# I – Quelques outils de dénombrement

Définition 0 L'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 dit alors que E est un $n$-ensemble et on note $\mathrm{Card}(E)=|E|=n$.

## 1. Le raisonnement par récurrence

Définition 1 On appelle P une propriété définie sur $\mathbb{N}$, une application de $\mathbb{N}$ dans $\{V,F\}$. On dit que P est vraie (ssi) $\forall n\in\mathbb{N}, P(n)=V$.

Théorème 2 Soit P une propriété définie sur $\mathbb{N}$
- Si $P(0)=V$ est vraie et si, pour tout $n\in\mathbb{N}$, « $[P(n)=V]\Rightarrow[P(n+1)=V]$ » est vraie, alors P vraie
- Si $P(0)=V$ est vraie et si, pour tout $n\in\mathbb{N}$, « $\{\forall k, k\in[\![0,n]\!], P(k)=V\}\Rightarrow[P(n+1)=V]$ » est vraie, alors P est vraie

## 2. Ensembles finis

### ⓐ Réunion d'ensembles

Proposition 3 Soient A, B deux ensembles, alors
$$|A\cup B|=|A|+|B|-|A\cap B|$$

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

FORMULE DU CRIBLE (5) Soit $(E_i)_{1\leq i\leq n}$ une famille d'ensembles finis, alors :
$$\left|\bigcup_{1\leq i\leq n}E_i\right|=\sum_{i=1}^{n}|E_i|-\sum_{i<j}|E_i\cap E_j|+\sum_{i<j<k}|E_i\cap E_j\cap E_k|+\dots+(-1)^{n-1}\left|\bigcap_{i=1}^{n}E_i\right|$$

EXEMPLE Il y a 684 nombres de 3 chiffres contenant au moins l'un des chiffres 0, 3, 6, 9

### ⓑ Produits d'ensembles finis

Définition 6 Étant donnés $p$ ensembles finis $A_1,\dots,A_p$, tout élément de la forme $(x_1,\dots,x_p)$ où, $\forall k\in[\![1,p]\!]$, $x_k\in A_k$, est appelé $p$-uplet. L'ensemble de ces $p$-uplets, noté $A_1\times\dots\times A_p$, est le produit cartésien.

Théorème 7 $|A_1\times\dots\times A_p|=\prod_{i=1}^{p}|A_i|$

EXEMPLE $p$ tirages ordonnés avec remise dans un ensemble de $n$ boules : $n^p$ issues.

Applications
- Le cardinal des applications de X ($|X|=n$) dans Y ($|Y|=p$) est $p^n$
- Le nombre de parties de X ($|X|=n$) est $2^n$

## 3. Arrangements et combinaisons

Définition 8 Soit $(p,n)\in\mathbb{N}^{*2}$, $1\leq p\leq n$. Soit E un ens. de cardinal $n$. Un arrangement $p$ à $p$ de E est un $p$-uplet $(e_1,\dots,e_p)$ formé de $p$ éléments de E deux à deux distincts.

Remarque On peut identifier les arrangements $p$ à $p$ de E et les injections de $[\![1,p]\!]$ dans E

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

EXEMPLE $p$ tirages ordonnés sans remise dans un ensemble de $n$ boules $A_n^p$

Définition 10 Pour $n\geq 1$, on appelle permutation d'un $n$-ensemble E, tout arrangement $n$ à $n$ de E.

Remarque Le nombre de permutations est donc $A_n^n=n!$

Définition 11 Soit E un $n$-ensemble. On appelle combinaison $p$ à $p$ de E une partie de E à $p$ éléments

Théorème 12 Le nombre de combinaisons $p$ à $p$ d'un $n$-ensemble E est $\binom{n}{p}=\frac{n!}{p!\,(n-p)!}$

[DE BIASI pages 13 → 16]

<u>Propriété 13</u> • $\binom{n}{p} = \binom{n}{n-p}$ • $\binom{n}{p} = \binom{n-1}{p} + \binom{n-1}{p-1}$

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

<u>Formule du binôme (de Newton) 14</u>

Si $(a,b) \in \mathbb{R}$, alors $(a+b)^n = \sum_{p=0}^{n} \binom{n}{p} a^p b^{n-p}$

EXEMPLES • $p$ tirages non ordonnés sans remise dans un ensemble de $n$ boules : $\binom{n}{p}$

• Dans une course de 20 chevaux, il y a $A_{20}^3 = 6840$ tiercés dans l'ordre et $\binom{20}{3} = 1140$ tiercés dans le désordre.

<u>Applications</u> : • Soit $\Pi$ la matrice de Pascal d'ordre $n+1$ ($\forall 0 \leq j < i \leq n$ ; $\Pi_{ij} = \binom{i}{j}$ , $\Pi_{ij} = 0$ sinon). Alors $\Pi^{-1}$ est la matrice triangulaire inférieure de terme général $(-1)^{i-j}\binom{i}{j}$.

• Nombre de surjections de $[\![1,n]\!]$ dans $[\![1,p]\!]$ (avec $p \leq n$) est $\sigma_p^n = \sum_{k=0}^{p} (-1)^k \binom{p}{k} (p-k)^n$.

• Nombre de permutations sans points fixes d'un ensemble à $n$ éléments : $d_n = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}$

## 4 - Lemme des Bergers

[DE BIASI 20] <u>Lemme des bergers 15</u> Soit A et B deux ensembles finis, $\varphi$ une application de A dans B. Si $\forall x \in B$, $|\varphi^{-1}(x)| = n$ alors $|A| = n\,|B|$

<u>Exemple</u> Soit $p$ premier, $p \geq 3$. Le nombre de carrés dans $\mathbb{F}_p$ est $\frac{p+1}{2}$.

<u>Application (Théorie des groupes)</u> :

[ULMER p67/68] <u>Relation orbite - stabilisateur 16</u> Soient X un G-ensemble, $x \in X$. Alors :

$$|G| = |Stab_G(x)|\,|Orb(x)|$$

<u>Corollaire formule des classes 17</u> Soient G groupe fini et $X = \bigcup_{i=1}^{r} Orb(x_i)$ un G-ensemble. Alors $|X| = \sum_{i=1}^{r} \frac{|G|}{|Stab(x_i)|}$

## 5 - Autres principes

• <u>Principe du double comptage</u>

Soient A, B deux ensembles finis et P une propriété sur A×B. Alors $|\{(x,y) \in A \times B \,/\, (x,y) \text{ vérifie } P\}| = \sum_{x \in A} |\{y \in B \,/\, (x,y) \text{ vérifie } P\}|$

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

<u>Application (Théorie des groupes)</u>

<u>Formule de Burnside 18</u> Soient G un groupe fini et X un G-ensemble fini tel que $X = \bigcup_{i=1}^{k} \mathcal{O}_i$. Alors, [COMBES p43]

$$k = \frac{1}{|G|} \sum_{g \in G} \text{card}(\text{fix}\, g) \quad \text{où fix}\, g = \{x \in X \,/\, gx = x\}$$

EXEMPLES → Problème du collier [p44]

Avec 4 perles bleues, 3 blanches et 2 noires ; on peut faire 76 colliers.

→ Problème du coloriage du cube. [LEHMAN]

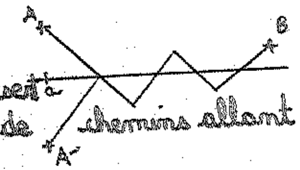
Avec $n$ couleurs, il y a $\frac{1}{24}(n^6 + 3n^4 + 12n^3 + 8n^2)$ façons de colorier un cube. [DEV 1]

• <u>Principe des tiroirs</u> Si $(n+1)$ objets sont rangés dans $n$ tiroirs ; au moins un tiroir contient au moins 2 objets

<u>EXEMPLE</u> Dans un groupe de 6 personnes, il y a

- soit 3 personnes qui se connaissent mutuellement
- soit 3 personnes qui ne connaissent aucune des 2 autres

• <u>Principe de reflexion</u> [FOATA - FUCHS Calcul des proba p35 → 37]




<u>Lemme 19</u> Le nombre de chemins de A$(a,\alpha)$ à B, qui touchent ou traversent l'axe horizontal est égal au nombre de chemins allant de A'$(a,-\alpha)$ à B.

<u>Application</u> : Soient $n \geq 1$, $s \geq 1$. Le nombre de chemins allant de $(0,0)$ à $(n,s)$ et restant toujours strictement au dessus de l'axe horizontal est : $\frac{p-q}{p+q}\binom{p+q}{p}$ où $p = \frac{n+s}{2}$ ; $q = \frac{n-s}{2}$

<u>EXEMPLE</u> Dans un scrutin, il y a $p$ bulletins pour le candidat P et $q$ pour le candidat Q. On suppose $p > q$. Alors la probabilité pour que durant le dépouillement, P soit toujours en tête, est $\frac{p-q}{p+q}$

Remarque Lien avec le problème du parenthésage.

## II - Utilisation des séries génératrices

Définition 20 Étant donnée $(a_n)_{n\in\mathbb{N}}$ suite de réels. On définit la série génératrice de $(a_n)$ comme étant la série formelle $\sum_{n\in\mathbb{N}} a_n X^n \in \mathbb{R}[[X]]$.

Remarque On rappelle que l'ensemble des séries formelles $\mathbb{R}[[X]]$ est une $\mathbb{R}$-algèbre.

Applications

[CORMEN p 264]

- Nombres de Catalan

Soit $C_n$ le nombre d'arbres binaires à $n$ noeuds. Alors $C_n = \frac{1}{n+1}\binom{2n}{n}$ est le $n$-ième nombre de Catalan.

Remarque : $C_n$ est aussi le nombre de façons de parenthéser $n+1$ facteurs dans une expression faisant intervenir une loi de composition non-associative.

[DEV 2]
[X-ENS Alg 1 p 12]

- Nombres de Bell

Si on note $B_n$ le nombre de partitions de l'ensemble $[\![1,n]\!]$, $B_n$ est le $n$-ième nombre de Bell donné par $B_n = \frac{1}{e}\sum_{k\geq 0}\frac{k^n}{k!}$

[X-ENS An 2 p 197]

- Partition d'un entier en part fixées

Soient $a_1,\dots,a_k \in \mathbb{N}^*$, premiers entre eux dans leur ensemble. On note $U_n$ le nombre de $k$-uplet $(x_1,\dots,x_k)\in\mathbb{N}^k$ tq $\sum a_i x_i = n$. Alors $U_n \sim \frac{1}{a_1\dots a_k}\frac{n^{k-1}}{(k-1)!}$

EXEMPLE : On peut trouver le nombre de façons d'obtenir $m$€ avec des pièces de 1 et 2€ et des billets de 5€, à l'aide d'une décomposition en éléments simples. C'est un cas particulier de l'application précédente.

## III - Fonctions multiplicatives

[PERRIN] p 24 → 25

### 1 - Indicatrice d'Euler

Définition 21 On appelle indicatrice d'Euler et on note $\varphi(n)$ le nombre d'entiers $x$ tels que $1\leq x\leq n$ et $x$ est premier avec $n$.

Remarque : Si $p$ est premier, $\varphi(p)=p-1$.

Proposition 22 $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$

Proposition 23 Si $m\wedge n=1$, alors $\varphi(mn)=\varphi(m)\varphi(n)$

Corollaire 24 Soit $n\in\mathbb{N}$, $n=p_1^{\alpha_1}\cdots p_r^{\alpha_r}$ avec les $p_i$ premiers distincts, $\alpha_i\in\mathbb{N}^*$. Alors $\varphi(n)=n\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_k}\right)$

EXEMPLE Il y a 96 inversibles dans $\mathbb{Z}/360\mathbb{Z}$

Proposition 25. $n=\sum_{d|n}\varphi(d)$.

### 2 - Fonction de Möbius

p 89.

Définition 26 On définit la fonction de Möbius $\mu : \mathbb{N}^* \to \{0,\pm1\}$ par $\mu(1)=1$, $\mu(n)=0$ si $n$ contient un facteur carré et $\mu(p_1\cdots p_r)=(-1)^r$ si $p_1,\dots,p_r$ sont des nombres premiers distincts.

Proposition 27 $\mu$ est multiplicative ; si $m\wedge n=1$, alors $\mu(mn)=\mu(m)\mu(n)$.

Proposition 28. $\forall n\in\mathbb{N}^*, n\neq 1, \sum_{d|n}\mu(d)=0$

Formule d'inversion de Möbius 29 Soit $f:\mathbb{N}^*\to A$, où $A$ désigne un groupe abélien noté additivement. On pose $g(n)\overset{\text{def}}{=}\sum_{d|n}f(d)$. Alors $f(n)=\sum_{d|n}\mu\left(\frac{n}{d}\right)g(d)$.

Corollaire 30 $\varphi(n)=\sum_{d|n}\mu(n/d)\,d$.

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

[FRANCINOU-GIANELLA exercices de maths pour l'agreg p 190]
(peut constituer un développement).