190 Méthodes combinatoires, problèmes de dénombrement

I Théorie des ensembles et combinatoire

1) Définitions

déf 1. On dit que E est un ensemble fini et de cardinal n si
- $n=0$ et $E=\emptyset$
- $n>0$ et s'il existe une bijection de E dans $[\![1,n]\!]$

on note card(E) ou $|E|$ son cardinal

ex 2 : $\{3,6,9,12,15\}$ est fini de cardinal 5 mais $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{N}$ ne sont pas finis

déf 3 : On définit $\cup$ l'union, $\cap$ l'intersection de la manière suivante.
- $A\cap B=\{x \mid x\in A \text{ et } x\in B\}$
- $A\cup B=\{x\mid x\in A \text{ ou } x\in B\}$

Soit I une partie de $\mathbb{N}$ et $(A_i)_{i\in\mathbb{N}}$ une famille d'ensemble finis
On définit. - $\bigcup_{i\in I} A_i=\{x \mid \exists i\in I, x\in A_i\}$
- $\bigcap_{i\in I} A_i=\{x\mid \forall i\in I, x\in A_i\}$

déf 4 : On définit $A\times B=\{(x,y)\mid x\in A \text{ et } y\in B\}$.
Soit $A_1 A_2 \dots A_p$ des ensembles finis, on définit
$A_1\times A_2\times\dots\times A_p=\{x=(x_1,\dots x_p)\mid \forall i\in[\![1,p]\!], x_i\in A_i\}$

2) Premières propriétés

Prop 5 : Soit A, B des ensembles finis, alors $|A\cup B|=|A|+|B|-|A\cap B|$

Prop 6 : On en déduit alors la formule du crible. Soit $(A_i)_{1\leq i\leq n}$ une famille d'ensemble fini, alors

$$|\bigcup_{1\leq i\leq n} A_i| = \sum_{i=1}^{n}|E_i| - \sum_{1\leq i<j\leq n}|E_i\cap E_j| + \dots (-1)^{n-1}|\bigcap_{1\leq i\leq n} E_i|$$

Rq 7 Pour A et B disjoint, on retrouve $|A\cup B|=|A|+|B|$

prop 8 : Soit A, B deux ensembles finis, alors $|A\times B|=|A|.|B|$.

prop 9. Soit $A_1 \dots A_p$ des ensembles finis, alors,
$|A_1\times A_2\times\dots A_p| = \prod_{i=1}^{p}|A_i|$

App 10 : le cardinal de l'ensemble des applications d'un ensemble X à n éléments dans un ensemble Y à p éléments est p^n

App 11 : voici deux méthodes pour dénombrer le cardinal de l'espace projectif $P(E)$ pour E un $\mathbb{K}$ ev avec $|E|=n$ et $|\mathbb{K}|=p$
- $E=P(E)\sqcup\{0\}$, donc $|P(E)|=p^n-1$.
- $P(E)=(1,e_2 \dots e_n)\sqcup(1,1,e_3,e_4 \dots e_n)\sqcup\dots\sqcup(1,1 \dots 1)$

donc $|P(E)|=1+p+\dots+p^{n-1}=p^n-1$.

3) Arrangements

déf 12 : Soit E un ensemble à n éléments. Soit $p\in\mathbb{N}$, $p\leq n$. un arrangement de E à p éléments est un p-uplet $(e_1,\dots e_p)$ d'éléments de E distinct deux à deux

Rq 13. Un arrangement est aussi une application injective de $[\![1,p]\!]$ dans $[\![1,n]\!]$

Prop 14 : Le nombre d'arrangement à p éléments dans un ensemble E de cardinal n est $A_n^p=\frac{n!}{(n-p)!}$.

déf-Prop 15. On appel permutation un arrangement avec $p=n$. A_n^n, le nombre de permutation d'un ensemble à n éléments est $n!$

App 16 : Le nombre de tirages de p boules sans remise dans un ensemble à n boules est $A_n^p=\frac{n!}{(n-p)!}$

App 17 : Alphabet de Braille : Un caractère est représenté avec 6 points o ou • ce qui donne $2^6=64$ possibilités, ce qui permet d'encoder les chiffres, les lettres et les signes de ponctuation

4) Combinaisons

déf 18 : Toute partie à p éléments d'un ensemble à n éléments, $p\leq n$ est appelée combinaison. C'est une application de $[\![1,p]\!]$ dans $[\![1,n]\!]$. On note son cardinal $\binom{n}{p}$

prop 19 : - $A_n^p=p!\binom{n}{p}$ donc en particulier $\binom{n}{p}=\frac{n!}{p!(n-p)!}$
- $\binom{n}{p}=\binom{n}{p-1}+\binom{n-1}{p-1}$
- $\binom{n}{p}=\frac{n}{p}\binom{n-1}{p-1}$

Rq 20. On représente souvent $\binom{n}{p}$ à l'aide du triangle de Pascal.

n\p	0	1	2	3	4
0	1				
1	1	1			
2	1	2	1		
3	1	3	3	1	
4	1	4	6	4	1

Prop 21 : $\forall a,b \in \mathbb{C}, (a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$.

App 22 : Le nombre d_n de permutations sans points fixes est $d_n = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}$

App 24 : calcul de $S_{n,p} = \sum_{k=1}^{n} k^p$. $(n+1)^p = 1 + \sum_{k=0}^{p} \binom{p}{k} S_{p,k}$.

En particulier : $S_{n,1} = \frac{n(n+1)}{2}$, $S_{n,2} = \frac{n(n+1)(2n+1)}{6}$

Rq 23 : La probabilité de tirer une permutation sans points fixes converge vers $(1-\frac{1}{e})$

Prop 25 : Lemme des bergers : soit A et B deux ensembles finis, φ une application de A dans B. Si $\forall x \in B, |\varphi^{-1}(x)| = n$, alors $|A| = n|B|$.

App 20 Le nombre de surjections d'un ensemble X à $n+1$ éléments sur Y un ensemble à n élément est $\frac{n}{2}(n+1)!$

II Fonction Möbius, séries génératrices. Exemples et Applications

1) Fonction Möbius

def 26 On définit la fonction Möbius de la manière suivante :

* $\mu(1) = 1$
* $\mu(n) = 0$ si n contient un facteur premier au carré
* $\mu(p_1 p_2 \dots p_k) = (-1)^k$ si les p_i sont premiers et distincts deux à deux.

prop 27 Si $m \wedge n = 1$ alors $\mu(mn) = \mu(m)\mu(n)$. On dit que μ est multiplicative.

Ex 28 : $\mu(2) = -1$, $\mu(4) = 0 \neq \mu(2)^2$, $\mu(3) = -1$, $\mu(6) = \mu(2.3) = \mu(2)\mu(3) = 1$.

App 29 : Si $n > 1$ et k est le nombre de facteurs premiers distincts de n, alors
$$\sum_{d|n} |\mu(d)| = 2^k$$

Thm 30 : Si $g(n) = \sum_{d|n} f(n)$, alors $f(n) = \sum_{d|n} \mu(\frac{n}{d}) g(d)$.
cette formule est appelée formule d'inversion

2) Applications de la formule d'inversion

* Indicatrice d'Euler

def 31 On définit l'indicatrice d'Euler $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$ où $\mathbb{Z}/n\mathbb{Z}^*$ désigne le groupe des inversibles de $\mathbb{Z}/n\mathbb{Z}$

App 32 : $n = \sum_{d|n} \varphi(d)$ et $\varphi(n) = \sum_{d|n} \mu(\frac{n}{d}) d$

* Polynômes irréductibles sur un corps fini

def 32 On désigne par $\mathbb{F}_q$ le corps fini à q éléments

Thm 33 : Soit $A(n,q)$ l'ensemble des polynômes irréductibles de degré n sur $\mathbb{F}_q[X]$. En notant $I(n,q) = |A(n,q)|$ leur nombre, alors

- $X^{q^n} - X = \prod_{d|n} \prod_{P \in A(d,q)} P$
- $I(n,q) = \frac{1}{n} \sum_{d|n} \mu(\frac{n}{d}) q^d$
- $I(n,q) \underset{n \to +\infty}{\sim} \frac{q^n}{n}$

DEV 1

* Probabilité que deux nombres soient premiers entre eux

def 34 : On note π_n la probabilité que deux nombres choisis uniformément dans $[\![1,n]\!]$ soient premiers entre eux.

Thm 35 : $\lim_{n \to +\infty} \pi_n = \frac{6}{\pi^2}$ DEV 2

3) Séries génératrices

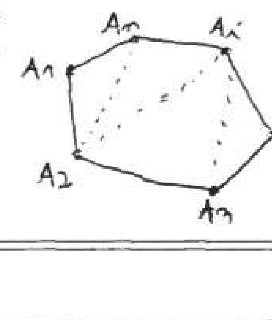
Def 35 Soit $(a_n)_{n\in\mathbb{N}}$ une suite de réels. On définit la série génératrice de $(a_n)_{n\in\mathbb{N}}$ comme la série formelle $\sum_{n\in\mathbb{N}} a_n X^n \in \mathbb{R}[X]$

ex 36 : e^u est la série formelle $e^u = \sum_{n \geq 0} \frac{u^n}{n!}$

App 37 : Soient $a_1, \dots a_n \in E$ avec E un ensemble muni d'une loi interne non associative. On note C_n le n-ième nombre de Catalan, le nombre de valeurs différentes que peut prendre le produit $a_1 \dots a_n$. Alors $C_n = \binom{2n-2}{n-1}/n$

App 38 : Soit A_n le nombre de triangulations d'un polygône convexe $A_1 \dots A_n$ par $n-3$ diagonales non sécantes en $n-2$ triangles. Alors

$$A_n = \frac{1}{n-1} \cdot \binom{2n-4}{n-2} = C_{n-1}$$



4) Séries génératrices de Dirichlet.

déf 39 : Une série de Dirichlet est une série de la forme
$$F(s)=\sum_{n=1}^{+\infty}\frac{a_n}{n^s} \quad \text{avec } s\in\mathbb{K},\ \mathbb{K}=\mathbb{R} \text{ ou } \mathbb{C} \text{ et } (a_n) \text{ une suite donnée}$$

Prop 40 : Si $\sum_{n=1}^{+\infty}\frac{a_n}{n^s}=0$, alors la suite $(a_n)_{n\in\mathbb{N}}$ est nulle

Cor 41 : Si $\sum_{n=1}^{+\infty}\frac{a_n}{n^s}=\sum_{n=1}^{+\infty}\frac{b_n}{n^s}$ alors les deux suites $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$ sont les mêmes

déf 42 : On définit la fonction Zêta de Riemann
$$\zeta(s)=\sum_{n=1}^{+\infty}\frac{1}{n^s} \quad \text{avec } Re(s)>1$$

Thm 43 : Soient $G(s)=\sum_{n=1}^{+\infty}\frac{a_n}{n^s}$ et $F(s)=\sum_{n=1}^{+\infty}\frac{b_n}{n^s}$ deux séries de Dirichlet.

Si elles convergent absolument, alors $G(s)F(s)=\sum_{n=1}^{+\infty}\frac{\gamma_n}{n^s}$ noté

avec $\gamma_n=\sum_{uv=n}a_u b_v=\sum_{d|n}a_d b_{\frac{n}{d}}=\sum_{d|n}a_{\frac{n}{d}}b_d$

Thm 44 : - $\frac{1}{\zeta(s)}=\sum_{n=1}^{+\infty}\frac{\mu(n)}{n^s}$ pour $Re(s)>1$

- $\frac{\zeta(s-1)}{\zeta(s)}=\sum_{n=1}^{+\infty}\frac{\varphi(n)}{n^s}$ avec $Re(s)>2$

App 45 : On retrouve $\varphi(n)=\sum_{d|n}\mu\left(\frac{n}{d}\right)d$

III Applications en Algèbre

1) Action de groupe

déf 46. Soit G un groupe multiplicatif d'élément unité e. Soit E un ensemble non vide. On dit que E opère à gauche sur E s'il existe une application
$$G\times E\longrightarrow E$$
$$(g,x)\longmapsto g.x$$
telle que
- $\forall (g_1,g_2)\in G\times G$, $\forall x\in E$, $(g_1.g_2)x=g_1.(g_2.x)$
- $\forall x\in E$, $e.x=x$

déf 47 : - On définit pour tout $x\in E$ le stabilisateur $G_x=\{g\in G,\ g.x=x\}$
- On définit pour tout $x\in E$ l'orbite $\Omega_x=\{g.x,\ g\in G\}$

ex 48. Si G opère sur G par translation à gauche, alors $\forall x\in G$:
- $G_x=\{e\}$
- $\Omega_x=G$

Prop 49 : Formule des classes. Soit Θ une famille de représentants des G-orbites distinctes.
- $|E|=\sum_{x\in\Theta}|\Omega_x|$
- $|\Omega_x|=[G:G_x]$

Th 50 : Formule de Burnside. Soit $Fix(g)=\{x\in X,\ g.x=x\}$ et Θ défini ci-dessus.
alors $|\Theta|=\frac{1}{|G|}\sum_{g\in G}|Fix(g)|$

App 51 : il y a 8 manières différentes de colorier un collier de 5 perles avec 2 couleurs différentes

2) Dénombrements de quelques structures algébriques

Soit $\mathbb{K}$ un corps commutatif de cardinal q

Th 52 : - $|GL_n(\mathbb{K})|=(q^n-1)(q^n-q)\dots(q^n-q^{n-1})$
- $|SL_n(\mathbb{K})|=(q^n-1)\dots(q^n-q^{n-1})/q$
- $|SO(\mathbb{F}_p)|=\begin{cases}2 & \text{si } p=2\\ p-1 & \text{si } p\equiv 1[4]\\ p+1 & \text{si } p\equiv 3[4]\end{cases}$ p premier
- $|\{A\in GL_n(\mathbb{F}_q),\ A^2=I_n\}|=\sum_{p=0}^{n}\frac{|GL_n(\mathbb{F}_p)|}{|GL_p(\mathbb{F}_p)||GL_{n-p}(\mathbb{F}_q)|}$

- Il y a 28 sous-espaces vectoriels de $(\mathbb{F}_3)^3$
- Il y a $\frac{(2^n-1)(2^{n-1}-1)\dots(2^{n-k+1}-1)}{(2^k-1)(2^{k-1}-1)\dots(2-1)}$ sous espaces vectoriels de dimension k de $(\mathbb{F}_2)^n$

- Soit q une puissance d'un nombre premier, le nombre de matrices diagonalisables de $M_n(\mathbb{F}_q)$ est :
$$\sum_{n_1+\dots+n_q=n}\frac{|GL_n(q)|}{\prod_{i=1}^{q}(GL_{n_i}(q))}$$

Références : - An introduction to the theory of Numbers E.M Wright
- FGN algèbre tome 1
- Élément de théorie des groupes (Calais)
- Mathématique pour le CAPES (Biasi)
- FG Essence de Mathématique pour l'agrégation