

30 Leçon 190 : Méthodes combinatoires, problèmes de dénombrement.

I. Généralités sur le dénombrement

1. Cardinal des ensembles finis [GOU]

Cardinal, lien avec les bijection/injection/surjection, principe des tiroirs, lemme des bergers, formule du crible de Poincaré

2. Listes et arrangements [GOU]

Cardinal du produit cartésien, p -lise, p -arrangement, cardinal des applications et des injections, $|\mathcal{P}([1; n])|$

3. Combinaisons [GOU]

p -combinaison, formule de Pascal, formule du binôme, formule de Vandermonde

II. Dénombrement en algèbre

1. Théorie des groupes [BER] [ULM]

Ordre d'un groupe et d'un élément, théorème de Lagrange, cardinal dans le premier théorème d'isomorphisme, stabilisateur/orbite/points fixes, formule des classes (x2), p -groupe, théorème de Cauchy

DEV 1 : formule de Burnside + application

2. Indicatrice d'Euler [ROM]

$(\mathbb{Z}/n\mathbb{Z})^\times$, éléments inversibles, fonction indicatrice d'Euler, formule générale de l'indicatrice d'Euler, théorème d'Euler

3. Corps finis [PER]

Cardinal d'un corps fini, morphisme de Frobenius, existence et unicité des corps finis, toutes les propriétés sur les carrés de $\mathbb{F}_q$

III. Dénombrement en analyse

1. Probabilités discrètes [KUR]

Loi uniforme, loi de Bernoulli, loi binomiale

2. Utilisation des séries [GOU]

Nombre de dérangements, DEV 2 : Nombres de Bell

Présentation :

- On détermine parfois le cardinal d'un ensemble en construisant une bijection avec un autre ensemble plus simple dont on connaît le cardinal.
- Le nom « lemme des bergers » vient du fait qu'un berger peut compter ses moutons s'il ne voit que leurs pattes, en divisant le nombre total de pattes par quatre.
- Il arrive souvent que pour trouver le cardinal d'un ensemble, on trouve une partition dont les éléments sont de cardinal plus simple à exprimer.
- Pour dénombrer le nombre de parties d'un ensemble à n éléments (qui est 2^n) on peut soit utiliser un argument combinatoire, soit utiliser le binôme de Newton.
- Le dénombrement est très utile pour les probabilités. En effet, dans une situation d'équiprobabilité sur un espace fini, la probabilité d'un événement s'obtient comme le rapport entre le nombre d'issues favorables et le nombre total d'issues possibles.

- Dans la partie sur l'utilisation des séries, on utilise des séries entières dans les preuves pour ne pas s'embêter, mais en fait on peut utiliser seulement la théorie des séries génératrices.

Développements :

- Formule de Burnside + application
 - Algèbre : le grand combat, Berhuy, p172
 - Carnet de voyage en Algèbre, Caldero-Peronnier, p163
- Nombres de Bell
 - Oaux X-ENS 6, FGN, p338
 - Analyse pour l'agrégation, Bernis, p285

Références :

- [GOU] Algèbre-Probabilités, Gourdon
- [BER] Algèbre : le grand combat, Berhuy
- [ULM] Théorie des Groupes, Ulmer
- [ROM] Mathématiques pour l'agrégation : Algèbre et géométrie, Rombaldi
- [PER] Cours d'algèbre, Perrin
- [KUR] De l'intégration aux probabilités, Garet-Kurtzman

Leçon 190: Méthodes combinatoires, problèmes de dénombrement

I Généralité sur le dénombrement

Soit E et F deux ensembles

1) Cardinal des ensembles finis [600]

Déf 1: On dit que E est fini s'il est vide ou s'il existe $n \in \mathbb{N}^*$ tel qu'il existe une bijection $f: \mathbb{N}, n \rightarrow E$. L'entier n est appelé cardinal de E , noté $|E|$ ou $\#E$.

Prop 2: 1) Si E est fini et $f: E \rightarrow F$ bijection, alors F est fini et $|F| = |E|$.

2) Si F est fini et $f: E \rightarrow F$ injection, alors E est fini et $|E| \leq |F|$.

3) Si E est fini et $f: E \rightarrow F$ surjection, alors F est fini et $|F| \leq |E|$.
Corollaire 3: Soit B un ensemble fini et $A \subset B$. Alors A est fini $|A| \leq |B|$. Si $|A| = |B|$, alors $A = B$.

Corollaire 4 (principe des tiroirs): Soit E et F finis avec $|E| > |F|$. Si $f: E \rightarrow F$, alors il existe $\gamma \in F$ ayant au moins deux antécédents par f dans E .

Exemple 5: Si on doit ranger $n+1$ chaussettes dans n tiroirs, au moins un des tiroirs contiendra 2 chaussettes ou plus.

Prop 6: Soit A et B deux ensembles finis. Alors:

$$|A \cup B| = |A| + |B| - |A \cap B|$$

$$|A \setminus B| = |A| - |A \cap B|$$

Remarque 7: Si $A_1, \dots, A_n$ forment une partition de E qui est fini, alors $|E| = \sum_{i=1}^n |A_i|$.

Prop 8 (formule de Poincaré): Soit $A_1, \dots, A_n$ des ensembles finis. Alors on a:

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

2) Listes et arrangements [600]

Prop 9: Soit $E_1, \dots, E_n$ des ensembles finis. Alors $E_1 \times \dots \times E_n$ est fini et $|E_1 \times \dots \times E_n| = |E_1| \times \dots \times |E_n|$. Donc $|E_n^n| = |E_n|^n$.

Déf 10: Soit $p \in \mathbb{N}^*$. On appelle p -liste (ou p -uplet) de E tout élément $(x_1, \dots, x_p)$ de E^p .

Exemple 11: Les listes modélisent les tirages successifs avec remise, dans un jeu de 52 cartes, le nombre de façons de tirer 10 cartes avec remise est 52^{10} .

Déf 12: Soit $|E| = n$. Soit $p \leq n$. On appelle p -arrangement de E toute p -liste de E d'éléments distincts.

Prop 13: Il y a $A_n^p = n(n-1)\dots(n-p+1) = \frac{n!}{(n-p)!}$ p -arrangements de E .

Exemple 14: Les arrangements modélisent les tirages successifs sans remise. Dans un jeu de 52 cartes, le nombre de façons de tirer 10 cartes sans remise est $A_{52}^{10} = 52 \times 51 \times \dots \times 43$.

Prop 15: Soit E et F finis avec $|E| = p$ et $|F| = m$.

1) L'ensemble des applications de E dans F , noté F^E , est fini et on a: $|F^E| = |F|^{|E|} = m^p$.

2) Si $p \leq m$, l'ensemble des injections de E dans F est fini et de cardinal $A_m^p = \frac{m!}{(m-p)!}$.

Exemple 16: Le groupe des permutations de $\mathbb{N}, n \rightarrow \mathbb{N}, n$, S_n , est de cardinal $n!$.

Prop 17: Soit E fini. Alors $\mathcal{P}(E)$ est fini et $|\mathcal{P}(E)| = 2^{|E|}$.

3) Combinaisons [600]

Déf 18: Soit $|E| = n$. Soit $p \in \mathbb{N}$. On appelle p -combinaison de E toute partie de E de cardinal p . Le nombre de p -combinaisons de E est noté $\binom{n}{p}$.

Prop 19: Si $0 \leq p \leq n$, $\binom{n}{p} = \frac{n!}{p!(n-p)!}$. Si $p > n$, $\binom{n}{p} = 0$.

Exemple 20: Les combinaisons modélisent les tirages simultanés: Dans un jeu de 52 cartes, le nombre de façons de tirer 10 cartes simultanément est $\binom{52}{10}$.

Exemple 21: Le nombre de fonctions strictement croissantes de $\mathbb{N}, p \rightarrow \mathbb{N}, n$ dans $\mathbb{N}, n \rightarrow \mathbb{N}, n$ est $\binom{n}{p}$.

Prop 22: Soit $p, m \in \mathbb{N}$. Si $0 \leq p \leq m$, $\binom{m}{p} = \binom{m}{m-p}$.

Si $m, p > 1$: $\binom{m}{p} = \binom{m-1}{p-1} + \binom{m-1}{p}$ (formule de Pascal)

Prop 23 (Formule du binôme): Soit a, b deux éléments d'une algèbre qui commutent. Alors: $(a+b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}$.

Exemple 24: On retrouve que $1^{\mathcal{P}(E)} = 2^n$.

Prop 25 (Formule de Vandermonde): Soit $m, n, p \in \mathbb{N}$. On a:

$$\sum_{k=0}^p \binom{m}{k} \binom{n}{p-k} = \binom{m+n}{p}.$$

Corollaire 26: $\sum_{k=0}^m \binom{m}{k} \binom{n}{k} = \binom{m+n}{m}$; $\sum_{k=0}^m \binom{m}{k}^2 = \binom{2m}{m}$.

II Dénombrement en algèbre

1) Théorie des groupes [BER][ULM]

Soit $(G, \cdot)$ un groupe fini.

Def 27: Le nombre d'éléments de G est appelé l'ordre de G .

Soit $x \in G$. L'ordre de x est l'ordre du sous-groupe $\langle x \rangle$.

Théorème 28 (de Lagrange): Soit H un sous-groupe de G .

Alors: $|H| \mid |G|$.

Corollaire 29: L'ordre d'un élément divise l'ordre du groupe.

Prop 30: Si f est un morphisme de groupes de G dans G' , alors: $|G| = |\text{Ker } f| \times |\text{Im } f|$.

On suppose que G agit sur un ensemble X fini.

Def 31: L'ensemble $\text{Stab}_G(x) = \{g \in G; g \cdot x = x\}$ est appelé le stabilisateur de x sous G . C'est un sous-groupe de G .

Def 32: L'ensemble $\mathcal{O}(x) = \{g \cdot x; g \in G\} \subset X$ est appelé

orbite de x sous l'action de G .

Def 33: On dit que $x \in X$ est un point fixe sous G si l'on a $g \cdot x = x \forall g \in G$. On note X^G cet ensemble.

Prop 34: Soit $x \in X$. Alors: $|G| = |\text{Stab}_G(x)| \cdot |\mathcal{O}(x)|$.

Théorème 35 (Formule des classes): Si $\{x_1, \dots, x_n\}$ est un système de représentants des orbites on a:

$$|X| = \sum_{i=1}^n |\mathcal{O}(x_i)| = \sum_{i=1}^n \frac{|G|}{|\text{Stab}_G(x_i)|}.$$

Def 36: Soit p un nombre premier. Un p -groupe est un

groupe dont l'ordre est une puissance de p .

Prop 37: Soit G un p -groupe agissant sur X . Alors: $|X^G| \equiv |X| \pmod{p}$.

Corollaire 38: Le centre d'un p -groupe est non trivial.

Théorème 39 (de Cauchy): Soit G d'ordre divisible par un nombre premier p . Alors G admet un élément d'ordre p .

Def 40: Soit $g \in G$. On pose $\text{Fix}(g) = \{x \in E; g \cdot x = x\}$, l'ensemble des points fixés par g .

Prop 41 (Formule de Burnside): Soit X/G l'ensemble des orbites de X sous l'action de G . Alors:

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g)|.$$

Application 42: On considère l'action de S_n sur $E_n = \mathbb{Z}$.

Soit χ la variable associée à S_n qui associe à $\sigma \in S_n$ son nombre d'invariants $\text{Fix}(\sigma)$. Alors

$$|\chi| = 1 \text{ et } \chi(\sigma) = 1.$$

DEV 1

2) Indicatrice d'Enfer [ROM]

Théorème 43: Soit $n \in \mathbb{Z}$. On a l'équivalence entre:

1) n est inversible dans $\mathbb{Z}/n\mathbb{Z}$

2) n est premier avec n

3) n est un générateur du groupe cyclique $(\mathbb{Z}/n\mathbb{Z}, +)$

Def 44: On appelle fonction indicatrice d'Enfer la fonction qui à $n \in \mathbb{N}^*$ associe $\varphi(n)$ le nombre d'entiers de $\mathbb{Z}/n\mathbb{Z}$ qui sont premiers avec n .

Remarque 45: $|\{(\mathbb{Z}/n\mathbb{Z})^\times\}| = \varphi(n)$.

Exemple 46: Si p est premier, $\varphi(p) = p-1$.

Si p est premier et $d \in \mathbb{N}^*$, on a: $\varphi(p^d) = (p-1)p^{d-1}$.

Si n et m sont premiers entre eux, alors

$$\varphi(nm) = \varphi(n) \cdot \varphi(m).$$

Théorème 47: Soit $m = \prod_{i=1}^k p_i^{d_i}$ sa décomposition en

facteurs premiers. Alors:

2

$$\varphi(n) = \prod_{i=1}^r p_i^{a_i-1} (p_i - 1) = n \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right)$$

Théorème 48 (Euler): Pour tout $n \in \mathbb{Z}$ premier avec m ,
On a: $a^{\varphi(m)} \equiv 1 \pmod{m}$.

3) Corps finis [PER]

Prop 49: Le cardinal d'un corps fini est une puissance d'un nombre premier: Sa caractéristique.

Prop 50: Soit K un corps de caractéristique $p > 0$. L'application $F: K \rightarrow K$ définie par $F(x) = x^p$ est un morphisme de corps appelé morphisme de Frobenius. Si K est fini, c'est un automorphisme. Si $K = \mathbb{F}_p$, c'est l'identité.

Théorème 51: Soit p premier et $n \in \mathbb{N}^*$. Soit $q = p^n$. Il existe un corps K à q éléments, c'est le corps de décomposition de $x^q - x$ sur $\mathbb{F}_p$. En particulier, il est unique à isomorphisme près. On le note $\mathbb{F}_q$.

Notation 52: Soit $q = p^n$. Soit $\mathbb{F}_q^* = \{x \in \mathbb{F}_q; x \neq 0\}$ et $\mathbb{F}_q^{*1} = \mathbb{F}_q^* \cap \mathbb{F}_q^*$.

Prop 53: 1) Pour $q = 2$, on a $\mathbb{F}_q^* = \mathbb{F}_q$.

2) Pour $p > 2$, on a $|\mathbb{F}_q^*| = \frac{q+1}{2}$ et $|\mathbb{F}_q^{*2}| = \frac{q-1}{2}$

Prop 54: Soit $p > 2$. Alors: $x \in \mathbb{F}_q^{*1} \Leftrightarrow x^{\frac{q+1}{2}} = 1$
Corollaire 55: Soit $p > 2$. Alors (-1) est un carré dans $\mathbb{F}_q$ ssi $q \equiv 1 \pmod{4}$.

Application 56: Il existe une infinité de nombres premiers de la forme $4k+1$.

III Dénombrement en analyse

1) Probabilités discrètes [KUR]

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

Déf 57: Soit $E \subset \Omega$ un ensemble fini. On appelle loi uniforme sur E la loi définie sur $\mathcal{P}(E)$ par:
 $\mathcal{P}(A) = \frac{|A \cap E|}{|E|}$, $A \subset \mathcal{P}(E)$.

Remarque 58: Il s'agit du nombre de cas favorables sur le nombre de cas possibles. Par exemple la VA X qui donne le résultat d'un dé suit la loi uniforme sur $\{1, \dots, 6\}$.

Déf 59: On dit que la VA X suit la loi de Bernoulli de paramètre p si $\mathbb{P}(X=1) = p$ et $\mathbb{P}(X=0) = 1-p$.

Exemple 60: Cela modélise le lancer d'une pièce déséquilibrée.

Déf 61: On dit que X suit la loi binomiale de paramètres n et p si $\mathbb{P}(X=k) = \binom{n}{k} p^k (1-p)^{n-k}$ $\forall k \in \{0, \dots, n\}$.

Exemple 62: Cela compte le nombre de succès. Par exemple, si on lance n fois une pièce de monnaie équilibrée, le nombre de "pile" obtenus suit une loi binomiale de paramètres n et $\frac{1}{2}$.

2) Utilisation des séries [GOU]

Application 63: Soit $n \in \mathbb{N}^*$. On note $\mathcal{D}_n$ l'ensemble des permutations de $\{1, \dots, n\}$ sans point fixe (on appelle cela des dérangements). Pour tout $n \in \mathbb{N}^*$, on a que $n! = \sum_{k=0}^n \binom{n}{k} d_k$ où $d_k = |D_k|$.

Ainsi: $|D_n| = n! \sum_{k=0}^n \frac{(-1)^k}{k!}$.

Exemple 63 bis: probline de l'espérance

Application 64 (nombres de Bell): Pour $n \in \mathbb{N}^*$, on note B_n le nombre de partitions de $\{1, \dots, n\}$. On pose $B_0 = 1$ par convention. Alors: $\forall k \in \mathbb{N}$,

$$B_k = \frac{1}{e} \sum_{m=0}^{+\infty} \frac{m^k}{m!}$$

DEV 2