Leçon 190 - Méthodes combinatoires, problèmes de dénombrement.

1. Quelques outils de dénombrement. —

1. Ensembles finis. —

- Def : Un ensemble E est fini ssi $\exists n \geq 1$ tq E est en bijection avec $\{1, .., n\}$.
  On définit alors le cardinal de E par $|E| = n$.
- Rem : Dans la suite, tous les ensembles considérés seront finis (sauf contre-indication).
- Pro : Si E et F sont en bijection, alors $|E| = |F|$.
- Pro : Pour $E_1, .., E_n \subset E$ disjoints 2 à 2, $|\bigcup_i E_i| = [E_1| + .. + |E_n|$.
- Pro : Formule du crible : Pour $E_1, .., E_n \subset E$,
  $|\bigcup_i E_i| = \sum_{p=1}^{n} (-1)^{p+1} \sum_{1 \leq i_1 < .. < i_p \leq n} |E_{i_1} \cap .. \cap E_{i_p}|$.
- Pro : $|A_1 \times .. \times A_n| = \Pi_i |A_i|$.
- App : $|Fonctions(E, F)| = |F|^{|E|}$.
- App : $|P(E)| = 2^{|E|}$.
- Ex : L'alphabet braille comporte 2^6 signes possibles.
- Ex : Si l'on tire p fois une boule dans une urne à n éléments avec remise, il y a n^p combinaisons possibles dans l'ordre.

2. Arrangements, permutations et combinaisons. —

- Def : Pour $k \geq 1$, un k-arrangement d'un ensemble E est une injection de $\{1, .., k\}$ dans E.
- Pro : Pour $n = |E|$, E possède $n(n-1)...(n-(k-1))$ k-arrangements si $k \leq n$, et 0 sinon.
- App : $|\Sigma_n| = n!$.
- Def : Pour $n, k \in \mathbb{N}$, on note $\binom{n}{k}$ le nombre de parties de $\{1, .., n\}$ à k éléments.
- Pro : Si $k \leq n$, $\binom{n}{k} = \frac{n!}{k!(n-k)!} = \binom{n}{n-k}$.
  $\binom{n}{k} = 0$ sinon.
- Pro : Formule du binôme : Pour a, b dans un anneau commutatif A, $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$
- App : $\sum_{k=0}^{n} \binom{n}{k} = 2^n$.
- App : $\sum_{k=0}^{n} \binom{n}{k}\binom{n}{n-k} = \binom{2n}{n}$.
- App : Avec $(y+1)^l = \sum_{k=0}^{l} \binom{l}{k} y^k$, on trouve :
  $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$,$\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$, $\sum_{k=1}^{n} k^3 = (\frac{n(n+1)}{2})^2$
- Pro : Deux permutations de Σ_n sont conjuguées ssi elles ont le même nombre de points fixes ainsi que le même nombre de k-cycles dans leur décomposition en produit de cycles à supports disjoints, $\forall 2 \leq k \leq n$.
- Pro : Soit $\sigma \in \Sigma_n$ possédant a_1 points fixes, et dont la décomposition en cycles à supports disjoints comporte a_k cycles de longueur k.
  Alors, $\forall d \geq 1$, σ^d possède $\sum_{l=1}^{n} a_l.pgcd(l, d)$ cycles et points fixes.
- **Dev** : Théorème de Brauer : Soit $\mathbb{K}$ un corps de caractéristique quelconque, $n \geq 1$, et $\sigma, \sigma' \in \Sigma_n$.
  Alors σ et σ' sont conjuguées si et seulement si leurs matrices de permutation $T_\sigma, T_{\sigma'}$ sont semblables dans $Gl_n(\mathbb{K})$.

3. Quelques principes fondamentaux de combinatoire. —

- Lemme des bergers : Soit $\phi : A \to B$ tel que pour tout $x \in B$, $|\phi^{-1}(x)| = n$.
  Alors $|A| = n|B|$.
- App : Théorème de Lagrange : Pour G groupe fini et H sous-groupe de G,
  $|G/H|.|H| = |G|$.
- Pro : Soit p premier et $r \geq 1$. $\mathbb{F}_{p^r}$ possède $\frac{p^r-1}{2}$ carrés.
- Pro : Principe des tiroirs : Si k objets sont rangés dans $n \geq 1$ tiroirs, alors au moins l'un des tiroirs contient $\lceil \frac{k}{n} \rceil$ objets.
- App : L'équation $ax^2 + by^2 = 1$ possède au moins une solution dans $\mathbb{F}_{p^r} \times \mathbb{F}_{p^r}$.
- 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.

2. Dénombrement en théorie des groupes et sur les corps finis. —

1. Utilisation de la théorie des groupes. —

- Pro : Soit G un groupe fini agissant sur un ensemble X. $\forall x \in X$, on a :
  $|Stab(x)|.|Ord(x) = |G|$.
- Pro : (Formule des classes) Soit G un groupe fini agissant sur un ensemble fini X, et soit $X = \bigcup_{i=1}^{r} Orb(x_i)$ la partition de X en orbites sous l'action de G. On a :
  $|X| = \sum_{i=1}^{r} |Orb(x_i)| = \sum_{i=1}^{r} (G : Stab(x_i)) = \sum_{i=1}^{r} \frac{|G|}{|Stab(x_i)|}$.
- App : Soit G un groupe fini non abélien. On note $n(G)$ la proportion de couples $(x, y) \in G^2$ commutant. Alors $n(G) \leq \frac{5}{8}$.
- Cor : (Formule de Burnside) Le nombre r d'orbites de X sous l'action de G est :
  $r = \frac{1}{|G|} \sum_{g \in G} |X^g|$.
- App : Le nombre moyen de points fixes d'une permutation de Σ_n est 1.
- Pro : Soit p premier, G un p-groupe, et X un ensemble fini sur lequel G agit. On a alors $|X^G| \equiv |X| \ mod(p)$.
- App : Le centre d'un p-groupe G est non-trivial.
- App : Les groupes de cardinal p, p^2 sont toujours abéliens.
- App : Théorème de Cauchy : Soit G un groupe et p premier tq $p||G|$.
  Alors G possède un élément d'ordre p.

2. Dénombrement sur les corps finis. —

- Ex : Pour p premier et $q = p^r$, on a :
  $Card(GL_n(\mathbb{F}_q)) = (q^n - 1)..(q^n - q^{n-1}) = (q^n - 1)..(q-1).q^{\frac{n(n-1)}{2}}$.
  $Card(Sl_n(\mathbb{F}_q)) = (q^n - 1)..(q^2 - 1).q^{\frac{n(n-1)}{2}}$.
  $Card(PGl_n(\mathbb{F}_q)) = \frac{Card(Gl_n(\mathbb{F}_q)}{q-1}$ et $Card(PSl_n(\mathbb{F}_q)) = \frac{Card(Sl_n(\mathbb{F}_q)}{pcgd(q,n)}$.

- App : Quelques isomrphismes exceptionnels : $Gl_2(\mathbb{F}_2) = Sl_2(\mathbb{F}_2) = PGl_2(\mathbb{F}_2) \simeq \Sigma_3$
  $PGl_2(\mathbb{F}_3) \simeq \Sigma_4$, $PSl_2(\mathbb{F}_3) \simeq A_4$.
  $PGl_2(\mathbb{F}_4) = PSl_2(\mathbb{F}_4) \simeq A_5$
- Pro : Le groupe $UT_n(\mathbb{F}_p)$ des matrices trigonales supérieures avec des 1 sur la diagonale est un p-Sylow de $Gl_n(\mathbb{F}_p)$.
- Pro : Soit G un groupe et H un sous-groupe de G. Soit S un p-Sylow de H. Alors il existe un p-Sylow S' de G tel que $S = S' \cap H$.
- App : 1er Théorème de Sylow : Soit G un groupe fini de cardinal n, et p premier divisant n. Alors G admet un p-Sylow.

3. Fonctions multiplicatives. —

1. Indicatrice d'Euler. —

- Def : Une fonction $f : \mathbb{N}^* \to \mathbb{C}$ est multiplicative ssi pour tout $m \wedge n = 1$, on a $f(m.n) = f(m)f(n)$.
- Def : On définit l'indicatrice d'Euler de n, $\phi(n)$, comme le nombre de $1 \leq k \leq n$ qui sont premiers à n.
- Pro : ϕ est multiplicative.
- Pro : On a $\phi(n) = n.\Pi_{p\in\mathscr{P},p|n}(\frac{p-1}{p})$, et $n = \sum_{d|n}\phi(d)$
- App : $\mathbb{F}_{p^r}^*$ possède $\phi(d)$ éléments d'ordre d si $d|p^r - 1$ et 0 sinon. Ce sont les x racines de $X^d - 1$ et non-racines de $X^l - 1$ $\forall l|d, l < d$.
- App : $\mathbb{F}_{p^r}^*$ est cyclique.
- App : Théorème de Wedderburn : Tout anneau intègre fini (non supposé unitaire ni commutatif) est un corps.

2. Fonction de Moëbius. —

- Def : On définit la fonction de Moëbius $\mu : \mathbb{N}^* \to \{-1, 0, 1\}$ par :
  $\begin{cases} 0 \text{ si n a un facteur carré} \\ (-1)^r \text{ si } n = p_1\dot{p}_r \text{ avec } p_i \text{ premiers distincts} \end{cases}$.
- Pro : La fonction de Moëbius est multiplicative.
- Formule d'inversion de *Moëbius* : Pour $f, g : \mathbb{N}^* \to \mathbb{C}$, on a :
  $(g(n) = \sum_{d|n} f(d) \Leftrightarrow f(n) = \sum_{d|n} \mu(d)g(\frac{n}{d})$.
- App : $\phi(n) = \sum_{d|n} \mu(d)\frac{n}{d}$.
- App : Pour $r > 1$, la série $\sum_n \frac{1}{n^r}$ est une série absolument convergente, avec :
  $(\sum_n \frac{1}{n^r})(\sum_n \frac{\mu(n)}{n^r}) = 1$
- Def : On note $I(n, q)$ l'ensemble des polynômes irréductibles de degré n sur $\mathbb{F}_q$.
- Pro : $\forall n \geq 1$, $X^{q^n} - X = \Pi_{d|n}\Pi_{P\in I(d,q)}P$
- **Dev** : Pour tout $n \geq 1$, on a : $n.|I(n, q)| = \sum_{d|n} \mu(\frac{n}{d}).q^d$.
  On a ainsi $I(n, q) \sim \frac{q^n}{n}$ pour $n \to +\infty$.
- App : Test de Rabin : $P \in \mathbb{F}_q[X]$ est irréductible sur $\mathbb{F}_q$ ssi P divise $X^{q^n} - X$ et si $P \wedge X^{q^d} - X = 1$ pour tout d diviseur strict de n.

3. Symbole de Legendre. —

- Def : Pour tout $x \in \mathbb{F}_p$, on définit $(\frac{x}{p}) = \begin{cases} 1 \text{ si x} \in (\mathbb{F}_p^*)^2 \\ 0 \text{ si } x = 0 \\ -1 \text{ sinon} \end{cases}$ le symbole de Legendre.
- Pro : Le symbole de Legendre est une fonction pleinement multiplicative : $\forall m, n \in \mathbb{N}^*$, $(\frac{mn}{p}) = (\frac{m}{p})(\frac{n}{p})$.
- Ex : $(\frac{-1}{p}) = (-1)^{\frac{p-1}{4}}$.
- Pro : $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$.
- **Dev** : Loi de réciprocité quadratique : Soient p,m des nombres premiers impairs distincts.
  Alors $(\frac{p}{m}) = (\frac{m}{p}).(-1)^{\frac{p-1}{2}\cdot\frac{m-1}{2}}$.
- App : Les équations de la forme $x^2+py = q$, pour p premier impair et q non-multiple de p, ont une solution si et seulement si $(\frac{q}{p}) = 1$.
  Pour $x_0 \in \mathbb{Z}$ tel que $x_0^2 \equiv q\ mod(p)$, les solutions sont de la forme $(x_0+k.p, \frac{(x_0+k.p)^2-q}{p})$.
  La loi de réciprocité quadratique, les formules pour -1 et 2, et la division euclidienne permettent de toujours calculer le symbole de Legendre $(\frac{q}{p})$.
- Ex : $x^2 + 59y = 23$ n'a pas de solutions.

4. Utilisation des séries formelles. —

- Def : La série génératrice de $(a_n)_n$ est la série formelle $\sum_n a_n X^n$.
- Thm : (Partitions d'un entier en parts fixées) Soient $a_1, .., a_k$ premiers entre eux dans leur ensemble. Pour $n \geq 1$, on pose $u_n := Card(\{(x_1, .., x_k) \in \mathbb{N}^k \text{ tq } a_1x_1 + .. + a_kx_k = n\})$.
  Alors $u_n \sim \frac{1}{a_1..a_k}\frac{n^{k-1}}{(k-1)!}$
- Pro : Soit D_n le nombre de permutations de Σ_n sans points fixes (nombre de dérangements). On a : $\sum_{k=0}^n \binom{n}{k} D_{n-k} = n!$, $D_0 = 1$, ainsi que $D_n = n!(\sum_{k=0}^n \frac{(-1)^k}{k!})$. et d'involutions dans Σ_n.
- Thm : (Nombres de Bell) : Soit B_n le nombre de partitions de $\{1, .., n\}$.
  On a $B_{n+1} = \sum_{k=0}^n \binom{n}{k} B_k$, ainsi que $B_n = \frac{1}{e}(\sum_{k\geq 0} \frac{k^n}{k!})$.
- Thm : (Nombres de Catalan) On considère un ensemble E muni d'une loi de composition interne non-associative, et des $a_1, .., a_n \in E$ distincts.
  Alors le nombre C_n de valeurs possibles du produit $a_1..a_n$ selon le parenthésage vaut : $C_n = \frac{\binom{2n-2}{n-1}}{n}$.

Références

De Biasi : Ensembles finis, cardinal, crible, cardinal d'un produit, alphabet braille, tirage avec remise, exemples. Arrangements, permutations, dénombrement, coeffs binomiaux, formule du binôme, nombre de surjections, nombre de dérangements, tiercé. Lemme des Bergers.
Perrin : Nombre de carrés de F_q^*, Th de Lagrange, Principe des tiroirs, $ax^2 + by^2 = 1$ a

une sol dans $\mathbb{F}_q$. Cardinalité sur les corps finis, isomorphismes exceptionnels, $UTN(\mathbb{F}_p)$, 1er Th de Sylow.
FGN (Algèbre 1) : Fonction de Moëbius, formule d'inversion de Moëbius, Polynômes irréductibles de degré n sur $\mathbb{F}_q$.(Dev), Proba que deux entiers soient premiers entre eux. Nombre de dérangements, Nombres de Bell, Problèmes de parenthésages.
Ulmer : Relation orbite-stabilisateur, formule des classes, formule de Bernstein, nb moyen de points fixes d'une permutation, p-groupes, Th de Cauchy.
Caldero, Germino : Nombre de matrices de rang r de $M_n(\mathbb{F}_p)$, nombre de p-Sylow de $Gl_n(\mathbb{F}_p)$. Symbole de Legendre, Loi de réciprocité quadratique.(Dev)
Saux-Picart : Série génératrice, nombres de Catalan.
FGN (Algèbre 2) : Partitions en parts fixées.
Gourdon : Indicarice d'Euler.
Sans Ref : Principe de double-comptage. Th de Wedderburn, Th de Brauer.(Dev)

May 27, 2017

Vidal Agniel, École normale supérieure de Rennes