Leçon 190 : Méthodes combinatoires. Problèmes de dénombrement

Ouvrages : Gourdon (Proba), Francinou exos agreg alg. 1, Rombaldi, Perrin, Francinou oraux X-ENS 1.

I - Dénombrement et combinatoire

1) Ensembles finis et cardinaux

2) Applications et cardinaux

3) Combinatoire

a) Listes et arrangements

b) Combinaisons

4) Séries génératrices

II - Situations de dénombrement en mathématiques

1) Théorie des groupes

2) Corps finis

a) Caractéristique

b) Les carrés de $\mathbb{F}_q$

c) Polynômes irréductibles sur $\mathbb{F}_q$

DEV 1 : Nombres de Bell

DEV 2 : Polynômes irréductibles sur $\mathbb{F}_q$.

Leçon 190 : Méthodes combinatoires, problèmes de dénombrement

I - Dénombrement et combinatoire

1) Ensembles finis et cardinaux [GOU]

DEF 1 : On dit qu'un ensemble E est fini lorsqu'il est vide ou lorsqu'il existe $n \in \mathbb{N}^*$ tel que E soit en bijection avec $[\![1;n]\!]$. L'entier n est alors appelé cardinal de E. On le note $\#E$. Si $E = \emptyset$, on convient que $\#E = 0$.

PROP 2 : Soit E un ensemble fini et $A \subset E$. Alors A est fini et $\#A \leq \#E$. Si $\#A = \#E$, alors $A = E$.

PROP 3 : Soient A, B deux ensembles finis. On a :
- $\#(A \cup B) = \#A + \#B - \#A \cap B$
- $\#(A \setminus B) = \#A - \#A \cap B$, si $B \subset A$, $\#(A \setminus B) = \#A - \#B$.

PROP 4 : Soient $A_1, \dots, A_m$ des ensembles finis deux à deux disjoints i.e. pour tout $(i,j) \in [\![1;m]\!]^2$, $i \neq j \Rightarrow A_i \cap A_j = \emptyset$.
Alors $\#\left(\bigcup_{i=1}^{m} A_i\right) = \sum_{i=1}^{m} \#A_i$.

REM 5 : Si $A_1, \dots, A_m$ forment une partition d'un ensemble fini E, alors $\#E = \sum_{i=1}^{m} \#A_i$

PROP 6 : (Formule du crible de Poincaré) : Soient $A_1, \dots, A_m$ des ensembles finis. Alors on a :
$$\#\left(\bigcup_{i=1}^{m} A_i\right) = \sum_{k=1}^{m} (-1)^{k-1} \sum_{1 \leq i_1 < \dots < i_k \leq m} \#(A_{i_1} \cap \dots \cap A_{i_k})$$

EX 7 : $\forall n \geq 1$, $n = \sum_{d \mid n} \varphi(d)$

PROP 8 . Soient E, F deux ensembles finis : $\#(E \times F) = \#E \#F$

COR 9 : $\#(E^F) = (\#E)^{\#F}$, $\#\mathcal{P}(E) = 2^{\#E}$

2) Applications et cardinaux [GOU]

PROP 10 . Soient E et F deux ensembles finis, $f : E \to F$.
- Si f est injective, alors $\#E \leq \#F$
- Si f est surjective, alors $\#F \leq \#E$
- Si f est bijective, alors $\#E = \#F$.

PROP 11 : Si $f : E \to F$ est bijective, alors f est injective $\Leftrightarrow$ f est surjective $\Leftrightarrow$ f est bijective.

COR 12 (Principe des tiroirs) : Soient E, F deux ensembles finis avec $\#E > \#F$. Soit $\varphi : E \to F$, alors il existe $y \in F$ ayant au moins deux antécédents par φ dans E.

EX 13 : Si on doit ranger $n+1$ chaussettes dans n tiroirs alors un des tiroirs au moins contiendra deux chaussettes ou plus.

EX 14 : $\forall x \in \mathbb{R}$, $\forall n \in \mathbb{N}^*$, $\exists \frac{p}{q} \in \mathbb{Q}$, $1 \leq q \leq n$, $|x - \frac{p}{q}| < \frac{1}{qn}$

PROP 15 : (lemme des bergers) Soient E, F deux ensembles finis et $f : E \to F$.
On suppose que : $\exists k \in \mathbb{N}^*$, $\forall y \in F$, $\#f^{-1}(\{y\}) = k$.
Alors $\#E = k \#F$

3) Combinatoire [GOU]

DEF 16 : 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.

PROP 17 : Lorsque E est fini, il y a $(\#E)^p$ p-listes de E^p.

REM 18 : Dans une liste, l'ordre des éléments importe et un même élément peut figurer plusieurs fois dans la liste.

EX 19 : Tirage avec remise dans une urne.

DEF 20 : Soit E un ensemble fini, $n = \#E$, $p \in \mathbb{N}^*$ tel que $p \leq n$. On appelle p-arrangement de E toute p-liste de E d'éléments distincts

PROP 21 : Il y a $A_n^p = \frac{n!}{(n-p)!} = n(n-1)\cdots(n-p+1)$ p-arrangements de E.

REM 22 : Dans les arrangements, l'ordre des éléments importe mais ceux-ci sont distincts

EX 23 : Tirage dans une urne sans remise.

COR 24 : Soient E et F deux ensembles finis, $n = \#F$, $p = \#E$.
- Lorsque $p \leq n$, il y a A_n^p applications injectives de E dans F.
- L'ensemble des bijections de E est de cardinal $p!$.

PROP 25 : Soit E un ensemble fini. Alors l'ensemble $\mathcal{P}(E)$ des parties de E est fini et $\#\mathcal{P}(E) = 2^{\#E}$.

DEF 26 : Soit E un ensemble fini, $n = \#E$. Soit $p \in \mathbb{N}$. On appelle p-combinaison de E toute partie de E de cardinal p. On note $\binom{n}{p}$ le nombre de p-combinaisons.

PROP 27: Si $0 \leq p \leq n$, il y a $\binom{n}{p} = \frac{n!}{p!(n-p)!}$ p-combinaisons de E. Lorsque $p > n$, $\binom{n}{p} = 0$.

REM 28: Dans les combinaisons, les éléments sont distincts et leur ordre n'importe pas. Elles modélisent les tirages simultanées.

EX 29: Il y a $\binom{n}{p}$ fonctions strictement croissantes de $[\![1;p]\!]$ dans $[\![1;n]\!]$.

PROP 30: Soient n, p deux entiers naturels. Alors :

- Si $0 \leq p \leq n$, $\binom{n}{p} = \binom{n}{n-p}$
- Si $p, n \geq 1$, $\binom{n}{p} = \binom{n-1}{p-1} + \binom{n-1}{p}$
- Si $p, n \geq 1$, $\binom{n}{p} = \frac{n}{p}\binom{n-1}{p-1} = \frac{n-p+1}{p}\binom{n}{p-1}$
- Si $p, n \geq 0$, $\binom{n+1}{p+1} = \sum_{q=p}^{n} \binom{q}{p}$

PROP 31: Soit $n \in \mathbb{N}$, alors : $\sum_{k=0}^{n} \binom{n}{k} = 2^n$

PROP 32: Soient a, b deux éléments d'une algèbre qui commutent. Alors : $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$

PROP 33 (formule de Vandermonde) : Soient m, n et p des entiers naturels. Alors on a :

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

COR 34: $\sum_{k=0}^{n} \binom{n}{k}\binom{m}{k} = \binom{n+m}{m}$ et $\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}$.

4) Séries génératrices [GOU] [FRA]

DEF 35: Soit K un corps de caractéristique nulle. Soit $(a_n)_{n \in \mathbb{N}} \in K^{\mathbb{N}}$. La série $\sum a_n z^n$ est appelée série génératrice de (a_n).

(Nombres de Bell) DEV 1

PROP 36: Soit $n \in \mathbb{N}^*$. On pose B_n le nombre de partitions de $[\![1;n]\!]$, et $B_0 = 1$. On a pour tout $n \geq 1$,

$$B_n = \sum_{k=0}^{+\infty} \frac{k^n}{k!}$$

DEF 37: Soit $n \in \mathbb{N}^*$. On appelle dérangement toute permutation de $\mathfrak{S}_n$ n'ayant aucun point fixe. On note D_n l'ensemble des dérangements de $\mathfrak{S}_n$.

PROP 38: On a pour tout $n \in \mathbb{N}$, $n! = \sum_{k=0}^{n} \binom{n}{k} d_k$ où $d_n = \# D_n$.
On montre que $\sum_{n=0}^{+\infty} \frac{D_n}{n!} x^n = \sum_{n=0}^{+\infty} \left(\sum_{k=0}^{n} \frac{(-1)^k}{k!} \right) x^n$ d'où

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

II - Situations de dénombrement en mathématiques

1) Théorie des groupes [ROM]

Soit G un groupe fini et E un ensemble fini.

THM 39 (Lagrange) : Soit H un sous-groupe de G. Alors $\#G = \#H\,[G:H]$ où $[G:H] = \#(G/H)$ $(= \frac{\#G}{\#H})$

COR 40: $\forall g \in G$, $g^{\#G} = e_G$.

THM 41: Soit φ un morphisme de groupes de G dans G'. Alors $\#G = \#\ker(\varphi)\,\#\mathrm{Im}(\varphi)$.

DEF 42: On dit que G opère (ou agit) sur E lorsqu'on a une application $(g, x) \in G \times E \mapsto g \cdot x \in E$ telle que

$$\begin{cases} \forall x \in E, \ e_G \cdot x = x \\ \forall g, g' \in G, \ \forall x \in E, \ g \cdot (g' \cdot x) = gg' \cdot x \end{cases}$$

PROP 43: La donnée d'une action de groupes est équivalente à la donnée d'un morphisme de G dans $\mathfrak{S}_E$.

DEF 44: Pour $x \in E$, on définit l'orbite de x sous l'action de G : $\mathrm{Orb}(x) = \{g \cdot x \mid g \in G\}$

REM 45: L'ensemble des orbites forme une partition de E.

DEF 46: Pour $x \in E$, on définit le stabilisateur de x sous l'action de G par $\mathrm{Stab}(x) = \{g \in G \mid g \cdot x = x\}$, c'est un sous-groupe de G.
On définit aussi l'ensemble des points fixes de l'action : $\forall g \in G$, $\mathrm{Fix}(g) = \{x \in E \mid g \cdot x = x\}$.

THM 47: Soit $x \in E$. Il y a une bijection d'ensembles :

$$G/\mathrm{Stab}(x) \longrightarrow \mathrm{Orb}(x)$$
$$\bar{g} \longmapsto g \cdot x$$

THM 48: Soit $(G, \cdot)$ un groupe fini opérant sur E fini. En notant $\mathrm{Orb}(x_1), \dots, \mathrm{Orb}(x_r)$ toutes les orbites deux à deux distinctes, on a

$$\#E = \sum_{i=1}^{r} \#\mathrm{Orb}(x_i) = \sum_{i=1}^{r} \frac{\#G}{\#\mathrm{Stab}(x_i)}.$$

DEF 49 : Si $p \geq 2$ est un nombre premier, on appelle p-groupe tout groupe de cardinal p^α où $\alpha \in \mathbb{N}^*$.

COR 50 : Si $p \geq 2$ est un nombre premier et $(G, \cdot)$ est un p-groupe opérant sur un ensemble fini E, on a alors
$$\# E^G \equiv \# E \pmod p.$$

THM 51 : Pour tout nombre premier p, le centre d'un p-groupe n'est pas réduit à $\{e_G\}$.

2) Corps finis

~~a) Caractéristique~~ [PER]

DEF 52 : Soit K un corps. On appelle sous-corps premier de K le plus petit sous-corps de K (contenant 1).

PROP 53 : Soit $\varphi : \mathbb{Z} \to K$, $n \mapsto n \cdot 1$. φ est un morphisme d'anneaux. $\ker(\varphi)$ est un idéal de $\mathbb{Z}$, donc $\ker(\varphi) = p\mathbb{Z}$ et $\mathbb{Z}/p\mathbb{Z} \simeq \mathrm{Im}(\varphi) \subset K$ est intègre donc $p\mathbb{Z}$ est un idéal premier. Donc $p = 0$ ou p est un nombre premier.

DEF 54 : Le nombre p, générateur de $\ker(\varphi)$ est appelé la caractéristique du corps K.

REM 55 : • Si $car(K) = 0$, $\varphi(\mathbb{Z}) \subset K$ et $\varphi(\mathbb{Z}) \simeq \mathbb{Z}$, K est donc infini. Le corps des fractions $\mathbb{Q}$ est le sous-corps premier de K.
• Si K est fini, $car(K) = p > 0$. Le sous-corps premier de K est $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

PROP 56. Si K est fini, K est un $\mathbb{F}_p$-espace vectoriel donc : $\exists n \in \mathbb{N}^*$, $\# K = q = p^n$.

THM 57 : Il existe un corps K à $q = p^n$ éléments. C'est le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$.
En particulier, K est unique à isomorphisme près. On le note $\mathbb{F}_q$.

~~THM 58~~ (Wedderburn) Tout corps fini est commutatif.

b) Les carrés de $\mathbb{F}_q$ [PER]

DEF 58 : On pose $\mathbb{F}_q^2 = \{x \in \mathbb{F}_q \mid \exists y \in \mathbb{F}_q, x = y^2\}$ et $(\mathbb{F}_q^*)^2 = \mathbb{F}_q^2 \cap \mathbb{F}_q^*$.

PROP 59. Soit $q = p^n$.
• Si $p = 2$, $\mathbb{F}_q^2 = \mathbb{F}_q$
• Si $p > 2$, $\# \mathbb{F}_q^2 = \frac{q+1}{2}$ et $\#(\mathbb{F}_q^*)^2 = \frac{q-1}{2}$

PROP 60 : On suppose $p > 2$. Alors : $x \in (\mathbb{F}_q^*)^2 \iff x^{\frac{q-1}{2}} = 2$

COR 61 : Soit p premier, $p > 2$, $q = p^n$, $n \in \mathbb{N}^*$.
$-1 \in (\mathbb{F}_q^*)^2 \iff q \equiv 1 \mod 4$.

c) Polynômes irréductibles sur $\mathbb{F}_q$ [FRA 1]

DEF 62 : On définit la fonction de Möbius par
$$\mu : \mathbb{N}^* \to \{0; -1; 1\}, \quad n \mapsto \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n \text{ contient un facteur carré} \\ -1 & \text{sinon} \end{cases}$$

DEV 2

PROP 63 : On a que $\sum_{d|n} \mu(d) = 0$ pour tout $n \geq 2$.

PROP 64 : Soit $g : n \in \mathbb{N}^* \mapsto \sum_{d|n} f(d)$ avec $f : \mathbb{N}^* \to \mathbb{R}$.
Alors : $\forall n \geq 1$, $f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right)$

THM 65 : Soit $n \in \mathbb{N}^*$, $q = p^m$, $m \in \mathbb{N}^*$, p un nombre premier. On note $A(n, q)$ l'ensemble des polynômes unitaires irréductibles de degré n sur $\mathbb{F}_q$. Alors :
$$X^{q^n} - X = \prod_{d|n} \prod_{P \in A(d,q)} P(X)$$

THM 66 : Si $I(n,q) = \# A(n,q)$, alors $I(n,q) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d$ et $I(n,q) \underset{n \to +\infty}{\sim} \frac{q^n}{n}$.