I] Outils de dénombrement

A] Cardinal d'un ensemble fini

Def 1 : Soit E un ensemble. On dit qu'il est fini de cardinal $n \in \mathbb{N}^*$ si il est équipotent à $I_n = [\![1;n]\!]$. On note $\mathrm{Card}\, E = n$. Par convention, $\emptyset$ est fini de cardinal 0.

Ex 2 : L'ensemble $D_n = \{k \in [\![1;n]\!] \mid k | n\}$ est fini. Si n est premier, $\mathrm{Card}\, D_n = 2$.

Prop 3 : Si $E_1, \dots, E_n$ sont finis de cardinaux $n_1, \dots, n_n$ et $\forall i \neq j, E_i \cap E_j = \emptyset$, alors $\bigcup_{i=1}^{n} E_i$ est fini de cardinal $\sum_{i=1}^{n} n_i$.

Thm 4 : (Formule du Crible) Soient $E_1, \dots, E_n$ finis. Alors $\bigcup_{i=1}^{n} E_i$ est fini et $\mathrm{Card}\left(\bigcup_{i=1}^{n} E_i\right) = \sum_{k=1}^{n} \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} (-1)^{k-1} \mathrm{Card}\left(\bigcap_{j=1}^{k} E_{i_j}\right)$

Thm 5 : Si $E_1, \dots, E_n$ sont des ensembles finis, alors le produit cartésien $\prod_{i=1}^{n} E_i$ de même et $\mathrm{Card} \prod_{i=1}^{n} E_i = \prod_{i=1}^{n} \mathrm{Card}\, E_i$.

App 6 : Il y a p^n applications de I_n vers I_p, $n, p > 0$.

App 7 : Si E est fini de cardinal $n \in \mathbb{N}^*$ alors $\mathcal{P}(E)$ de même et $\mathrm{Card}\, \mathcal{P}(E) = 2^n$.

B] Arrangements et combinaisons

Def 8 : Soit E fini de cardinal n. Un arrangement à p éléments de E est un élément de E^p formé d'éléments 2 à 2 distincts.

Rem 9 : Les arrangements à p-éléments sont en bijection avec les applications injectives de I_p dans E.

Thm 10 : Le nombre d'arrangements à p-éléments de E est $A_n^p = \frac{n!}{(n-p)!}$ pour $p \leq n$.

Rem 11 : Si $p = n$, on parle de permutations.

App 12 : $\forall n \in \mathbb{N}^*, |S_n| = n!$

App 13 : Il y a 720 nombres pouvant obtenus en permutant les chiffres 1, 2, 3, 4, 5, 6.

Def 14 : Une combinaison à p éléments de E correspond à une partie à p éléments de E.

Rem 15 : Une combinaison correspond à un arrangement auquel on ne tient pas compte de l'ordre.

Thm 16 : Si $0 \leq p \leq n$, le nombre de combinaisons à p éléments de E est $\binom{n}{p} = \frac{n!}{p!(n-p)!} = \frac{1}{p!} A_n^p$.

Prop 17 : Soient $n \in \mathbb{N}^*$ et $0 \leq p \leq n$. Alors :
- $\binom{n}{p} = \binom{n}{n-p}$
- $\binom{n+1}{p+1} = \binom{n}{p} + \binom{n}{p}$ (Formule de Pascal)

Thm 18 : (Formule du binôme de Newton) $\forall n \in \mathbb{N}$, $\forall x, y \in \mathbb{C}$, $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$

App 19 : $\sum_{k=0}^{n} \binom{n}{k} = 2^n$, $\sum_{k=0}^{n} \binom{n}{k} k = n 2^{n-1}$

C] Principes de combinatoire

Prop 20 : (Principe d'addition) Si $A_1, \dots, A_p$ est une partition de l'ensemble fini E alors $\mathrm{Card}\, E = \sum_{i=1}^{p} \mathrm{Card}\, A_i$.

En particulier :

Lem 21 : (des Bergers) Soient A, B deux ensembles finis et $\varphi : A \to B$ telle que $\exists n \in \mathbb{N}^*$, $\forall x \in B$, $\mathrm{Card}\, \varphi^{-1}(x) = n$. Alors $\mathrm{Card}\, A = n \,\mathrm{Card}\, B$.

[6] [4] [7] [7]

App22 : Le nombre de surjection de I_{n+1} vers I_n est $\frac{n}{2}(n+1)!$. Celui de I_{n+2} vers I_n est $\frac{n(3n+1)}{24}(n+2)!$

Prop23 : (Principe de multiplication) Si on a un procédé d'énumération de E en p étapes indépendantes à n_i choix pour l'étape i alors $\mathrm{Card}\, E = \prod_{i=1}^{p} n_i$;

Prop24 : (Double comptage) On peut compter le cardinal d'un ensemble de deux manières pour obtenir une formule non triviale.

II) Le dénombrement en algèbre et en théorie des corps

A] Actions de groupes

Soient G un groupe fini et X un ensemble.

Def25 : Une action de G sur X est un morphisme de groupe de G vers les bijections de X dans X. Soit $x \in X$, son orbite est $\mathcal{O}_x = \{g.x \mid g \in G\}$ et son stabilisateur $\mathrm{Stab}_G(x) = \{g \in G \mid g.x = x\}$.

Prop26 : Si G est fini, alors $\forall x \in X$, $\mathrm{Card}\, \mathcal{O}_x = \frac{|G|}{\mathrm{Card}(\mathrm{Stab}_G(x))}$

Cor27 : (Formule des classes) Si G et X sont finis et que R est une famille de représentants des orbites alors $\mathrm{Card}\, X = \sum_{x \in R} \frac{|G|}{\mathrm{Stab}(x)}$

Cor28 : Soit G un p-groupe opérant sur X fini. Soit $X^G = \{x \in X \mid \forall g \in G, g.x = x\}$. Alors $\mathrm{Card}\, X = \mathrm{Card}\, X^G [p]$

App29 : Le centre d'un p-groupe non trivial est non trivial.

B] Théorie des corps

Prop30 : Tout corps fini est d'ordre la puissance d'un nombre premier.

Thm31 : Réciproquement, si $p \in \mathbb{N}$ est premier et $q = p^n$ il existe un unique corps $\mathbb{F}_q$ à isomorphisme près qui est le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$.

Thm32 : Soit $n \in \mathbb{N}^*$. On a alors les égalités :

- $|GL_n(\mathbb{F}_q)| = \prod_{i=0}^{n-1} (q^n - q^i)$
- $|SL_n(\mathbb{F}_q)| = \left(\prod_{i=0}^{n-2} (q^n - q^i)\right) q^{n-1}$
- $|PGL_n(\mathbb{F}_q)| = |SL_n(\mathbb{F}_q)|$
- $|PSL_n(\mathbb{F}_q)| = \frac{|SL_n(\mathbb{F}_q)|}{n \wedge (q-1)}$

App33 : $GL_n(\mathbb{F}_q)$ admet un p-Sylow

App34 : Tout groupe fini G avec $p \mid |G|$ admet un p-Sylow. De plus, si s est le nombre de p-Sylow de G, alors $s \mid |G|$ et $s \equiv 1 [p]$.

Def35 : Soit $\mathbb{F}_p^2 = \{x^2 \mid x \in \mathbb{F}_p\}$ les carrés de $\mathbb{F}_p$.

Thm36 : Si $p = 2$, $\mathbb{F}_q^2 = \mathbb{F}_q$. Sinon, $|\mathbb{F}_q^{*2}| = \frac{q-1}{2}$ et $|\mathbb{F}_q^2| = \frac{q+1}{2}$

Def37 : On définie le symbole de Legendre sur $\mathbb{F}_p$, $p > 2$, par : $\left(\frac{x}{p}\right) = \begin{cases} 1 \text{ si } x \in \mathbb{F}_p^{*2} \\ 0 \text{ si } x = 0 \\ -1 \text{ si } x \notin \mathbb{F}_p^2 \end{cases}$

Cor38 : $\forall x \in \mathbb{F}_p^*$, $x \in \mathbb{F}_p^{*2} \iff x^{\frac{p-1}{2}} = 1$.

Lem39 : (DEV 1) Soient $a \in \mathbb{N}^*$ et q premier impair. Alors $\mathrm{Card}\{x \in \mathbb{F}_q \mid ax^2 = 1\} = 1 + \left(\frac{a}{q}\right)$

Thm40 : (Loi de réciprocité quadratique) Soient $p \neq q$ premiers impairs. Alors $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$

Rem41 : Sachant que $\forall n, m \in \mathbb{N}^*$, $\left(\frac{nm}{p}\right) = \left(\frac{n}{p}\right)\left(\frac{m}{p}\right)$, ceci donne un moyen de calculer certains symboles de Legendre.

III) Fonctions arithmétiques multiplicatives

[2]

Def 42: $f : \mathbb{N}^* \to \mathbb{C}$ est dite **multiplicative** si $\forall n_1, n_2 \in \mathbb{N}^*$, $n_1 \wedge n_2 = 1 \Rightarrow f(n_1 n_2) = f(n_1) f(n_2)$.

Etudions deux exemples remarquables :

A] Indicatrice d'Euler

[2]

Def 43: On définit l'indicatrice d'Euler de $n \in \mathbb{N}^*$, notée $\varphi(n)$, comme $\varphi(n) = \mathrm{Card}\{k \in [\![1;n]\!] \mid k \wedge n = 1\}$

Rem 44: $\forall n \in \mathbb{N}^*$, $\varphi(n) = \mathrm{Card}\left((\mathbb{Z}/n\mathbb{Z})^*\right)$.

Prop 45: φ est multiplicative.

Thm 46: Si $n = \prod_{k=1}^{r} p_k^{\alpha_k}$ est la décomposition en facteurs premiers de n, alors $\varphi(n) = n \prod_{k=1}^{r} \left(1 - \frac{1}{p_k}\right)$

Ex 47: $\varphi(18) = 6$

Prop 48: $\forall n \in \mathbb{N}^*$, $n = \sum_{d \mid n} \varphi(d)$

App 49: (DEV 2) (Théorème de Brauer) Soient $\sigma, \sigma' \in S_n$ de matrices de permutations $P_\sigma, P_{\sigma'} \in GL_n(k)$ où k est un corps commutatif avec $\mathrm{car}(k) = 0$. Alors σ et σ' sont conjugués si et seulement si P_σ et $P_{\sigma'}$ sont semblables.

[2]

App 50: Si k est un corps fini, alors k^* est cyclique.

B] Fonction de Möbius

[2]

Def 51: On définit la fonction de Möbius par :

$$\forall n \in \mathbb{N}^*,\ \mu(n) = \begin{cases} 1 \text{ si } n = 1 \\ (-1)^r \text{ si } n = \prod_{i=1}^{r} p_i \text{ où les } p_1, \dots, p_r \text{ premiers 2 à 2 } \neq \\ 0 \text{ sinon} \end{cases}$$

Prop 52: μ est multiplicative.

Lem 53: $\forall n \in \mathbb{N}^*$, $\sum_{d \mid n} \mu(d) = \begin{cases} 1 \text{ si } n = 1 \\ 0 \text{ sinon} \end{cases}$

Thm 54: (Formule d'inversion de Möbius) Soient $f : \mathbb{N}^* \to \mathbb{C}$ et $g : \mathbb{N}^* \to \mathbb{C}$ définie par $\forall n \in \mathbb{N}^*$, $g(n) = \sum_{d \mid n} f(d)$. On a alors $\forall n \in \mathbb{N}^*$, $f(n) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) g(d)$

App 55: $\forall n \in \mathbb{N}^*$, $\varphi(n) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) d$

App 56: Soit $I(d,q)$ le nombre de polynômes unitaires et irréductibles de degré d sur $\mathbb{F}_q$. On a $\sum_{d \mid n} d\, I(d,q) = q^n$ soit $\forall n \in \mathbb{N}^*$, $I(n,q) = \frac{1}{n} \sum_{d \mid n} \mu\left(\frac{n}{d}\right) q^d$.

IV) Utilisation de séries

[3]

Def 57: On appelle série formelle de $\mathbb{K}$ corps commutatif toute suite $(a_n) \in \mathbb{K}^{\mathbb{N}}$. On note $\left(\sum_{n \geq 0} a_n X^n\right)$ cette série formelle et $\mathbb{K}[[X]]$ l'ensemble des séries formelle qu'on munit d'une somme naturelle et d'un produit par les produits de Cauchy. $\left(\sum a_n X^n\right)$ est appelée série génératrice de (a_n).

[1]

App 58: Soit d_n le nombre de triangulation d'un polygone convexe régulier à n côtés. On vérifie que $d_n = \sum_{k=2}^{n-1} d_k d_{n+1-k}$ et on introduit $\phi(X) = \sum_{n=1} d_{n+1} X^n$ dans $\mathbb{K}[[X]]$ vérifiant $\phi(X)^2 = \phi(X) - X$. Un développement en séries entières donne alors $d_n = \frac{1}{n-1}\binom{2n-4}{n-2}$

[2]

App 59: Soient $d_1, \dots, d_p \in \mathbb{N}^*$ premiers entre eux. Soit $S_n = \mathrm{Card}\left\{(n_1, \dots, n_p) \in \mathbb{N}^p \mid \sum_{i=1}^{p} n_i = n\right\}$.

Alors $S_n \underset{+\infty}{\sim} \frac{1}{d_1 \cdots d_p} \frac{n^{p-1}}{(p-1)!}$

Références :

- Maths pour le capes et l'agrégation interne, De Biasi [1]
- Cours d'algèbre, Perrin [2]
- Algèbre et géométrie, Pambaldi [3]
- Analyse, Gourdon [4]