Leçon 190. Méthodes combinatoires, problème de dénombrement.

1. Les premiers outils : les méthodes ensemblistes

1.1. Ensemble fini et cardinalité

1. Définition. Un ensemble non vide E est *fini* s'il existe un entier $n \in \mathbf{N}^*$ et une bijection $E \longrightarrow [\![1, n]\!]$. Un tel entier n est unique, on l'appelle le *cardinal* de E et on le note $|E|$. Par convention, l'ensemble vide $\emptyset$ est fini de cardinal 0.

2. Proposition. Soient E et F deux ensembles fini. Alors
   - toute partie $A \subset E$ est finie ;
   - les ensembles E et F ont même cardinal si et seulement s'ils sont en bijection.

3. Proposition. Soient E et F deux ensembles finis disjoints. Alors
$$|E \cup F| = |E| + |F|.$$

4. Exemple. Il existe 875 nombres à trois chiffres possédant au moins un chiffre pair.

5. Proposition *(formule du crible).* Soient A_1, ..., A_n des ensembles finis. Alors
$$|A_1 \cup \cdots \cup A_n| = \sum_{k=1}^{n} (-1)^{k-1} \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} |A_{i_1} \cap \cdots \cap A_{i_k}|.$$

6. Application. Soient φ l'indicatrice d'Euler et $n \in \mathbf{N}^*$ un entier. Alors
$$\frac{\varphi(n)}{n} = \prod_{p \mid n} \left(1 - \frac{1}{p}\right).$$

7. Proposition. Soient E et F deux ensembles finis. Alors $|E \times F| = |E|\,|F|$.

8. Exemple. Il existe 12 issues possibles à un lancer d'une pièce suivi d'un lancer d'un dé à six faces. Le nombre de mots à 5 lettres est $26^5 = 11\,881\,376$. Le cardinal du groupe linéaire sur un corps fini est
$$|\mathrm{GL}_n(\mathbf{F}_q)| = (q^n - 1)(q^n - q^2) \cdots (q^n - q^{n-1}).$$

9. Corollaire. Soient E et F deux ensembles finis. Alors $\left|E^F\right| = |E|^{|F|}$.

10. Corollaire. Soit E un ensemble fini. Alors $|\mathscr{P}(E)| = 2^{|E|}$.

11. Exemple. Le nombre de comités formés à partir de 7 personnes est $2^7 = 128$.

12. Proposition. Soient E et F deux ensemble finis et $f \colon X \longrightarrow F$ une surjection. Alors
$$|E| = \sum_{y \in F} |f^{-1}(\{y\})|.$$

13. Corollaire *(lemme des bergers).* Avec les mêmes hypothèses, on suppose que les ensembles $f^{-1}(\{y\})$ sont tous de même cardinal $n \in \mathbf{N}^*$. Alors $|E| = n\,|F|$.

14. Proposition *(lemme des tiroirs).* Soient E et F deux ensembles finis. Si $|E| > |F|$, alors il n'existe pas d'injection de E dans F.

1.2. Arrangements et combinaisons

15. Définition. Soient $n, k \in \mathbf{N}^*$ deux entiers vérifiant $k \leqslant n$. Un (n,k)-*arrangement* est une injection $[\![1, n]\!] \longrightarrow [\![1, k]\!]$.

16. Proposition. Le cardinal de l'ensemble A_k^n des (n,k)-arrangements vaut
$$\frac{k!}{(n-k)!}.$$
En particulier, le cardinal du groupe symétrique $\mathfrak{S}_n = A_n^n$ vaut $n!$.

17. Exemple. Vingt-cinq chevaux participent à la course du tiercé. Un tiercé étant un $(3, 25)$-arrangements, il y en a $25 \times 24 \times 23 = 13\,800$. Il existe $6! = 120$ anagramme du mot « cheval ».

18. Définition. Soient $n, k \in \mathbf{N}$ deux entiers avec $n \neq 0$. Une (n,k)-*combinaison* est une partie de l'ensemble $[\![1, n]\!]$ de cardinal k.

19. Proposition. Le nombre $\binom{n}{k}$ de (n,k)-combinaisons vérifie
$$\binom{n}{k} = \begin{cases} \dfrac{n!}{k!(n-k)!} & \text{si } k \leqslant n, \\ 0 & \text{si } k > n. \end{cases}$$

20. Exemple. Le nombre de main de 5 cartes, c'est-à-dire un ensemble de 5 cartes, d'un jeu de 52 cartes vaut $\binom{52}{5} = 2\,395\,120$.

21. Proposition. Avec la définition, on trouve les identités
   - $\sum_{k=0}^{n} \binom{n}{k} = 2^n$,
   - $\binom{n}{k} = \binom{n}{n-k}$,
   - $k\binom{n}{k} = n\binom{n-1}{k-1}$,
   - $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$.

22. Proposition *(formule de binôme de Newton).* Soient A un anneau et $a, b \in A$ deux éléments qui commutent. Pour tout entier $n \in \mathbf{N}$, on a
$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

2. Des méthodes issues de la théorie des groupes

2.1. Dénombrement dans les groupes

23. Théorème. Soit G un groupe fini. Tout sous-groupe H de G divise l'ordre de G. De plus, si $[G : H]$ désigne le cardinal du quotient G/H, on a $|G| = [G : H]\,|H|$.

24. Application. En étudiant le nombre de ses éléments dont l'ordre est fixé, le groupe alterné $\mathfrak{A}_5$ est simple.

25. Proposition. Soit G un groupe fini agissant sur un ensemble fini X. Soit $x \in X$ un élément. On note $\mathrm{Stab}_G(x)$ et $G \cdot x$ son stabilisateur et son orbite. Alors
$$|G \cdot x| = \frac{|G|}{|\mathrm{Stab}_G(x)|}.$$

26. Exemple. L'espace projection $\mathbf{P}^n(\mathbf{F}_q) = \mathbf{F}_q^n / \mathbf{F}_q^\times$ de dimension n sur le corps $\mathbf{F}_q$ est de cardinal
$$|\mathbf{P}^n(\mathbf{F}_q)| = \frac{q^{n+1} - 1}{q - 1}.$$

27. THÉORÈME *(équation aux classes)*. Soit $\{x_1, \dots, x_n\} \subset X$ un système de représentants des orbites. Alors

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

28. APPLICATION. De l'équation au classes se déduisent les deux faits suivants :
- le centre d'un p-groupe n'est pas trivial ;
- tout groupe d'ordre p^2 est abélien.

29. THÉORÈME *(Cauchy)*. Soient G un groupe fini et p un diviseur premier de $|G|$. Alors le groupe G contient un élément d'ordre p.

30. PROPOSITION *(formule de Burnside)*. Le nombre d'orbites vaut

$$\frac{1}{|G|} \sum_{g \in G} |\{x \in X \mid g \cdot x = x\}|.$$

2.2. Application des actions de groupes

D1

31. PROPOSITION. Pour tout élément $a \in \mathbf{F}_p^\times$, on a

$$|\{x \in \mathbf{F}_p \mid ax^2 = 1\}| = 1 + \left(\frac{a}{p}\right).$$

32. THÉORÈME *(loi de réciprocité quadratique)*. Soient p et q deux nombres premiers impairs. Alors

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)/2 \times (q-1)/2}.$$

33. DÉFINITION. On appelle *cône nilpotent* sur $\mathbf{K}$ l'ensemble $\mathrm{Nil}_n(\mathbf{K})$ des matrices nilpotentes à coefficients dans $\mathbf{K}$, c'est-à-dire des matrices $A \in \mathscr{M}_n(\mathbf{K})$ telle qu'il existe un entier $p \in \mathbf{N}^*$ vérifiant $A^p = I_n$.

34. THÉORÈME. Soit $\mathbf{F}_q$ un corps fini de cardinal q. Alors

$$|\mathrm{Nil}_n(\mathbf{F}_q)| = q^{n(n-1)}.$$

D2

35. LEMME. Un endomorphisme d'un $\mathbf{F}_q$-espace vectoriel de dimension finie est diagonalisable si et seulement s'il est annulé par le polynôme $X^q - X \in \mathbf{F}_q[X]$.

36. THÉORÈME. Le nombre de matrices diagonalisables de $\mathrm{GL}_n(\mathbf{F}_q)$ vaut

$$\sum_{\substack{(n_1,\dots,n_{q-1}) \in \mathbf{N}^{q-1} \\ n_1 + \dots + n_{q-1} = n}} \frac{|\mathrm{GL}_n(\mathbf{F}_q)|}{|\mathrm{GL}_{n_1}(\mathbf{F}_q)| \cdots |\mathrm{GL}_{n_{q-1}}(\mathbf{F}_q)|}.$$

3. Méthode algébriques : inversion et séries génératrices

3.1. Méthode par inversion

37. DÉFINITION. Pour un entier $n \in \mathbf{N}^*$ qu'on écrit $n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ en produit de nombres premiers, on définit

$$\mu(n) := \begin{cases} 1 & \text{si } n = 1, \\ -1 & \text{si } n \text{ contient un facteur carré,} \\ (-1)^s & \text{si } n \text{ est sans facteur carré.} \end{cases}$$

La fonction $\mu \colon \mathbf{N}^* \longrightarrow \{-1, 0, 1\}$ est le *fonction de Möbius*.

38. PROPOSITION. Soient $m, n \in \mathbf{N}^*$ deux entiers premiers entre eux. Alors

$$\mu(mn) = \mu(m)\mu(n).$$

39. THÉORÈME *(formule d'inversion de Möbius)*. Soient G un groupe abélien et $f \colon \mathbf{N}^* \longrightarrow G$ une application. Pour un entier $n \in \mathbf{N}^*$, on pose

$$g(n) := \sum_{d \mid n} f(d).$$

Pour tout entier $n \in \mathbf{N}^*$, on a

$$f(n) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) g(n).$$

40. COROLLAIRE. Soit $n \in \mathbf{N}^*$. La fonction indicatrice d'Euler vérifie

$$\varphi(n) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) n.$$

41. APPLICATION. Le nombre de polynôme irréductibles unitaires de degré n de $\mathbf{F}_q[X]$ vaut

$$\frac{1}{n} \sum_{d \mid n} \mu\left(\frac{n}{d}\right) q^d.$$

3.2. Séries génératrices et application aux nombres de Catalan et de Bell

42. DÉFINITION. Pour une suite $u := (u_n)_{n \in \mathbf{N}}$ d'un corps $\mathbf{K}$, on définit sa *série génératrice* comme la série formelle

$$G(u) := \sum_{n \in \mathbf{N}} u_n X^n \in \mathbf{K}[\![X]\!].$$

43. EXEMPLE. En considérant la suite $u := (1, 1, \dots) \in \mathbf{K}^{\mathbf{N}}$, on a

$$G(u) = \frac{1}{1 - X}.$$

44. APPLICATION. Pour tout entier $n, p \in \mathbf{N}^*$, en calculant la série formelle $(1 - X)^{-p}$ comme un produit de Cauchy, on trouve

$$|\{(n_1, \dots, n_p) \in \mathbf{N}^p \mid n_1 + \dots + n_p = n\}| = \binom{n + p - 1}{p - 1}.$$

45. DÉFINITION. Soit $n \in \mathbf{N}^*$. Le *n-ième nombre de Catalan* est le nombre γ_n de façon de placer les parenthèses dans une expression formelle $x_0 \cdots x_n$ afin qu'elle soit calculée lorsque le produit n'est pas associatif. On convient que $\gamma_0 = \gamma_1 = 1$.

46. EXEMPLE. L'expression $x_0 x_1 x_2$ admet deux parenthésages possibles, à savoir les expressions $x_0(x_1 x_2)$ et $(x_0 x_1) x_2$. D'où $\gamma_2 = 2$.

47. PROPOSITION. Pour tout entier $n \in \mathbf{N}^*$, on a

$$\gamma_n = \sum_{i=0}^{n-1} \gamma_i \gamma_{n-1}.$$

48. THÉORÈME. Pout tout entier $n \in \mathbf{N}^*$, on a

$$\gamma_n = \frac{1}{n+1}\binom{2n}{n}.$$

49. DÉFINITION. Soit $n \in \mathbf{N}$. Le *n-ième nombre de Bell* est le nombre B_n de partitions d'un ensemble de cardinal n.

50. PROPOSITION. Pour tout entier $n \in \mathbf{N}^*$, on a

$$B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_{n-k}.$$

51. THÉORÈME. Pour tout entier $n \in \mathbf{N}^*$, on a

$$B_n = e^{-1} \sum_{k=0}^{+\infty} \frac{k^n}{k!}.$$

[1] Josette CALAIS. *Éléments de théorie des groupes.* 3e édition. Presses Universitaires de France, 1998.

[2] Philippe CALDERO et Jérôme GERMONI. *Histoires hédonistes de groupes et de géométries.* T. Tome second. Calvage & Mounet, 2015.

[3] Dominique FOATA et Aimé FUCHS. *Calcul des probabilités.* Seconde édition. Dunod, 1998.

[4] Serge FRANCINOU, Hervé GIANELLA et Serge NICOLAS. *Exercices de mathématiques. Oraux X-ENS. Algèbre 1.* Cassini, 2001.

[5] Daniel PERRIN. *Cours d'algèbre.* Ellipses, 1996.

[6] Philippe SAUX PICART. *Cours de calcul formel. Algorithmes fondamentaux.* Ellipses, 1999.