145 - Méthodes combinatoires, problèmes de dénombrement.

Sauf mention contraire, tous les ensembles seront supposés finis.

1 Propriétés ensemblistes

1.1 Propriétés de base

Lemme 1 (du berger)**.** *Soient deux ensemblesX et Y et une surjection* $f : X \to Y$ *telle que les ensembles* $f^{-1}(y)$, *pour* $y \in Y$, *aient tous même cardinal* c, *alors on a* $|X| = c|Y|$.

Proposition 1. *Soient* E *et* F *de cardinaux resp.* n *et* p. *Alors* $|F^E| = p^n$ *et* $|P(E)| = 2^n$.

Proposition 2. $|\mathfrak{S}_n| = n!$
$|injections\ E \to F| = \frac{n!}{(n-p)!}$
$|parties\ de\ E\ \grave{a}\ p\ \acute{e}l\acute{e}ments| = \binom{n}{p}$

Proposition 3. $|F \times G| = |F||G|$.

Théorème 1 (Formule de Poincaré)**.**

$$\left|\bigcup_{i=1}^{n} E_i\right| = \sum_{k=1}^{n}\left(\sum_{1\leq i_1<\cdots<i_k\leq n}(-1)^{k+1}\left|E_{i_1}\cap\cdots\cap E_{i_k}\right|\right)$$

1.2 Propriétés des coefficients binomiaux

Proposition 4. *Triangle de Pascal,* $\sum_{k=p}^{n}\binom{k}{p} = \binom{n+1}{p+1}$.

Proposition 5 (Multinôme de Newton)**.** *Soit* A *un anneau et* $(x_1, \ldots, x_m)$ *des éléments de* A *qui commutent. Alors* $(x_1 + x_2 + x_3 + \cdots + x_m)^n = \sum_{k_1+k_2+k_3+\ldots+k_m=n}\binom{n}{k_1,k_2,k_3,\ldots,k_m}x_1^{k_1}x_2^{k_2}x_3^{k_3}\ldots x_m^{k_m}$.

Corollaire 1. *Calcul de* $\sum_{k=0}^{n}\binom{n}{k} = 2^n$, $\sum_{k=0}^{n}k\binom{n}{k} = n2^{n-1}$ *(par série génératrice)...*

Application. Un ensemble fini admet le même nombre de parties paires que de parties impaires (calcul de $(1-1)^n$).

Théorème 2 (Tchebycheff). *Il existe des réels $0 < a < A$ tels que $\forall x \geq 1,\ a\frac{x}{\ln x} \leq \pi(x) \leq A\frac{x}{\ln x}$.*

2 Quelques outils importants

2.1 Principe des tiroirs

Proposition 6 (Dirichlet). *Soient N et R deux ensembles tq $|N| = n > r = |R|$, et $f : N \to R$. Alors f n'est pas injective et $\exists a \in R : |f^{-1}(a)| \geq [n/r]$.*

Application (Kronecker, Arnaudiès p. 127, FGN). Un polynôme unitaire non constant irréductible sur $\mathbf{Q}$ dont toutes les racines sont de module ≥ 1 est un polynôme cyclotomique.

Application (Approximation des rationnels, FGN). Soient $x \in \mathbf{R}$ et $Q \in \mathbf{Q}^*$, alors il existe $p \in \mathbf{Z}$ et $q \in [\![1, Q]\!]$ tels que $|x - \frac{p}{q}| \leq \frac{1}{qQ}$.

Application. Soit $\alpha \in]1,2[$ transcendant. Alors il existe une suite de polynômes $(P_n)_n$ non nuls à coefficients dans $\{-1,0,1\}$ tels que $P_n(\alpha) \to 0$.

Suite exemples Aigner ?

2.2 Double comptage

Application. Nombre de diviseurs.

Application (Comtet p. 44). $\sum_{A,B\subset N} |A \cap B| = n4^{n-1}$.

2.3 Séries génératrices

Dérangements, progressions arithmétiques (TD), nombres de Catalan, partitions de $\{1,\ldots,n\}$ (nombres de Stirling et k-partitions, application au dénombrement des classes de similitude), partitions de n.

3 Dénombrement et structures algébriques finies

3.1 Groupes

Lagrange, Sylow (RMS 117-1 ?) et $|Gl_n(\mathbf{F}_p)|$, $\mathfrak{A}_5$ simple, équation aux classes, formule de Burnside et application au collier de perles...

3.2 Corps

Poly au plus n racines, sous-gpe corps cyclique, carrés Codes correcteurs (Hamming, Singleton...).

3.3 Représentations ?

Références

Aigner
Comtet
RDO
FGN1
Perrin
Combes