

1) Quelques outils de dénombrement

1) Ensembles finis

Def 1 : L'ensemble E est dit fini et de cardinal m , soit s'il est vide et dans ce cas $m=0$, soit, si m est strictement positif, s'il existe une bijection de E sur $\llbracket 1, m \rrbracket$. On note $\text{card}(E) = m$ (ou $|E|$)

Rq 2 : Si A est fini et $f: A \rightarrow B$ est bijective alors B est fini et $|B| = |A|$.

* 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 $(E_i)_{1 \leq i \leq m}$ m ensembles finis deux à deux disjoints.

$$\text{Alors } \left| \bigcup_{1 \leq i \leq m} E_i \right| = \sum_{i=1}^m |E_i|.$$

Prop 5 (Formule du crible) : Soit $(E_i)_{1 \leq i \leq m}$ m ensembles finis. Alors

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

Appli 6 : Il y a 684 nombres de trois chiffres contenant au moins l'un des chiffres 0, 3, 6, 9.

* Produit d'ensembles.

Def 7 : 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 $(x_1, \dots, x_p)$ tq $\forall k \in \llbracket 1, p \rrbracket, x_k \in A_k$.

$$\text{Thm 8 : } |A_1 \times \dots \times A_p| = \prod_{k=1}^p |A_k|.$$

Appli 9 : Tirages ordonnés (successifs) avec remise. C'est l'ensemble des applications de l'ensemble des p emplacements dans l'ensemble des m boules. Donc leur nombre est m^p .

Appli 10 : Nombre de parties d'un ensemble A à m éléments. XCA est déterminée par $\mathbb{1}_X$. Donc le nb de parties de A est égal au nb d'applications de A dans $\{0, 1\}$, i.e. 2^m .

Appli 11 : Alphabet Braille. Avec une configuration de six points disposés en rectangle et tq chacun peut être en relief ou non, on dispose $2^6 = 64$ signes différents permettant d'écrire l'alphabet, les chiffres et la ponctuation.

Appli 12 : Le cardinal de l'ensemble des applications d'un ensemble à m élts dans un ensemble à p élts est p^m .

2) Arrangements, permutations et combinaisons.

Def 13 : Soit $(p, m) \in \mathbb{N}^2, 1 \leq p \leq m$ et E un ensemble de cardinal m . Un arrangement p à p de E est une injection de $\llbracket 1, p \rrbracket$ dans E .

Thm 14 : Le nombre d'arrangements de E est $A_m^p = \frac{m!}{(m-p)!}$.

Ex 15 : Tirages ordonnés sans remise.

Leur nb est A_m^p car il s'agit des applications injectives de l'ensemble des p cases de rangement dans l'ensemble des m boules.

Def 16 : Pour $m \geq 1$, on appelle permutation d'un ensemble E à m élts tout arrangement de m à m .

Rq 17 : Le nb de permutations d'un ensemble à m élts est $m!$.

$$\text{Appli 18 : } |S_m| = m!$$

Def 19 : Soit $(m, p) \in \mathbb{N}^2, 0 \leq p \leq m$ et E de cardinal m . Une combinaison p à p de E est une partie de E à p élts.

Thm 20 : Le nb de combinaisons p à p d'un ensemble E à m élts est $\binom{m}{p} = \frac{m!}{p!(m-p)!}$.

$$\text{Prop 21 : } \binom{m}{p} = \binom{m}{m-p}$$

$$\binom{m}{p} = \binom{m-1}{p} + \binom{m-1}{p-1} \quad (\text{Formule de Pascal})$$

$$\binom{m}{p} = \frac{m}{p} \binom{m-1}{p-1} = \frac{m}{m-p} \binom{m-1}{p} = \frac{m-p+1}{p} \binom{m}{p-1}.$$

Appli 22 : Une course comporte vingt chevaux. Le nb de tiercés dans le désordre est $\binom{20}{3} = 1140$.

Prop 23 (Formule du binôme de Newton) : Soit $(a, b) \in \mathbb{C}^2, m \in \mathbb{N}$.

$$(a+b)^m = \sum_{k=0}^m \binom{m}{k} a^k b^{m-k}.$$

Appli 24 : L'inverse de la matrice de Pascal de terme général $\binom{i}{j}$ (ligne $i+1$, colonne $j+1$) est la matrice de terme général $(-1)^{i-j} \binom{i}{j}$.

Appli 25 : Le nb σ_p^m de surjections de $\llbracket 1, m \rrbracket$ dans $\llbracket 1, p \rrbracket$ est $\sigma_p^m = \sum_{k=0}^p (-1)^{p-k} \binom{p}{k} k^m$.

Appli 26 : Le nb de dérangements d'un ensemble à m éléments est

$$d_m = m! \sum_{k=0}^m \frac{(-1)^k}{k!}.$$

[BIA] p4

[BIA] p5

[BIA] p4

[BIA] p7

[BIA] p7

[BIA] p10

[BIA] p3-10

3) Autres principes:

Prop 27 (Lemme des berges): Soit A et B deux ensembles finis, φ une application de A dans B. Si $\forall x \in B, |\varphi^{-1}(x)| = m$ alors $|A| = m|B|$.

Appli 28: Il y a $\frac{p+1}{2}$ carrés dans $\mathbb{F}_p$, $p \geq 3$.

Appli 29: Théorie des groupes
Soit G un groupe fini. Soit X un ensemble fini, $G \curvearrowright X$.

- $|G| = |\text{orb}(x)| \cdot |\text{Stab}_G(x)|$
- Formule des classes: $X = \bigsqcup_{i=1}^m \text{Orb}(x_i)$, $|X| = \sum_{i=1}^m \frac{|G|}{|\text{Stab}_G(x_i)|}$

Prop 30 (Principe du double comptage): Soient A, B deux ensembles finis et P une propriété sur $A \times B$. Alors $|\{(x, y) \in A \times B / (x, y) \text{ vérifie } P\}| = \sum_{x \in A} |\{y \in B / (x, y) \text{ vérifie } P\}| = \sum_{y \in B} |\{x \in A / (x, y) \text{ vérifie } P\}|$.

Appli 31: Formule de Burnside: $|\Omega| = \frac{1}{|G|} \sum_{g \in G} |\text{Stab}_G(g)|$ avec $\Omega = \{\text{orbites}\}$.

Ex 32: Avec 4 perles bleues, 3 blanches et 2 oranges on peut faire 76 colliers.

Principe des tiroirs: Si $(m+1)$ objets sont rangés dans m tiroirs, au moins un tiroir contient deux objets.

Ex 33: Dans un groupe de 3 personnes, 2 au moins sont de même sexe.

4) Dénombrement et théorie des corps.

Prop 34 (Cardinaux de groupes classiques): Soient $m \geq 2$ et q une puissance d'un nb impair.

- 1) $|GL_m(\mathbb{F}_q)| = \prod_{i=0}^{m-1} (q^m - q^i)$
- 2) $|SL_m(\mathbb{F}_q)| = |PGL_m(\mathbb{F}_q)| = \frac{|GL_m(\mathbb{F}_q)|}{q-1}$
- 3) $|PSL_m(\mathbb{F}_q)| = \frac{|PGL_m(\mathbb{F}_q)|}{\text{Pgcd}(m, q-1)}$
- 4) $|P_2(\mathbb{F}_q)| = q+1$

Appli 35: $P = \{A = (a_{ij}) \mid a_{ij} = 0 \text{ si } i > j \text{ et } a_{ii} = 1\}$ est un p-Sylow de $GL_m(\mathbb{F}_q)$

Appli 36: $GL_2(\mathbb{F}_2) = SL_2(\mathbb{F}_2) = PSL_2(\mathbb{F}_2) \cong G_3$

- $PGL_2(\mathbb{F}_3) \cong G_4$, $PSL_2(\mathbb{F}_3) \cong A_4$
- $PGL_2(\mathbb{F}_4) = PSL_2(\mathbb{F}_4) \cong A_5$
- $PGL_2(\mathbb{F}_5) \cong G_5$, $PSL_2(\mathbb{F}_5) \cong A_5$.

Thm 37 (Chevalley, Warning): Soit K un corps fini de cardinal $q = p^k$, p premier.

Soit $(f_a)_{a \in A}$ une famille de polynômes de $K[X_1, \dots, X_m]$, indexée par un ensemble fini A. Soit $V = \{x \in K^m / \forall a \in A, f_a(x) = 0\}$.
Si $\sum_{a \in A} \deg(f_a) < m$ alors $\text{Card}(V) \equiv 0 [p]$.

Appli 38: Théorème d'Erdős-Ginzburg-Ziv **[DVPT]**

Soit $m \in \mathbb{N}^*$ et $a_1, \dots, a_{2m-1}$ des entiers. Alors il existe des indices $i_1, \dots, i_m \in \{1, \dots, 2m-1\}$ tels que $a_{i_1} + \dots + a_{i_m} \equiv 0 [m]$.

Ex 39: Soit $E = \{1, \dots, 2p\}$. Soit N_0 le nb de sous ensemble de E contenant p éléments dont la somme de élt est divisible par p.

Alors $N_0 = \frac{\binom{2p}{p} - 2}{p} + 2$.

II) Utilisation des séries formelles et séries entières.

* Séries formelles

Def 40: Soit $(d_m)_m \in \mathbb{K}^{\mathbb{N}}$, on définit sa série génératrice par $G(x) = \sum_{m \geq 0} d_m X^m \in \mathbb{K}[[X]]$.

Appli 41: Partitions d'un entier en parts fixées. **[DVPT]**

Soient $a_1, \dots, a_k \in \mathbb{N}^*$ premiers entre eux dans leur ensemble. Soient $x_1, \dots, x_k \in \mathbb{N}^*$ premiers entre eux dans leur ensemble. Pour $n \geq 1$, on note $u_n = \#\{(x_1, \dots, x_k) \in \mathbb{N}^k \mid a_1 x_1 + \dots + a_k x_k = n\}$. Alors on a $u_n \sim_{n \rightarrow \infty} \frac{1}{a_1 a_2 \dots a_k} \frac{n^{k-1}}{(k-1)!}$.

Appli 42: Nombres de Catalan

Soit C_m le nb de parenthésages possibles d'un produit de m termes. Soit $C_m = \frac{1}{m} \sum_{k=1}^{m-1} C_k C_{m-k}$. L'étude de sa série génératrice nous donne $C_m = \frac{1}{m} \binom{2m-2}{m-1}$.

Appli 43: Le nb d'involutions d'un ensemble à m élt est $u_m = \sum_{p+2q=m} \frac{m!}{p!q!}$

* Séries entières.

Prop 44 (Nombres de Bell): Pour $m \in \mathbb{N}^*$ on note B_m le nb de partitions distinctes de l'ensemble $[1, m]$, avec par convention $B_0 = 1$. Alors

- la série entière $\sum_{m \geq 0} \frac{B_m}{m!} z^m$ a un rayon de convergence $R > 0$ et sa somme f vérifie: $\forall z \in]-R, R[$, $f(z) = e^{e^z - 1}$. **[DVPT]**
- pour tout $k \in \mathbb{N}$ on a $B_k = \frac{1}{e} \sum_{m=0}^{\infty} \frac{m^k}{m!}$.

II) Fonctions multiplicatives.

1) Indicatrice d'Euler.

Def 45: On appelle fonction d'Euler et on note $\varphi(m)$ le nombre d'entiers x tels que $1 \leq x \leq m$ et x premier avec m.

Prop 46: $\varphi(m) = |(\mathbb{Z}/m\mathbb{Z})^*|$.

Ex 47: si p premier, $\varphi(p) = p-1$ et $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$, $\alpha \in \mathbb{N}^*$

Prop 48: (i) La fonction d'Euler φ est multiplicative dans le sens suivant : $m \wedge n = 1 \Rightarrow \varphi(mn) = \varphi(m)\varphi(n)$.
(ii) Si la décomposition en facteurs premiers de $n \geq 2$ est $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ alors on a $\varphi(n) = n(1 - \frac{1}{p_1}) \dots (1 - \frac{1}{p_k})$.

Prop 49: Pour $n \geq 2$, $n = \sum_{d|n} \varphi(d)$.

Appl 50: Si $\mathbb{K}$ est un corps fini, $\mathbb{K}^*$ est cyclique.

2) Fonction de Möbius.

Def 51: On définit la fonction de Möbius $\mu: \mathbb{N}^* \rightarrow \{0, 1, -1\}$ par $\mu(1) = 1$, $\mu(n) = 0$ si n est divisible par le carré d'un nb premier et $\mu(p_1 \dots p_r) = (-1)^r$ si les p_i sont des nbs premiers $\neq$ à 2 distincts.

Ex 52: $\mu(42) = \mu(2 \times 3 \times 7) = -1$.

Prop 53: si $m \wedge n = 1$, $\mu(mn) = \mu(m)\mu(n)$.

Prop 54: Pour $n \geq 2$, $\sum_{d|n} \mu(d) = 0$.

Formule d'inversion de Möbius: Soit $f: \mathbb{N}^* \rightarrow \mathbb{R}$ et $g: m \in \mathbb{N}^* \rightarrow \sum_{d|m} f(d)$

$\forall m \geq 1$ $f(m) = \sum_{d|m} \mu(\frac{m}{d}) g(d)$.

Appl 55: $\varphi(m) = \sum_{d|m} \mu(\frac{m}{d}) d$.

Appl 56: Soit $I(m, q)$ le nombre de polynômes irréductibles de degré m de $\mathbb{F}_q$. Alors $I(m, q) = \frac{1}{m} \sum_{d|m} \mu(\frac{m}{d}) q^d$. DVPT

Références:

- [BIA]: Jean de Biasi, Mathématiques pour le Capes et l'agrég interne, 3^{ème} ed.
- [CON]: Combes, Algèbre et géométrie.
- [PER]: Perrin, Cours d'algèbre.
- [ZAV]: Zavidovique, Un max de math. (Chevalley, Warning et EGZ)
- [FGN Am2]: Orlaux X-ENS analyse 2 (partitions d'un entier en parts fixées).
- [FGN M1]: Orlaux X-ENS algèbre 1 (nb de Bell).
- [SP]: Saux-Picant, Cours de calcul formel: algorithmes fondamentaux.