

190 Méthodes combinatoires, problèmes de dénombrement.

I – Dénombrement

1. Principes de base

DÉFINITION 1

On dit qu'un ensemble E est **fini** s'il est vide ou s'il existe $n \in \mathbb{N}^*$ tel qu'il existe une bijection de $\llbracket 1, n \rrbracket$ dans E . Dans ce cas, l'entier n ne dépend pas de la bijection, on l'appelle **cardinal** de E . Il est noté $|E|$. Si E est vide, on pose $|E| = 0$.

[GOU21]
p. 299

PROPOSITION 2

Soient E et F deux ensembles.

- (i) Si F est fini et s'il existe une injection de E vers F , alors E est fini et $|E| \leq |F|$.
- (ii) Si E est fini et s'il existe une surjection de E vers F , alors F est fini et $|E| \geq |F|$.
- (iii) Si E est fini et s'il existe une bijection de E vers F , alors F est fini et $|E| = |F|$.

COROLLAIRE 3

Soit B un ensemble fini et $A \subseteq B$. Alors A est fini et $|A| \leq |B|$. Si $|A| = |B|$, alors $A = B$.

COROLLAIRE 4

Principe des tiroirs.

Soient E et F deux ensembles finis avec $|E| > |F|$. Si φ est une application de E vers F , alors il existe $y \in F$ ayant au moins deux antécédents par φ dans E .

REMARQUE 5

Interprétation.

Si on doit ranger $n + 1$ chaussettes dans n tiroirs, alors un des tiroirs (au moins) contiendra deux chaussettes ou plus.

PROPOSITION 6

Soient A et B deux ensembles finis. Alors,

- (i) $|A \cup B| = |A| + |B| - |A \cap B|$.
- (ii) $|A \setminus B| = |A| - |A \cap B|$.

PROPOSITION 7**Formule du crible de Poincaré.**

Soient $A_1, \dots, A_n$ des ensembles finis. Alors,

$$\left| \bigcup_{i=1}^n A_i \right| = \sum_{k=1}^n (-1)^{k-1} \sum_{1 \leq i_1 < \dots < i_k \leq n} |A_{i_1} \cap \dots \cap A_{i_k}|$$

EXEMPLE 8

Pour $n = 3$, on a

$$|A_1 \cap A_2 \cap A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_2 \cap A_3| - |A_1 \cap A_3| + |A_1 \cup A_2 \cup A_3|$$

[G-K]
p. 401

LEMME 9**des bergers.**

Soient A et B deux ensembles. On suppose A fini. Soit $\varphi : A \rightarrow B$ surjective telle que tout élément de B admet exactement a antécédents par φ . Alors,

$$|A| = \frac{|B|}{a}$$

2. Combinatoire

a. Listes

PROPOSITION 10

Soient n ensembles finis $E_1, \dots, E_n$. Le produit cartésien $E_1 \times \dots \times E_n$ est un ensemble fini et vérifie $|E_1 \times \dots \times E_n| = |E_1| \times \dots \times |E_n|$. En particulier, pour un ensemble E fini, on a $|E^n| = |E|^n$.

[GOU21]
p. 301

DÉFINITION 11

Soit E un ensemble et $p \in \mathbb{N}^*$. On appelle **p -liste** (ou **p -uplet**) de E , tout élément $(x_1, \dots, x_p)$ de E^p .

REMARQUE 12

- Si E est fini, il y a $|E|^p$ p -listes de E .
- Dans une liste, l'ordre des éléments importe.

EXEMPLE 13

Dans un jeu de 52 cartes, le nombre de façons de tirer 10 cartes avec remise est 52^{10} .

b. Arrangements

DÉFINITION 14

Soit E un ensemble fini de cardinal n . Soit p un entier inférieur à n . On appelle **p -arrangement** de E toute p -liste de E d'éléments distincts.

PROPOSITION 15

En reprenant les notations précédentes, le nombre de p -arrangements de E est

$$A_n^p = n(n-1)\dots(n-p+1) = \frac{n!}{(n-p)!}$$

REMARQUE 16

- Si $p = n$, on trouve que le nombre de n -arrangements est $n!$.
- Dans les arrangements, l'ordre des éléments importe, mais ceux-ci sont distincts.

EXEMPLE 17

Dans un jeu de 52 cartes, le nombre de façons de tirer 10 cartes sans remise est $A_{52}^{10} = 52 \times \dots \times 43$.

APPLICATION 18**Nombre d'applications entre deux ensembles finis.**

Soient E et F deux ensembles finis.

- (i) L'ensemble des applications de E vers F , noté F^E est fini, de cardinal $|F|^{|E|}$.
- (ii) Lorsque $|E| \leq |F|$, l'ensemble des applications injectives de E dans F est fini, de cardinal $A_{|F|}^{|E|}$.
- (iii) L'ensemble des bijections de E vers E appelées permutations de E , noté $\mathcal{S}(E)$, est fini et de cardinal $|E|!$.

COROLLAIRE 19

Soit E un ensemble fini. Le nombre total de parties de E est $|\mathcal{P}(E)| = 2^{|E|}$.

c. Combinaisons

DÉFINITION 20

Soit E un ensemble fini de cardinal n . Soit $p \in \mathbb{N}$. On appelle **p -combinaison** de E toute partie de E de cardinal p . Ce nombre ne dépend que de n et de p , on le note $\binom{n}{p}$.

PROPOSITION 21

Soient $n, p \in \mathbb{N}$. Alors,

$$\binom{n}{p} = \begin{cases} \frac{n!}{p!(n-p)!} & \text{si } p \leq n \\ 0 & \text{sinon} \end{cases}$$

REMARQUE 22

Dans les combinaisons, l'ordre des éléments n'importe pas, mais ceux-ci sont distincts.

EXEMPLE 23

Dans un jeu de 52 cartes, le nombre de façons de tirer 10 cartes simultanément est $\binom{52}{10}$.

DÉFINITION 24

Soit E un ensemble fini de cardinal n . Soit p un entier inférieur à n . On appelle **p -combinaison avec répétition** les p -listes dans lesquelles on autorise les répétitions, mais dans lesquelles l'ordre ne compte pas.

PROPOSITION 25

En reprenant les notations précédentes, il y a $\binom{n+p-1}{p}$ p -combinaisons avec répétition.

PROPOSITION 26

Soit $n \in \mathbb{N}$.

(i) On a :

$$\sum_{k=0}^n \binom{n}{k} = 2^n$$

(ii) Soient a et b deux éléments d'une algèbre qui commutent. Alors,

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

APPLICATION 27

Soit (F_n) la suite de Fibonacci définie par $F_0 = 0$, $F_1 = 1$ et $\forall n \geq 2$, $F_n = F_{n-1} + F_{n-2}$. Alors,

$$\forall n \in \mathbb{N}, F_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1 + \sqrt{5}}{2} \right)^n - \left(\frac{1 - \sqrt{5}}{2} \right)^n \right) = \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n-k}{k}$$

p. 311

II – En théorie des groupes

Soit G un groupe fini.

1. Actions de groupes

Soit X un ensemble fini. On considère une action $\cdot$ de G sur X .

[ULM21]
p. 71**PROPOSITION 28**

Soit $x \in X$. Alors :

- $|G \cdot x| = (G : \text{Stab}_G(x))$.
- $|G| = |\text{Stab}_G(x)| |G \cdot x|$.
- $|G \cdot x| = \frac{|G|}{|\text{Stab}_G(x)|}$

THÉORÈME 29

Formule des classes.

Soit Ω un système de représentants d'orbites de l'action de G sur X . Alors,

$$|X| = \sum_{\omega \in \Omega} |G \cdot \omega| = \sum_{\omega \in \Omega} (G : \text{Stab}_G(\omega)) = \sum_{\omega \in \Omega} \frac{|G|}{|\text{Stab}_G(\omega)|}$$

DÉFINITION 30

On définit :

- $X^G = \{x \in X \mid \forall g \in G, g \cdot x = x\}$ l'ensemble des points de X laissés fixes par tous les éléments de G .
- $X^g = \{x \in X \mid g \cdot x = x\}$ l'ensemble des points de X laissés fixes par $g \in G$.

THÉORÈME 31

Formule de Burnside.

Le nombre r d'orbites de X sous l'action de G est donné par

$$r = \frac{1}{|G|} \sum_{g \in G} |X^g|$$

APPLICATION 32

Deux colorations des faces d'un cube sont les mêmes si on peut passer de l'une à l'autre par une isométrie du dodécaèdre. Alors, le nombre de colorations distinctes d'un cube avec c couleurs est

$$\frac{c^2}{24}(c^4 + 3c^2 + 12c + 8)$$

[I-P]
p. 121**2. p -groupes****DÉFINITION 33**

On dit que G est un **p -groupe** s'il est d'ordre une puissance d'un nombre premier p .

[ROM21]
p. 22**PROPOSITION 34**

Soit p un nombre premier. Si G est un p -groupe opérant sur un ensemble X , alors,

$$|X^G| \equiv |X| \pmod{p}$$

où X^G désigne l'ensemble des points fixes de X sous l'action de G .

COROLLAIRE 35

On note $G \cdot h_1, \dots, G \cdot h_r$ les classes de conjugaison de G . Alors,

$$\begin{aligned} |G| &= |Z(G)| + \sum_{\substack{i=1 \\ |G \cdot h_i| > 1}}^r |G \cdot h_i| \\ &= |Z(G)| + \sum_{\substack{i=1 \\ |G \cdot h_i| > 1}}^r \frac{|G|}{|\text{Stab}_G(h_i)|} \end{aligned}$$

COROLLAIRE 36

Soit p un nombre premier. Le centre d'un p -groupe non trivial est non trivial.

COROLLAIRE 37

Soit p un nombre premier. Un groupe d'ordre p^2 est toujours abélien.

APPLICATION 38

Théorème de Cauchy.

On suppose G non trivial et fini. Soit p un premier divisant l'ordre de G . Alors il existe un élément d'ordre p dans G .

DEV

APPLICATION 39

Premier théorème de Sylow.

On suppose G fini d'ordre np^α avec $n, \alpha \in \mathbb{N}$ et p premier tel que $p \nmid n$. Alors, il existe un sous-groupe de G d'ordre p^α .

[GOU21]
p. 44

III – En théorie des corps finis

Soit $q = p^n$ avec p premier et $n \geq 2$.

1. Polynômes irréductibles

THÉORÈME 40

Il existe un polynôme irréductible $P \in \mathbb{F}_p[X]$ de degré n tel que

$$\mathbb{F}_q = \mathbb{F}_p[X]/(P)$$

[GOZ]
p. 87

COROLLAIRE 41

- (i) Il existe des polynômes irréductibles de tout degré dans $\mathbb{F}_p[X]$.
- (ii) Si $P \in \mathbb{F}_p[X]$ est un polynôme irréductible sur $\mathbb{F}_p$ de degré n , alors P divise $X^q - X$. En particulier, il est scindé sur $\mathbb{F}_q$. Donc son corps de rupture $\mathbb{F}_q = \mathbb{F}_p[X]/(P)$ est aussi son corps de décomposition.

THÉORÈME 42

Pour tout $j \in \mathbb{N}^*$, on note $I(p, j)$ l'ensemble des polynômes irréductibles unitaires de degré j sur $\mathbb{F}_p$. Alors,

$$X^q - X = \prod_{d|n} \prod_{Q \in I(p, d)} Q$$

COROLLAIRE 43

$$q = \sum_{d|n} d |I(p, d)|$$

DÉFINITION 44

On définit la **fonction de Möbius**, notée μ , par

$$\mu: \mathbb{N}^* \rightarrow \mathbb{Z} \quad n \mapsto \begin{cases} 1 & \text{si } n = 1 \\ (-1)^k & \text{si } n = p_1 \dots p_k \text{ avec } p_1, \dots, p_k \text{ premiers distincts} \\ 0 & \text{sinon} \end{cases}$$

THÉORÈME 45**Formule d'inversion de Möbius.**

Soient f et g des fonctions de $\mathbb{N}^*$ dans $\mathbb{C}$ telles que $\forall n \in \mathbb{N}^*, f(n) = \sum_{d|n} g(d)$. Alors,

$$\forall n \in \mathbb{N}^*, g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right)$$

COROLLAIRE 46

$$\forall n \in \mathbb{N}^*, |I(p, n)| = \frac{1}{n} \sum_{d|n} \mu(d) p^{\frac{n}{d}} = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) p^d$$

2. Carrés dans les corps finis

PROPOSITION 47

On note $\mathbb{F}_q^2 = \{x^2 \mid x \in \mathbb{F}_q\}$ et $\mathbb{F}_q^{*2} = \mathbb{F}_q^2 \cap \mathbb{F}_q^*$. Alors $\mathbb{F}_q^{*2}$ est un sous-groupe de $\mathbb{F}_q^*$.

p. 93

PROPOSITION 48

(i) Si $p = 2$, $\mathbb{F}_q^2 = \mathbb{F}_q$, donc $\mathbb{F}_q^{*2} = \mathbb{F}_q^*$.

(ii) Si $p > 2$, alors :

- $\mathbb{F}_q^{*2}$ est le noyau de l'endomorphisme de $\mathbb{F}_q^*$ défini par $x \mapsto x^{\frac{q-1}{2}}$.
- $\mathbb{F}_q^{*2}$ est un sous-groupe d'indice 2 de $\mathbb{F}_q^*$.
- $|\mathbb{F}_q^{*2}| = \frac{q-1}{2}$ et $|\mathbb{F}_q^2| = \frac{q+1}{2}$.
- $(-1) \in \mathbb{F}_q^{*2} \iff q \equiv 1 \pmod{4}$.

3. Groupe linéaire sur un corps fini

Soit V un espace vectoriel de dimension finie n sur un corps $\mathbb{K}$.

DÉFINITION 49

- Le **groupe linéaire** de V , $\text{GL}(V)$ est le groupe des applications linéaires de V dans lui-même qui sont inversibles.
- Le **groupe spécial linéaire** de V , $\text{SL}(V)$ est le sous-groupe de $\text{GL}(V)$ constitué des applications de déterminant 1.
- Les quotients de ces groupes par leur centre sont respectivement notés $\text{PGL}(V)$ et $\text{PSL}(V)$.

[PER]
p. 119

PROPOSITION 50

On se place dans le cas où $\mathbb{K} = \mathbb{F}_q$. Alors, les groupes précédents sont finis, et :

$$(i) \quad |\mathrm{GL}(V)| = q^{\frac{n(n-1)}{2}} ((q^n - 1) \dots (q - 1)).$$

$$(ii) \quad |\mathrm{PGL}(V)| = |\mathrm{SL}(V)| = \frac{|\mathrm{GL}(V)|}{q-1}.$$

$$(iii) \quad |\mathrm{PSL}(V)| = \frac{|\mathrm{SL}(V)|}{\mathrm{pgcd}(n, q-1)} = \frac{|\mathrm{GL}(V)|}{(q-1)\mathrm{pgcd}(n, q-1)}.$$

p. 124

IV – En analyse

1. Probabilités sur un ensemble fini

Soit $(\Omega, \mathcal{A}, \mathbb{P})$ un espace probabilisé.

[G-K]
p. 137**DÉFINITION 51**

Soit $E \subseteq \Omega$ fini et non vide. On appelle loi uniforme sur E la loi discrète définie sur $\mathcal{P}(\Omega)$ par

$$\begin{aligned} \mathcal{P}(\Omega) &\rightarrow [0, 1] \\ A &\mapsto \frac{|A \cap E|}{|E|} \end{aligned}$$

REMARQUE 52

Il s'agit du nombre de cas favorables sur le nombre de cas possibles. Ainsi, X suit la loi uniforme sur E si on a $\forall x \in E, \mathbb{P}(X = x) = \frac{1}{|E|}$ et $\forall x \notin E, \mathbb{P}(X = x) = 0$.

C'est, par exemple, la loi suivie par une variable aléatoire représentant le lancer d'un dé non truqué avec $E = \llbracket 1, 6 \rrbracket$.

DÉFINITION 53

Une variable aléatoire X suit une **loi de Bernoulli** de paramètre $p \in [0, 1]$, notée $\mathcal{B}(p)$, si $\mathbb{P}(X = 1) = p$ et $\mathbb{P}(X = 0) = 1 - p$.

PROPOSITION 54

En reprenant les notations précédentes, X est une loi discrète et on a

$$\mathbb{P}_X = (1 - p)\delta_0 + p\delta_1$$

DÉFINITION 55

Une variable aléatoire X suit une **loi de binomiale** de paramètres $n \in \mathbb{N}$ et $p \in [0, 1]$, notée $\mathcal{B}(n, p)$, si X est la somme de n variables aléatoires indépendantes qui suivent des lois de Bernoulli de paramètre p .

PROPOSITION 56

En reprenant les notations précédentes, X est une loi discrète et on a

$$\forall k \in \llbracket 0, n \rrbracket, \mathbb{P}(X = k) = \binom{n}{k} p^k (1-p)^{n-k}$$

REMARQUE 57

Il s'agit du nombre de succès pour n tentatives.

C'est, par exemple, la loi suivie par une variable aléatoire représentant le nombre de "Pile" obtenus lors d'un lancer de pièce équilibrée.

2. Utilisation des séries pour dénombrer

THÉORÈME 58**Formule des dérangements.**

Soit $n \in \mathbb{N}^*$. On note $\mathcal{D}_n$ l'ensemble des permutations de $\llbracket 1, n \rrbracket$ sans point fixe. Alors,

$$|\mathcal{D}_n| = n! \sum_{k=0}^n \frac{(-1)^k}{k!} = \left\lfloor \frac{n!}{e} + \frac{1}{2} \right\rfloor$$

[GOU21]
p. 312

EXEMPLE 59

n personnes laissent leur chapeau à un vestiaire. En repartant, chaque personne prend un chapeau au hasard. La probabilité que personne ne reprenne son propre chapeau est d'environ $\frac{1}{e}$.

THÉORÈME 60**Nombres de Bell.**

Pour tout $n \in \mathbb{N}^*$, on note B_n le nombre de partitions de $\llbracket 1, n \rrbracket$. Par convention on pose $B_0 = 1$. Alors,

$$\forall k \in \mathbb{N}^*, B_k = \frac{1}{e} \sum_{n=0}^{+\infty} \frac{n^k}{n!}$$

p. 314

DEV

Bibliographie

De l'intégration aux probabilités

[G-K]

Olivier GARET et Aline KURTZMANN. *De l'intégration aux probabilités*. 2^e éd. Ellipses, 28 mai 2019.
<https://www.editions-ellipses.fr/accueil/4593-14919-de-l-integration-aux-probabilites-2e-edition-augmentee-9782340030206.html>.

Les maths en tête

[GOU21]

Xavier GOURDON. *Les maths en tête. Algèbre et probabilités*. 3^e éd. Ellipses, 13 juill. 2021.
<https://www.editions-ellipses.fr/accueil/13722-25266-les-maths-en-tete-algebre-et-probabilites-3e-edition-9782340056763.html>.

Théorie de Galois

[GOZ]

Ivan GOZARD. *Théorie de Galois. Niveau L3-M1*. 2^e éd. Ellipses, 1^{er} avr. 2009.
<https://www.editions-ellipses.fr/accueil/4897-15223-theorie-de-galois-niveau-l3-m1-2e-edition-9782729842772.html>.

L'oral à l'agrégation de mathématiques

[I-P]

Lucas ISENMANN et Timothée PECATTE. *L'oral à l'agrégation de mathématiques. Une sélection de développements*. 2^e éd. Ellipses, 26 mars 2024.
<https://www.editions-ellipses.fr/accueil/15218-28346-loral-a-lagregation-de-mathematiques-une-selection-de-developpements-2e-edition-9782340086487.html>.

Cours d'algèbre

[PER]

Daniel PERRIN. *Cours d'algèbre. pour l'agrégation*. Ellipses, 15 fév. 1996.
<https://www.editions-ellipses.fr/accueil/7778-18110-cours-d-algebre-agregation-9782729855529.html>.

Mathématiques pour l'agrégation

[ROM21]

Jean-Étienne ROMBALDI. *Mathématiques pour l'agrégation. Algèbre et géométrie*. 2^e éd. De Boeck Supérieur, 20 avr. 2021.
<https://www.deboecksuperieur.com/ouvrage/9782807332201-mathematiques-pour-l-agregation-algebre-et-geometrie>.

Théorie des groupes

[ULM21]

Felix ULMER. *Théorie des groupes. Cours et exercices*. 2^e éd. Ellipses, 3 août 2021.
<https://www.editions-ellipses.fr/accueil/13760-25304-theorie-des-groupes-2e-edition-9782340057241.html>.