Leçon N° 190 : Méthodes combinatoires, problèmes de dénombrement.

Dans toute cette leçon, E et F sont des ensembles finis. $\mathbb{K}$ est un corps de caractéristique nulle et G est un groupe.

I) Dénombrement

Dans toute cette partie : $n \in \mathbb{N}^*$ et $k \in [\![0, n]\!]$.

[Gou]

1) Les classiques

Proposition 1 : 1) E et F sont en bijection ssi $|E| = |F|$
2) Il existe une injection de E vers F ssi $|E| \leq |F|$.
3) Il existe une surjection de E vers F ssi $|E| \geq |F|$

Corollaire 2 : (Principe des tiroirs) Si $|E| > |F|$ et si $\varphi : E \to F$, alors $\exists y \in F$ ayant au moins deux antécédents par φ dans E. (Cf annexe 1)

[Gou]

Application 3 : $\forall x \in \mathbb{R}$, $\exists p/q \in \mathbb{Q}$ avec $q \in [\![1, n]\!]$ tel que $|x - p/q| < \frac{1}{qn}$

Proposition 4 : (Formule du crible de Poincaré) Soient $A_1, \dots, A_n$ des ensembles finis, on a $\left|\bigcup_{i=1}^n A_i\right| = \sum_{j=1}^n (-1)^{j-1} \sum_{1 \leq i_1 < \dots < i_j \leq n} |A_{i_1} \cap \dots \cap A_{i_j}|$
(Cf annexe 2)

Proposition 5 : Soient $A_1, \dots, A_n$ des ensembles finis $\left|\prod_{i=1}^n A_i\right| = \prod_{i=1}^n |A_i|$

Définition - Proposition 6 : On appelle k-arrangement de E tout k-uplet de E d'éléments distincts. Si $|E| = n$, alors le nombre de k-arrangements de E est $A_n^k = \frac{n!}{(n-k)!}$

Proposition 7 : 1) Le nombre d'applications de E vers F vaut : $|F^E| = |F|^{|E|}$
2) Si $|E| = k$ et $|F| = n$, le nombre d'applications injectives de E vers F vaut A_n^k

Corollaire 8 : Le nombre de parties de E vaut : $|\mathcal{P}(E)| = 2^{|E|}$

Corollaire 9 : Si $|E| = n$, alors le nombre de permutations de E vaut : $|\mathfrak{S}_E| = n!$

Proposition - définition 10 : Si $|E| = n$ et si $(i_1, \dots, i_k) \in \mathbb{N}^k$ tel que $\sum_{j=1}^k i_j = n$, alors le nombre de partitions ordonnées $(A_1, \dots, A_p)$ de E tel que $\forall j \in [\![1, k]\!]$, $|A_j| = i_j$ vaut $\binom{n}{i_1, \dots, i_k} = \frac{n!}{i_1! \dots i_k!}$

Notation 11 : (binôme de Newton) $\binom{n}{k} := \binom{n}{n-k}$

Proposition 12 : $\forall (a_1, \dots, a_k) \in A^k$ où $(A, +, \times)$ est un anneau commutatif, $\left(\sum_{i=1}^k a_i\right)^n = \sum_{i_1 + \dots + i_k = n} \binom{n}{i_1, \dots, i_k} a_1^{i_1} \times \dots \times a_k^{i_k}$

Application 13 : Si $E \neq \emptyset$, il y a autant de sous parties de E de cardinal pair que de cardinal impair.

2) Un peu de fantaisie ...

[FGN]

Exemple 14 : Le nombre a_n de manières de recouvrir un damier de dimension $2 \times n$ avec des pièces de dimension 1×2 vaut :
$a_n = \frac{1}{\sqrt{5}} \left(\phi^{n+1} - \left(-\frac{1}{\phi}\right)^{n+1}\right)$ où $\phi = \frac{1+\sqrt{5}}{2}$ est le nombre d'or (Cf annexe 3).

Proposition 15 : Soit $q = p^n$ où p est un nombre premier.
1) $\#GL_n(\mathbb{F}_q) = (q^n - 1)(q^n - q) \dots (q^n - q^{n-1})$
2) $\#SL_n(\mathbb{F}_q) = \frac{\#GL_n(\mathbb{F}_q)}{q-1}$.

Proposition 16 : Si $|E| = n$. Soit $\mathcal{R}$ une relation d'équivalence sur E avec k classes. On note $m = \#\{(x, y) \in E^2 \text{ tq } x \mathcal{R} y\}$, alors $n^2 \leq k\, m$.

3) Probabilités sur un ensemble fini (ou pas)

[Gou]

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

Affirmation 17 : Si Ω est fini et si $\mathcal{A} = \mathcal{P}(\Omega)$. En situation d'équiprobabilité : $\forall A \in \mathcal{A}$, $P(A) = \frac{|A|}{|\Omega|}$

Exemple 18 : On tire 5 cartes dans un jeu de 52 cartes au hasard.
La probabilité d'avoir une paire est : $\frac{13 \times \binom{4}{2} \times \binom{12}{3} \times 4 \times 4 \times 4}{\binom{52}{5}} \approx 0,42$.

Proposition 19 : Soit $p \in]0, 1[$. Si on réalise successivement n épreuves de Bernoulli de paramètre p de manière indépendante, la variable aléatoire X qui compte le nombre de succès suit une $\mathcal{B}(n, p)$, c'est-à-dire que $P(X = k) = \binom{n}{k} p^k (1-p)^{n-k}$.

Dans les énoncés qui suivent, $n \in \mathbb{N}^*$ et $k \in \mathbb{N}^*$.

Lemme 20 : On note $c_{n,k} := \max_{n_1 + \dots + n_k = n} \binom{n}{n_1, \dots, n_k}$

On effectue la division euclidienne de n par k : $\exists ! (\ell, r) \in \mathbb{N} \times [\![0, k-1]\!]$ tq $n = k\ell + r$
Alors $c_{n,k} = \frac{n!}{(\ell!)^{k-r} ((\ell+1)!)^r}$

Lemme 21 : La suite $\left(\frac{c_{n,k}}{k^n}\right)_{n \in \mathbb{N}^*}$ est décroissante.

Théorème 22 : Les états de la marche aléatoire symétrique sur $\mathbb{Z}^k$ sont récurrents ssi $k \leq 2$.

[GGD]

Dev 1.

II) Séries formelles

1) Définitions

[Rom] **Définition 23 :** On appelle série formelle à une indéterminée à coefficient dans $\mathbb{K}$ toute suite $(a_n)_{n\in\mathbb{N}} \in \mathbb{K}^{\mathbb{N}}$ que l'on note plutôt $\sum_{n\in\mathbb{N}} a_n X^n$.
On note $\mathbb{K}[[X]]$ l'ensemble des séries formelles sur $\mathbb{K}$.
On définit une addition et une multiplication sur $\mathbb{K}[[X]]$:
- $\left(\sum_{n\in\mathbb{N}} a_n X^n\right) + \left(\sum_{n\in\mathbb{N}} b_n X^n\right) := \sum_{n\in\mathbb{N}} (a_n + b_n) X^n$
- $\left(\sum_{n\in\mathbb{N}} a_n X^n\right)\left(\sum_{n\in\mathbb{N}} b_n X^n\right) := \sum_{n\in\mathbb{N}} c_n X^n$ où $\forall n\in\mathbb{N}$, $c_n = \sum_{k=0}^{n} a_k b_{n-k}$.

Proposition 24 : Si $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, on considère la série entière $\sum a_n z^n$.
$\exists R \in \mathbb{R}_+ \cup \{+\infty\}$ tel que le domaine de convergence de la série D soit tel que $B(0,R) \subset D \subset B_f(0,R)$.
La série entière converge normalement sur tout compact inclus dans $B(0,R)$.

Proposition 25 : La somme de la série entière $\sum a_n z^n$ est une fonction $\mathcal{C}^\infty$ sur $B(0,R)$ et sa dérivée vaut $\forall z \in B(0,R)$, $\sum_{n=0}^{+\infty} (n+1) a_{n+1} z^n$.

[Cou] ### 2) Séries formelles usuelles

Définition 26 : Soit $(a_n)_{n\in\mathbb{N}} \in \mathbb{N}^{\mathbb{N}}$
1) La série génératrice ordinaire de (a_n) est $\sum_{n\geq 0} a_n z^n$
2) La série génératrice exponentielle de (a_n) est $\sum_{n\geq 0} \frac{a_n z^n}{n!}$

Proposition 27 : La série formelle $\sum_{n\geq 0} X^n$ vérifie $\left(\sum_{n\geq 0} X^n\right)(1-X) = 1$.

[Cou] ### 3) Applications

Application 28 : Soit $n \in \mathbb{N}^*$. On note D_n le nombre de permutations $\sigma \in \mathfrak{S}_n$ sans points fixes avec comme convention $D_0 = 1$
Par la série génératrice exponentielle de $(D_n)_{n\in\mathbb{N}}$, on a que $D_n = \sum_{k=0}^{n} \frac{(-1)^k n!}{k!}$

Application 29 : Soit $n \in \mathbb{N}^*$. Notons C_n le nombre de façons de parenthéser un produit de $n+1$ facteurs avec la convention $C_0 = 1$.
Par la série génératrice ordinaire de $(C_n)_{n\in\mathbb{N}}$, on a que $C_n = \frac{1}{n+1}\binom{2n}{n}$

Application 30 : Soit $n \in \mathbb{N}^*$. On note B_n le nombre de partitions de $[\![1,n]\!]$ avec par convention $B_0 = 1$.
Par la série génératrice exponentielle de $(B_n)_{n\in\mathbb{N}}$, on a que $B_n = \frac{1}{e}\sum_{k=0}^{+\infty} \frac{k^n}{k!}$

III) Inversion de Möbius

[Rom]

1) Fonction de Möbius

Définition 31 : Soit $n \in \mathbb{N}$. Si $n \geq 2$, on note $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ sa décomposition en produits de facteurs premiers.
On définit la fonction de Möbius par $\mu(n) = \begin{cases} 1 \text{ si } n = 1 \\ (-1)^r \text{ si } n \text{ est sans facteurs premiers carrés} \\ 0 \text{ sinon.} \end{cases}$

Exemple 32 : $\mu(1) = 1$, $\mu(2) = -1$, $\mu(3) = -1$, $\mu(4) = 0$, $\mu(5) = -1$, $\mu(6) = 1$, ...

Définition 33 : Soient $(u,v) \in (\mathbb{R}^{\mathbb{N}^*})^2$, on définit le produit de convolution de Dirichlet de u et v comme $u * v : n \mapsto \sum_{d|n} u(d)\, v\left(\frac{n}{d}\right)$.

Proposition 34 : L'ensemble $\mathbb{R}^{\mathbb{N}^*}$ muni de $+$ et $*$ est un anneau commutatif unitaire et les éléments inversibles sont les suites telles que $u(1) \neq 0$

Exemple 35 : 1) La fonction de Möbius μ est inversible
2) La fonction indicatrice d'Euler φ est inversible

2) Inversion de Möbius

Lemme 36 : On note e le neutre de $\mathbb{R}^{\mathbb{N}^*}$ pour la loi $*$ et $\mathbb{1}$ la suite constante égale à 1. Alors $\mu * \mathbb{1} = e$

Théorème 37 : (formule d'inversion de Möbius) : $\forall (u,v) \in (\mathbb{R}^{\mathbb{N}^*})^2$,
il y a équivalence entre : i) $\forall n \in \mathbb{N}^*$, $u(n) = \sum_{d|n} v(d)$
ii) $\forall n \in \mathbb{N}^*$, $v(n) = \sum_{d|n} \mu(d)\, u\left(\frac{n}{d}\right)$,

3) Applications

Notation 38 : Pour $n \in \mathbb{N}^*$, on se place sur $([\![1,n]\!]^2, \mathcal{P}([\![1,n]\!]^2), P)$ où P est la mesure de probabilité uniforme sur $[\![1,n]\!]^2$.
On note $C_n = \{(a,b) \in [\![1,n]\!]^2,\ a \wedge b = 1\}$.

Lemme 39 : 1) $\forall n \geq 2$, $P(C_n) = \frac{1}{n^2}\left(2\sum_{k=1}^{n} \varphi(k) - 1\right)$
2) $\forall n \geq 2$, $P(C_n) = \frac{1}{n^2}\sum_{d=1}^{n} \mu(d)\left\lfloor \frac{n}{d} \right\rfloor^2$

3) $P(n) \xrightarrow[n\to+\infty]{} \sum_{q=1}^{+\infty} \frac{\mu(q)}{q^2}$

Théorème 40 : $P(n) \xrightarrow[n\to+\infty]{} \frac{6}{\pi^2}$.

Notation 41 : Soient $n, q \in \mathbb{N}^*$, p un nombre premier et $q := p^n$.
On note $A(n,q)$ l'ensemble des polynômes de $\mathbb{F}_q[X]$ irréductibles et unitaires de degré n et $I(n,q) := \# A(n,q)$.

Lemme 42 : $X^{q^n} - X = \prod_{d \mid n} \prod_{P \in A(d,q)} P \quad \forall n \in \mathbb{N}^*$.

Théorème 43 : $\forall n \in \mathbb{N}^* \quad I(n,q) = \frac{1}{n} \sum_{d \mid n} \mu\left(\frac{n}{d}\right) q^d$

Corollaire 44 : $\forall n \in \mathbb{N}^*, \ I(n,q) \geq 1$ et $I(n,q) \underset{n\to+\infty}{\sim} \frac{q^n}{n}$.

Dev 2.

II) Groupes et combinatoire

1) Actions de groupes

Définition 45 : Une action de G sur E est une application $G \times E \to E$, $(g,x) \mapsto g \cdot x$ telle que : 1) $\forall x \in E, \ 1_G \cdot x = x$
2) $\forall g, g' \in G, \forall x \in E, \ g \cdot (g' \cdot x) = (gg') \cdot x$.

Remarque 46 : Il revient au même de se donner un morphisme de groupes $\varphi : G \to \mathfrak{S}(E)$ en posant $g \cdot x = \varphi(g)(x)$.

Exemple 47 : G agit sur lui-même par conjugaison : $G \times G \to G$, $(g,h) \mapsto ghg^{-1}$

Lemme 48 : Si G opère sur E. La relation sur E définie par $x \sim y$ lorsque $\exists g \in G, \ y = g \cdot x$ est une relation d'équivalence.

Définition 49 : Si G opère sur E. Soit $x \in E$.
L'ensemble $Ox = \{g \cdot x, g \in G\} \subset E$ est appelé orbite de x sous G.
C'est la classe d'équivalence de x pour la relation d'équivalence définie ci-dessus.

Définition - Proposition 50 : Si G opère sur E. Pour $x \in E$, l'ensemble Stab_x est l'ensemble $\{g \in G, \ g \cdot x = x\}$ est appelé stabilisateur de x.
On a $|\mathrm{Stab}_x| = |\mathrm{Stab}_y|$ pour $x \sim y$.

2) Équation aux classes

Proposition 51 : (Équation aux classes) Si G est fini et opère sur E. On note Ω l'ensemble des orbites de E :
$|E| = \sum_{\omega \in \Omega} |\omega| = \sum_{\omega \in \Omega} \frac{|G|}{|\mathrm{Stab}_\omega|}$

Lemme 52 : (Cayley) Si G est fini de cardinal n, alors G est isomorphe à un sous-groupe de $\mathfrak{S}_n$

Définition 53 : Soit p premier. Si G est fini avec $|G| = p^m q$ et $p \wedge q = 1$ et $m \geq 0$ un p-Sylow de G est un sous-groupe de G de cardinal p^m.

Lemme 54 : Dans ces conditions, si H est un sous groupe de G et si G admet un p-Sylow S. Alors $\exists g \in G, \ gSg^{-1} \cap H$ est un p-Sylow de H.

Théorème 55 : (Sylow) Sous les mêmes conditions
1) $\exists$ des p-Sylows de G et tout p-sous groupe de G est contenu dans un p-Sylow
2) Le conjugué d'un p-Sylow de G est un p-Sylow de G et ils sont tous conjugués
3) Si N_p est le nombre de p-Sylows de G, alors $N_p \equiv 1 [p]$ et $N_p \mid q$.

Notation 56 : (Symbole de Legendre) Soient p premier et $a \in \mathbb{F}_p$.
On note $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} = \begin{cases} 1 & \text{si } a \in (\mathbb{F}_p^*)^2 \\ 0 & \text{si } a = 0 \\ -1 & \text{sinon.} \end{cases}$

Lemme 57 : Si p premier $\neq 2$ et $a \in \mathbb{F}_p^*$, $|\{x \in \mathbb{F}_p, \ ax^2 = 1\}| = 1 + \left(\frac{a}{p}\right)$

Théorème 58 : (Loi de réciprocité quadratique) Soient p et q deux nombres premiers impairs distincts. Alors $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$

3) Formule de Burnside

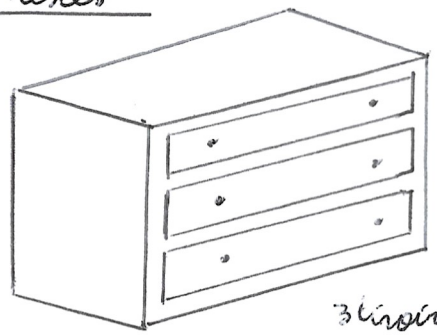
Notation 59 : Si G est fini et agit sur E. $\forall g \in G$, $\mathrm{Fix}(g) := \{x \in E, \ g \cdot x = x\}$

Proposition 60 : (Formule de Burnside) Si G est fini et agit sur E.
On note Ω l'ensemble des orbites de E.
Alors $|\Omega| = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)|$

Application 61 : Le nombre de manières possibles à rotation près de colorier un cube avec $n \in \mathbb{N}^*$ couleurs différentes vaut :
$\frac{1}{24}(n^6 + 8n^2 + 12n^3 + 3n^4)$

Annexes :

1)

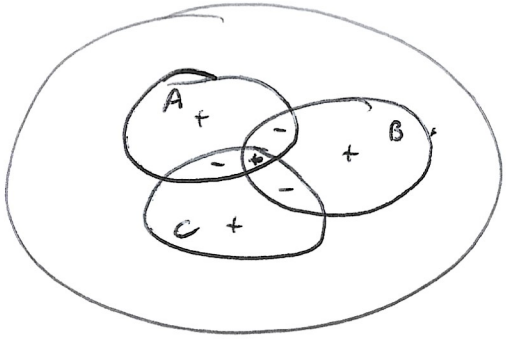


3 tiroirs

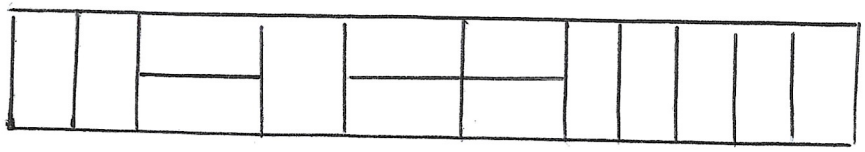
4 chaussettes

Un tiroir aura au moins deux chaussettes

2)



3) Un recouvrement possible



Références :

1) [Gou] Les maths en tête, Algèbre Probabilités, X. Gourdon

⚠ 3ème édition pour avoir du dénombrement

2) [Gou] Les maths en tête, Analyse, X. Gourdon

Uniquement pour avoir l'application 3 en entier (OSEF en vrai)

3) [FGN] Oraux X ENS algèbre 1, S. Francinou et Cie

4) [CGD] Exercices de probabilités, M. Cottrell et Cie

Pour le dev 1.

5) [Ber] Algèbre : le grand combat, G. Berhuy.

6) [Rom] Mathématiques pour l'agrégation, Algèbre et géométrie

J.-E. Rombaldi.

7) [FG] Exercices de mathématiques pour l'agrégation,

S. Francinou & H. Gianella pour le dev 2.

préfacé par MONSIEUR Perrin !

8) [HHGGI] Histoires hédonistes de groupes et de géométrie

tome I. P. Caldero et J. Germoni

9) [NHHGGII] Nouvelles histoires hédonistes de groupes et de géométrie tome II P. Caldero et J. Germoni.