A_i$ et $i \neq j \Rightarrow A_i \cap A_j = \emptyset$.

Proposition 11 : On a alors $|A| = \sum_{i \in I} |A_i|$.

Théorème 12 : Soit Ω un ensemble, I un ensemble fini ou dénombrable et $(\Omega_i)_{i \in I}$ une partition de Ω. Alors, les ensembles $(A \cap \Omega_i)_{i \in I}$ forment une partition de A.

Application 13 : (Lemme des bergers)

Soit $\phi : D \to A$ surjective. On suppose qu'il existe $a \geq 1$ tel que $\forall y \in A,\ |\phi^{-1}(y)| = |\{x \in D \mid \phi(x) = y\}| = a$. Alors $|A| = \frac{|D|}{a}$.

Remarque 14 : Dû à la procédure de comptage des moutons. Il s'agissait de compter le nombre de pattes et de diviser par 4. A = ensemble des moutons. D = l'ensemble des pattes de moutons. ϕ l'application qui à une patte associe le mouton auquel elle appartient.

Proposition 15 : $|A^D| = |A|^{|D|}$

Exemple 16 : Il y a 21^{30} résultats possibles à un examen noté de 0 à 20 dans une classe de 30 élèves.

Proposition 17 : On pose $|\Omega| = n$. Le nombre de permutations de Ω est $n!$ (qui se lit de préférence "factorielle n").

Exemple 18 : Un professeur a $5! = 120$ manières de choisir l'ordre dans lequel il va interroger 5 élèves un à un.

Proposition 19 : On pose $|A| = n$ et $|D| = p$ avec $p \leq n$. Le nombre d'injections de D dans A est $n(n-1)\cdots(n-p+1) = \frac{n!}{(n-p)!}$

Exemple 20 : 3500 personnes se présentent à l'agreg avec 300 places mises au concours. En supposant qu'il n'y ait pas d'ex-aequos, il y a $3500 \times \dots \times 3201$ palmarès possibles.

Proposition 21 : On note $\binom{n}{p}$ le nombre de parties à p éléments d'un ensemble à n éléments.

Alors $\binom{n}{p} = \frac{n(n-1)\cdots(n-p+1)}{p(p-1)\cdots 1} = \frac{n!}{p!(n-p)!}$.

Exemple 22. Reprenons l'exemple 20. Il y a $\binom{3500}{300}$ listes alphabétiques des reçus possibles

Proposition 23. Le nombre total de parties de Ω est $|\mathcal{P}(\Omega)| = 2^{|\Omega|}$

Exemple 24. 200 étudiants se présentent à un examen. Il y a 2^{200} listes alphabétiques des reçus possibles

3) Nombre de Bell

Définition 25. Soit $n \in \mathbb{N}^*$. Le n-ième nombre de Bell est le nombre de partitions de l'ensemble $[\![1, n]\!]$, avec, par convention $B_0 = 1$.

Proposition 26. Soit $n \in \mathbb{N}^*$. Le nombre de relations d'équivalences sur l'ensemble $[\![1, n]\!]$ est B_n.

Lemme 27. Pour tout $n \in \mathbb{N}$, $B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_k$.

Théorème 28. (Nombre de Bell) DEV 1
Pour tout $k \in \mathbb{N}$, $B_k = \frac{1}{e} \sum_{n=0}^{+\infty} \frac{n^k}{k!}$.

II Méthodes de dénombrement en théorie des groupes

1) Avec les groupes

Soit G un groupe fini et $H \subset G$ un sous-groupe, X un ensemble fini.

Théorème-définition 29. La relation $g_1 \sim g_2 \iff \exists h \in H, g_1 = g_2 h$ définit une relation d'équivalence sur G dont les classes d'équivalences notées gH sont les $\{gh \mid h \in H\}$. Elles sont appelées classes à gauche de G modulo H

Proposition 30. Pour tout $g \in G$, on a : $|gH| = |H|$

Définition 31. On appelle ensemble quotient de G par H, et on note G/H, l'ensemble des classes à gauche de G modulo H.

Théorème 32. (Lagrange)
On a la formule : $|G| = |H| \times |G/H|$. En particulier, $|H|$ divise $|G|$

Corollaire 33. L'ordre d'un élément de G divise $|G|$

Application 34. Un groupe d'ordre p premier est cyclique.

Définition 35. On dit que G opère sur X s'il existe une application $G \times X \to X$; $(g, x) \mapsto g.x$ satisfaisant les conditions :
i) $g.(h.x) = (gh).x$ pour tous $g, h \in G$ et $x \in X$
ii) $e.x = x$ pour tout $x \in X$. On note $G \curvearrowright X$.

Exemple 36. Pour un e.v V, $GL(V)$ opère sur V

Définition 37. Soit $G \curvearrowright X$ et $x \in X$. On appelle orbite de x l'ensemble $G.x = \{g.x \mid g \in G\}$. On appelle stabilisateur de x le sous-groupe $G_x := \{g \in G \mid g.x = x\}$.

Proposition 38. La relation sur X : $x \sim y \iff x \in G.y$ est une relation d'équivalence sur X dont les classes d'équivalences sont les orbites. Autrement dit, les orbites forment une partition de X

Proposition 39. Soit $G \curvearrowright X$ et $x \in X$. L'application $f : G/G_x \to G.x$; $gG_x \mapsto gx$ est une bijection.

Corollaire 40. $|G| = |G_x||G.x|$

Exemple 41. Un groupe fini ayant deux classes de conjugaison est d'ordre 2

Théorème 42. (Formule des classes)
Si $X = \bigcup_{i=1}^{n} X_i$ est la partition de X en orbites sous l'action de G et si $x_i \in X_i$, alors : $|X| = \sum_{i=1}^{n} |X_i| = \sum_{i=1}^{n} |G| / |G_{x_i}|$.

Application 43. Soit p premier et G un groupe.
Alors $|X^G| \equiv |X| \ (p)$ où X^G l'ensemble des $x \in X$ tels que $gx = x \ \forall g \in G$.

2) Avec les théorèmes de Sylow

Définition 44. Soient G un groupe fini et p premier divisant $|G|$. On écrit $|G| = p^\alpha m$ avec $p \wedge m = 1$ et $\alpha \geq 1$. Un p-Sylow de G est un sous-groupe de G de cardinal p^α.

Remarque 45 Un p-Sylow H de G est un p-groupe et $|G/H|$ est premier à p. Les deux propriétés caractérisent un p-Sylow.

Lemme 46: On a $|GL_n(\mathbb{F}_p)| = \prod_{i=0}^{n-1}(p^n - p^i) = p^{\frac{n(n-1)}{2}}(p^n-1)\cdots(p-1)$

Exemple 47: L'ensemble H formé des matrices triangulaires supérieures à diagonale unité dans $GL_n(\mathbb{F}_p)$ forme un p-Sylow de G avec $|H| = p^{n(n-1)/2}$

S/P **Proposition 48**: Soient G un groupe fini, p premier divisant $|G|$ et S un p-Sylow de G. Si H est un sous-groupe de G, il existe alors $g \in G$ tel que $gSg^{-1} \cap H$ est un p-Sylow de H.

Théorème 49: (d'existence de Sylow)
Dans ce cas, G contient au moins un p-Sylow.

Théorème 50: On a les propriétés suivantes :
i) Les p-Sylow de G sont 2 à 2 conjugués
ii) Si on note $n_p(G)$ le nombre de p-Sylows distincts de G, on a : $n_p(G)$ divise $|G|$ et $n_p(G) \equiv 1 \ [p]$.

Corollaire 51: Un p-Sylow de G est distingué dans G si et seulement si c'est l'unique p-Sylow de G.

Application 52: Tout groupe de cardinal 45 est isomorphe à l'un des produits directs : $(\mathbb{Z}/5\mathbb{Z})\times(\mathbb{Z}/9\mathbb{Z})$ ou $(\mathbb{Z}/5\mathbb{Z})\times(\mathbb{Z}/3\mathbb{Z})^2$.

Exemple 53: Si $|G| = 40$ alors il y a 4 éléments d'ordre 5 dans G

V/A **Application 54**: Il n'y a pas de groupe simple de cardinal 36.

III Application au symbole de Legendre.

Soit $p \geq 3$ premier.

Théorème 55: $x \in \mathbb{F}_p^*$ est un carré de $\mathbb{F}_p$ ssi $x^{\frac{p-1}{2}} = 1$.
Il y a $\frac{p-1}{2}$ carrés dans $\mathbb{F}_p^*$.

Définition 56: Pour tout $a \in \mathbb{F}_p^*$, le symbole de Legendre est l'entier $\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } a \text{ est un carré dans } \mathbb{F}_p^* \\ -1 & \text{sinon} \end{cases}$.

Lemme 57: Pour tout $a \in \mathbb{F}_p^*$, le nombre de solutions de $ax^2 = 1$ est : $\left(\frac{a}{p}\right) + 1$

Théorème 58: Pour tout $a \in \mathbb{F}_p^*$, on a $a^{\frac{p-1}{2}} = \left(\frac{a}{p}\right)$ et l'application $a \mapsto \left(\frac{a}{p}\right)$ est l'unique morphisme de groupes non trivial de $\mathbb{F}_p^* \to \{1,-1\}$.

Corollaire 59: $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

Proposition 60: Soient $q, p \geq 3$ premiers distincts.
On note $B = \{(x_0, \dots, x_{p-1}) \in (\mathbb{F}_q)^p : \sum_{i=0}^{p-1} x_i^2 = 1\}$
Alors $|B| = 1 + \left(\frac{p}{q}\right) \bmod p$

Proposition 61: On a également : $|B| = q^d\left(\frac{(-1)^d}{q}\right) + q^d$

Théorème 62: (Loi de réciprocité quadratique) DEV 2 + 60 + 61
Soient p et q deux nombres premiers impairs et distincts.
Alors : $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

Exemple 63: $\left(\frac{15}{19}\right) = -1$ donc $x^2 = 15 \ (19)$ n'a pas de solutions

A/M

V/A

I/S/E

V

KUR	Kurtzmann	De l'intégration à la proba
FGN	Francinou	X-ENS Algèbre 1
ULM	Ulmer	Théorie des groupes
SZP	Szpirglas	Maths L3 Algèbre
ROM	Rombaldi	Alg. et géo.
ISE	Isenmann	L'oral à l'agreg de maths