Leçon 190 : Méthodes combinatoires, problèmes de dénombrement.

1 Dénombrement et combinatoire

1.1 Cardinal

Définition 1. On dit qu'un ensemble E est fini lorsqu'il est vide ou qu'il existe $n \in \mathbb{N}^*$ tel qu'il existe une bijection de E dans $[\![1, n]\!]$. Dans ce cas n ne dépend pas de la bijection et est appelé cardinal de E. Il est noté $|E|$ ou $\#E$. Si E est vide son cardinal est 0.

Proposition 2. *Soient E et F des ensembles :*

1. *Si E fini et qu'il existe une bijection de E dans F alors F est fini et $|E| = |F|$.*
2. *Si F fini et qu'il existe une injection de E dans F alors E est fini et $|E| \leqslant |F|$ avec égalité si et seulement si c'est une bijection.*
3. *Si E fini et qu'il existe une surjection de E dans F alors F est fini et $|F| \leqslant |E|$avec égalité si et seulement si c'est une bijection.*

Corollaire 3. *(Principe des tiroirs) Soient E et F des ensembles finis avec $|E| > |F|$. Si $\varphi : E \to F$ une application alors il existe $y \in F$ ayant au moins deux antécédents par φ dans E.*

Exemple 4. On doit ranger $n+1$ chaussettes dans n tiroirs alors un des tiroirs contiendra 2 chaussettes ou plus.
Pour tout $x \in \mathbb{R}$ et tout $n \in \mathbb{N}^*$, il existe $p/q \in \mathbb{Q}$ avec $1 \leqslant q \leqslant n$ tel que $|x - p/q| < \frac{1}{qn}$.

Proposition 5. *Soit B ensemble fini et $A \subset B$. Alors A est fini et $|A| \leqslant |B|$. Si $|A| = |B|$ alors $A = B$.*

1.2 Principe additif

Proposition 6. *Soient A et B deux ensembles finis, on a :*

1. *$|A \cup B| = |A| + |B| - |A \cap B|$. En particulier si A et B sont disjoints alors $|A \cup B| = |A| + |B|$.*
2. *$|A \backslash B| = |A| - |A \cap B|$. En particulier si $B \subset A$ on a $|A \backslash B| = |A| - |B|$.*

Proposition 7. *Soient $A_1, \dots, A_n$ des ensembles finis deux à deux disjoints, alors $\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{i=1}^{n} |A_i|$.*

Corollaire 8. *(Lemme des bergers) Si $A_1, \dots, A_n$ forme une partition de E ($\bigcup_{i=1}^{n} A_i = E$) alors $|E| = \sum_{i=1}^{n} |A_i|$. Lorsque les A_i ont tous le même cardinal k alors $|E| = nk$.*

Proposition 9. *(Crible de Poincaré) Soient $A_1, \dots, A_n$ des ensembles finis, alors on a*

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{k=1}^{n} (-1)^{k-1} \sum_{1 \leqslant i_1 < i_2 < \cdots < i_k \leqslant n} |A_{i_1} \cap \cdots \cap A_{i_k}|$$

.

1.3 Principe multiplicatif

Proposition 10. *Soient $E_1, \dots, E_n$ des ensembles finis. Le produit cartésien $E_1 \times \cdots \times E_n$ est fini et vérifie $|E_1 \times \cdots \times E_n| = |E_1| \dots |E_n|$. En particulier pour E fini on a $|E^n| = |E|^n$.*

Définition 11. Soit E un ensemble et $p \in \mathbb{N}^*$. On appelle p-liste ou p-uplet tout élément $(x_1, \dots, x_p) \in E^p$.

Remarque 12. Dans une liste l'ordre importe et un même élément peut figurer plusieurs fois. Une liste modélise donc des tirages successifs avec remise.

Proposition 13. *Soit E un ensemble de cardinal n et $p \leqslant n$ un entier non nul. On appelle p-arrangement de E toute p-liste de E d'éléments distincts. Le nombre de p-arrangement de E est $A_n^p = \frac{n!}{(n-p)!}$, en particulier il y a $n!$ n-arrangements de E.*

Remarque 14. Dans un arrangement l'ordre importe mais ils sont distincts. Un arrangement modélise donc des tirages successifs sans remise.

Proposition 15. *Soient E et F des ensembles finis.*

1. *L'ensemble des applications de E vers F noté F^E est fini et $\left|F^E\right| = |F|^{|E|}$.*
2. *En notant $p = |E|$ et $n = |F|$, lorsque $p \leqslant n$, l'ensemble des applications injectives de E vers F est fini de cardinal A_n^p.*
3. *En notant $n = |E|$, l'ensemble des bijections de E dans E noté $\mathcal{S}_E$ est fini de cardinal $n!$. On l'identifiera alors à $\mathcal{S}_n$.*

Corollaire 16. *Soit E ensemble fini, alors $\mathcal{P}(E)$ l'ensemble des parties de E est fini de cardinal $2^{|E|}$.*

Définition 17. Soit $I_n = \{1, \dots, n\}$ on appelle dérangement de I_n toute permutation σ n'ayant aucun point fixe.

Théorème 18. *Pour tout $p \in \mathbb{N}^*$ on note D_p l'ensemble des dérangements de I_p, c'est-à-dire les permutations sans point fixe. On pose $\delta_p = |D_p|$ et on a $\delta_1 = 0$ et par convention $\delta_0 = 1$. La formule générale est $\lfloor \frac{n!}{e} + 1/2 \rfloor$.*

1.4 Combinaisons

Définition 19. Soit E ensemble fini de cardinal n et $p \in \mathbb{N}^*$. On appelle p-combinaison de E toute partie de cardinal p. Il ne dépend que de n et p et est noté $\binom{n}{p}$.

Proposition 20. *Si $0 \leqslant p \leqslant n$ on a $\binom{n}{p} = \frac{n!}{p!(n-p)!} \in \mathbb{N}$ et si $p > n$ on a $\binom{n}{p} = 0$.*

Remarque 21. Dans les combinaisons les éléments sont distincts mais l'ordre ne compte pas. Ainsi les combinaisons modélisent les tirages simultanés.

Proposition 22. *Soient $n, p \in \mathbb{N}$, on a alors :*

1. *Si $0 \leqslant p \leqslant n$ on a $\binom{n}{p} = \binom{n}{n-p}$ (symétrie).*
2. *Si $p, n \geqslant 1$ on a $\binom{n}{p} = \binom{n-1}{p-1} + \binom{n-1}{p}$ (formule de Pascal).*
3. *Si $p, n \geqslant 1$ on a $\binom{n}{p} = \frac{n}{p}\binom{n-1}{p-1} = \frac{n-p+1}{p}\binom{n}{p-1}$.*
4. *Si $p, n \geqslant 0$ on a $\binom{n+1}{p+1} = \sum_{q=p}^{n} \binom{q}{p}$.*

Proposition 23. *(Binôme) Soient a, b deux éléments d'une algèbre qui commutent, alors $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$*

Théorème 24. *(Vandermonde) Soient $m, n, p \in \mathbb{N}$ alors on a $\sum_{k=0}^{p} \binom{n}{k}\binom{m}{p-k} = \binom{n+m}{p}$.*

Proposition 25. *Soit E fini de cardinal n. Soit $p \in \mathbb{N}^*$ et $i_1, \dots, i_p \in \mathbb{N}$ tels que $i_1 + \dots + i_p = n$. Alors le nombre de partitions ordonnées $(A_1, \dots, A_p)$ de E tels que $|A_k| = i_k$ est égal à $\binom{n}{i_1, \dots, i_p} = \frac{n!}{i_1! \dots i_p!}$.*

Proposition 26. *Soient $a_1, \dots, a_p$ des éléments d'une algèbre qui commutent 2 à 2, alors pour tout $n \in \mathbb{N}^*$ on a $(a_1 + \dots + a_p)^n = \sum_{\substack{i_1, \dots, i_p \in \mathbb{N} \\ i_1 + \dots + i_p = n}} \binom{n}{i_1, \dots, i_p} a_1^{i_1} \dots a_p^{i_p}$*

2 Utilisations avec les corps finis

2.1 Matrices diagonalisables

Lemme 27. *Pour tout entier $p \in \{1, \dots, n\}$ il y $\prod_{k=1}^{p}(q^n - q^{k-1}) = q^{\frac{p(p-1)}{2}} \prod_{k=n-p+1}^{n}(q^k - 1)$ familles formées de p vecteurs linéairement indépendants dans un $\mathbb{F}_q$ espace vectoriel de dimension n.*

Théorème 28. *Pour tout $\mathbb{F}_q$ espace vectoriel E on a :*

1. $|GL(E)| = \prod_{k=1}^{n}(q^n - q^{k-1}) = q^{\frac{n(n-1)}{2}} \prod_{k=1}^{n}(q^k - 1)$
2. $|SL(E)| = q^{n-1}\prod_{k=1}^{n}(q^n - q^{k-1}) = q^{\frac{n(n-1)}{2}} \prod_{k=2}^{n}(q^k - 1)$

On note $D_n(\mathbb{F}_q)$ l'ensemble des matrices diagonalisables de taille n de $\mathbb{F}_q$.

Lemme 29. *On a $D_n(\mathbb{F}_q) = \{A \in GL_n(\mathbb{F}_q) | A^q = A\}$.*

Lemme 30. *Pour tout $A \in D_n(\mathbb{F}_q)$ on a $\mathbb{F}_q^n = \bigoplus_{k=1}^{q-1} \ker(A-\lambda_k I_n)$ où λ_k sont les valeurs propres de A.*

Définition 31. On pose $\mathcal{F} = \{(E_1, \dots, E_{q-1}) | \mathbb{F}_q^n = \bigoplus_{k=1}^{q-1} E_k\}$ et $\mathcal{F}_{(n_1,\dots,n_{q-1})} = \{(E_1, \dots, E_{q-1}) \in \mathcal{F} | \dim(E_i) = n_i, 1 \leqslant i \leqslant q-1\}$ ce qui nous donne une partition de $\mathcal{F}$.

Lemme 32. *L'application $\varphi : D_n(\mathbb{F}_q) \to \mathcal{F}$; $A \mapsto (\ker(A - \lambda_1 I_n), \dots, \ker(A - \lambda_{q-1} I_n))$ est bijective.*

Lemme 33. *Pour $(n_k)_{1\leqslant k\leqslant q-1} \in \mathbb{N}^{q-1}$ fixé tel que $\sum_{k=1}^{q-1} n_k = n$ l'application : $GL(\mathbb{F}_q^n) \times \mathcal{F}_{(n_1,\dots,n_{q-1})} \to \mathcal{F}_{(n_1,\dots,n_{q-1})}$; $(g, (E_1, \dots, E_{q-1})) \mapsto (g(E_1), \dots, g(E_{q-1})$ définit une action transitive de $GL(\mathbb{F}_q^n)$ vers $\mathcal{F}_{(n_1,\dots,n_{q-1})}$*

Lemme 34. *Pour $(n_k)_{1\leqslant k\leqslant q-1} \in \mathbb{N}^{q-1}$ fixé tel que $\sum_{k=1}^{q-1} n_k = n$ et $(E_k)_{1\leqslant k\leqslant q-1} \in \mathcal{F}_{(n_1,\dots,n_{q-1})}$, le stabilisateur de $(E_k)_{1\leqslant k\leqslant q-1}$ est de cardinal $\prod_{k=1}^{q-1} |GL(E_k)|$ et $\left|\mathcal{F}_{(n_1,\dots,n_{q-1})}\right| = \frac{\left|GL_n(\mathbb{F}_q^n)\right|}{\prod_{k=1}^{q-1} |GL(E_k)|}$*

Théorème 35. *Avec la convention $|GL_0(\mathbb{F}_q)| = 0$ on a :*

$$|D_n(\mathbb{F}_q)| = \sum_{\substack{(n_1,\dots,n_{q-1}) \in \mathbb{N}^{q-1} \\ n_1+\dots+n_{q-1}=n}} \frac{|GL_n(\mathbb{F}_q)|}{|GL_{n_1}(\mathbb{F}_q)| \dots \left|GL_{n_{q-1}}(\mathbb{F}_q)\right|}$$

2.2 Polynômes irréductibles

Définition 36. On définit la fonction de Möbius comme $\mu(1) = 1$, $\mu(n) = (-1)^r$ si $n = \prod_{i=1}^{r} p_i$ dans sa décomposition en facteurs carrés et $\mu(n) = 0$ sinon.

Théorème 37. *(Möbius) Soient $(u_n)_{n\in\mathbb{N}^*}$ et $(v_n)_{n\in\mathbb{N}^*}$ des suites réelles alors $\forall n \in \mathbb{N}^*, u_n = \sum_{d|n} v_d \iff \forall n \in \mathbb{N}^*, v_n = \sum_{d|n} \mu(d) u_{\frac{n}{d}}$.*

On pose $P_n(X) = X^{p^n} - X \in \mathbb{F}_p[X]$ et $\mathcal{U}_d(p) = \{P \in \mathbb{F}_p[X] | \deg(P) = d, \text{irréductible et unitaire}\}$ pour tout $n \in \mathbb{N}^*$ et p premier fixé.

Lemme 38. *Tout diviseur irréductible de P_n dans $\mathbb{F}_p[X]$ est de degré divisant n. Réciproquement pour tout diviseur d de n tout polynôme $P \in \mathcal{U}_d(p)$ divise P_n.*

Théorème 39. *Le polynôme P_n est sans facteur carré dans $\mathbb{F}_p[X]$ et on a $X^{p^n} - X = \prod_{d|n} \prod_{P\in\mathcal{U}_d(p)} P(X)$.*

Théorème 40. *Pour tout entier $n \in \mathbb{N}^*$ on a $|\mathcal{U}_n(p)| = \frac{1}{n}\sum_{d|n} \mu(\frac{n}{d}) p^d$.*

Dev 1 : Dénombrement des matrices diagonalisables de Fq 30 et 32,33, 34 et 35
Dev 2 : Dénombrement des polynômes irréductibles de Fp 37,38,39 et 40
Dev 3 : Nombre de dérangements de Sn 18

Références

[GOU21] Xavier GOURDON : Les maths en tête. Algèbre et probabilités. Ellipses, 2021.

[PER96] Daniel PERRIN : Cours d'algèbre. Ellipses, 1996.

[ROM17] JeanÉtienne ROMBALDI : Mathématiques pour l'Agrégation : Algèbre géométrie. De Boeck Superieur, 2017.

RAPPORT DU JURY :
Il est nécessaire de dégager clairement différentes méthodes de

dénombrement et de les illustrer d'exemples significatifs. De nombreux domaines des mathématiques sont concernés par des problèmes de dénombrement, cet aspect varié du thème de la leçon doit être mis en avant. L'utilisation de séries génératrices est un outil puissant pour le calcul de certains cardinaux. De plus, il est naturel de calculer des cardinaux classiques et certaines probabilités. Il est important de connaître l'interprétation ensembliste de la somme des coefficients binomiaux et ne pas se contenter d'une justification par le binôme de Newton. L'introduction des corps finis (même en se limitant aux cardinaux premiers) permet de créer un lien avec l'algèbre linéaire. Les actions de groupes peuvent également conduire à des résultats remarquables.
Pour aller plus loin, les candidates et candidats peuvent aussi présenter des applications de la formule d'inversion de Möebius ou de la formule de Burnside. Des candidates et candidats ayant un bagage probabiliste pourront explorer le champ des permutations aléatoires, en présentant des algorithmes pour générer la loi uniforme sur le groupe symétrique Sn et analyser certaines propriétés de cette loi uniforme (points fixes, cycles, limite $n \to \infty$, ...).