Leçon 190 : Méthodes combinatoires, problèmes de dénombrement.

Développements :

Loi de réciprocité quadratique, Polynômes irréductibles sur F_q.

Bibliographie :

De Biasi, Delaunay MPSI, Nourdin, Gourdon, Oraux X-ENS, Bernis, Demazure, Rombaldi.

Rapport du jury :

Il est nécessaire de dégager clairement différentes méthodes de dénombrement et les illustrer d'exemples significatifs. De nombreux domaines de 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. S'ils le désirent, les candidats peuvent aussi présenter des applications de la formule d'inversion de Möebius ou de la formule de Burnside. Des 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 S_n et analyser certaines propriétés de cette loi uniforme (points fixes, cycles, limite $n \to +\infty$ ...).

Remarque 1. *Les principaux résultats se trouvent également dans le Delaunay MPSI.*

1 Quelques outils et méthodes de dénombrement

1.1 Cardinaux et ensembles (manipulations ensemblistes)

Définition 2 (De Biasi p9)**.** *[Delaunay p205] Un ensemble est fini s'il existe $n \in \mathbb{N}$ et une bijection de E sur $\{1, .., n\}$. n est appelé cardinal de E.*

Remarque 3. *Dans la suite, tous les ensembles sont supposés finis.*

Proposition 4 (De Biasi p9)**.** *Cardinal d'une réunion (disjointe ou non).*

Application 5. *$ax^2 + by^2 = 1$ a toujours une solution.*

Proposition 6 (De Biasi p9)**.** *Formule du crible.*

Proposition 7. *Si $f : E \to F$ est injective et F est fini alors E est fini et $|E| \leq |F|$.*
Si f est surjective et E est fini alors F est fini et $|E| \geq |F|$.
Si f est bijective et E ou F est fini alors E et F sont finis et de même cardinal.

Proposition 8 (De Biasi p9)**.** *Cardinal d'un produit.*

Application 9 (De Biasi p9)**.** *Cardinal de A^p.*

Application 10. *Fonctions de E dans F de cardinal $|F|^{|E|}$.*

Application 11 (De Biasi p11)**.** *Nombres de trois chiffres contenant au moins l'un des chiffres $0, 3, 6, 9$.*

Application 12 (De Biasi p12)**.** *Cardinal de $P(E)$.*

Application 13 (De Biasi p12)**.** *Alphabet Braille.*

1.2 Arrangements, permutations et combinaisons (autour des coefficients binomiaux)

Définition 14 (De Biasi p10)**.** *Pour $k \geq 1$, un k-arrangement d'un ensemble E est une injection de $\{1, .., k\}$ dans E.*

Proposition 15. *Pour $n = |E|$, E possède $n(n-1)...(n-(k-1))$ k-arrangements si $k \leq n$, et 0 sinon.*

Application 16 (De Biasi p11)**.** *Tirages ordonnés sans remise. Cela correspond au nombre de tirages possibles de p boules dans une urne contenant n boules, sans remise.*

Application 17. *Paradoxe des anniversaires. La probabilité que deux élèves parmi n aient leur anniversaire le même jour est de $1 - A^n_{365}/365$.*

Définition 18 (De Biasi p11). *Permutation.*

Proposition 19 (de Biasi p11). *Le cardinal est $n!$.*

Définition 20 (De Biasi p13). *n parmi k est le nombre de parties de $\{1,..,n$ à k éléments.*

Proposition 21 (De Biasi p13). $\binom{n}{p}$ *= calcul avec les factoriels.*

Application 22 (De Biasi p14). *Dans une course de 20 chevaux, il y a 1140 tiercés dans le désordre et 6840 tiercés dans l'ordre.*

Application 23 (Tauvel théorie de Galois). *Nombre de 3-cycles dans S_n.*

Proposition 24 (De Biasi p13). *Les 4 propriétés principales du binomial, dont Pascal et formule du binôme.*

Application 25. $\sum \binom{n}{k} = 2^n$, $\sum \binom{n}{k}(-1)^k = 0$ *si* $n \neq 0$, $\sum \binom{n}{k}\binom{n}{n-k}$, *somme des* $1/k$, $1/k^2$, $1/k^3$.

Remarque 26. *Interprétation :* $card\{F \subset E, |F| = k\} = card(P(E))$.
$card\{F \subset E, |F|impair\} = card\{F \subset E, |F|pair\}$.

Application 27. *Morphisme de Frobenius.*

Application 28. *La somme de deux éléments nilpotents d'un anneau commutatif est nilpotente.*

Proposition 29 (Romb p53, Delaunay p229). *Nombre de dérangement, i.e. de permutations sans points fixes. L'inverse de la matrice de Pascal, le nombre de dérangements, de surjections, d'applications strictement croissantes, d'applications croissantes.[De Biasi p22]*

Proposition 30 (Romb). *Formule d'inversion de Pascal.*

Proposition 31 (Candelpergher p454). *Nombre de surjections.*

Remarque 32. *On cherche alors à mettre les ensembles quelconques en relation avec ces ensembles bien connus.*

1.3 Principes fondamentaux de combinatoire

Lemme 33 (De Biasi p21). *Lemme des Bergers.*

Application 34 (De Biasi p21). *Nombre de surjections de $\{1,..n+1\}$ sur $\{1,..,n\}$. (Déjà dit avant...)*

Exemple 35. *Pour compter ses moutons, le berger peut compter le nombre de pattes puis diviser par 4.*

Proposition 36 (Nourdin p174). *Principe des tiroirs. Si $f : \{1,..n\} \to \{1,..,m\}$ avec $n > m$, alors f n'est pas injective, autrement dit si on met plus de n chaussettes dans n tiroirs, au moins un tiroir contient plusieurs chaussettes.*

Application 37. *Parmi $n+1$ entiers de $\{1,..,2n\}$, il y en a toujours deux dont un est multiple de l'autre.*
Si on choisit 101 entiers parmi $\{1,..,200\}$ alors il y en a au moins 1 qui divise un autre

Application 38. *L'équation $ax^2 + by^2 = 1$ possède au moins une solution dans$F_{p^r} \times F_{p^r}$.*

Application 39 (Gourdon analyse p275). *Approximation rationnelle. Soit $x \in \mathbb{R}$, $n \in \mathbb{N}$, il existe $p/q \in Q$ tel que $|x - p/q| \leq 1/nq$.*

Application 40 (Nourdin p175). *La série $\sum \frac{1}{n^2 \sin(n)^2}$ diverge. (Pas très simple...)*

Proposition 41. *Principe de double dénombrement : On utilise des propriétés liées à la cardinalité d'un ensemble A afin de calculer $|A|$ de deux façons différentes pour obtenir une égalité entre deux valeurs. Ce principe est utilisé dans la démonstration de la formule de Burnside et dans la démonstration de la loi de réciprocité quadratique.*

Remarque 42. *Les récurrences. On cherche à ramener une situation combinatoire à celles d'ordres inférieurs. . Le principe de récurrence et les relations de récurrence linéaires sont très utiles pour compter des objets.*

1.4 Séries formelles, séries génératrices

Définition 43 (Nourdin p176). *Etant donné une suite $(a_n)_n \in \mathbb{Z}^{\mathbb{N}}$, on appelle série génératrice la série formelle $\sum a_n t^n$.*

Remarque 44 (Nourdin p174). *On peut parfois regarder la série génératrice au sens analytique ce qui permet d'utiliser des techniques d'analyse.*
En pratique, les a_n ont une signification combinatoire, et on ne peut pas les déterminer un par un. On peut par diverses méthodes (développements de fractions rationnelles, équations différentielles) déterminer la série génératrice de (a_n).

Application 45 (Nourdin p177). *Nombres de Catalan.*

Application 46 (Bernis). *Nombres de Bell.*

Application 47 (FGN AL1). *Nombre de dérangements, d'involutions, nombres de Bell, problèmes de parenthésages, partition d'un entier en parts fixées, nombre d'équivalences sur un ensemble.*

2 Structure algébrique finie et combinatoire

2.1 Utilisation de la théorie des groupes

Théoreme 48. *Théorème de Lagrange.*

Proposition 49. $|G| = |Im(f)||ker(f)|$.

Application 50. *Nombre de carrés dans F_p.*

Définition 51. *Orbite.*

Définition 52. *Stabilisateur.*

Théoreme 53. *Relation orbite-stabilisateur. Formule des classes.*

Proposition 54. *$card(S(E)) = n!$ par action de groupes.*

Application 55. *Lemme de Cauchy.*

Application 56. *Centre d'un p-groupe, les groupes d'ordre p^2 sont abéliens.*

Application 57. *Loi de réciprocité quadratique.*

Proposition 58. *Formule de Burnside.*

Application 59. *Collier de perles.*

2.2 Dénombrement sur les corps finis

Proposition 60. *$card(GL_(F_q))$, $card(SL_n(F_q))$, Nombre de vecteurs linéairement indépendants.*

Proposition 61. *Les matrices triangulaires forment un p-Sylow.*

Théoreme 62. *Théorème de Sylow : tout groupe admet un p-Sylow.*

Proposition 63 (Romb p151)**.** *Nombre de sev de dimension k sur F_q^m, nombre de matrices diagonalisables sur F_q.*

Proposition 64 (H2G2)**.** *Cardinal des matrices nilpotentes.*

Proposition 65 (Escofier)**.** *Nombre de classes de congruence des matrices symétriques sur F_q.*

3 Combinatoire et fonctions multiplicatives

3.1 Indicatrice d'Euler

Définition 66 (Demazure p56)**.** *Fonction multiplicative.*

Définition 67 (Demazure p55)**.** *$\phi(n)$ est le nombre d'entiers entre 0 et $n-1$ premiers avec n.*

Proposition 68 (Demazure p56)**.** *$phi(p^r)$.*

Proposition 69. *ϕ est multiplicative.*

Proposition 70 (Demazure p57)**.** *Expression de $\phi(n)$ et $n = \sum_{d|n} \phi(d)$.*

Application 71. *K^* est cyclique.*

Proposition 72 (Romb)**.** *Petit théorème de Fermat.*

3.2 Fonction de Mobius

Définition 73 (Romb p330)**.** *Fonction de Mobius.*

Proposition 74. *μ sont multiplicative.*

Proposition 75 (Romb p332)**.** *Formule d'inversion de Mobius.*

Application 76. *Inversion de $\phi(n)$.*

Application 77. *Pour $r > 1$, la série $\sum 1/n^r$ est une série absolument convergente, avec : $(\sum 1/n^r)(\sum \mu(n)/n^r) = 1$.*

Définition 78. *On note $I(n,q)$ l'ensemble des polynômes irréductibles de degré n sur F_q.*

Proposition 79. *$\forall n \geq 1$, $X^{q^n} - X = \prod_{d|n} \prod_{P \in I(d,q)} P$.*

Exemple 80 (Gozard)**.**

Proposition 81. *Pour tout $n \geq 1$, $n.|I(n,q)| = ...$ Puis développement asymptotique.*

Application 82. *Test de Rabin : $P \in F_q[X]$ est irréductible sur F_q si et seulement si P divise $X^{q^n} - X$ et si $pgcd(P, X^{q^d} - X) = 1$ pour tout d diviseur strict de n.*