190 Méthodes combinatoires, problèmes de dénombrement.

Refs : [DeBia] de Biasi : Mathématiques pour le CAPES et l'agrégation interne
[Com] Combes Algèbre et géométrie. [Per] Perrin, Cours d'Algèbre
[Ulm] Ulmer Théorie des groupes. [Sene] Serre Cours d'arithmétique.
[FGN1] Algèbre 1

Devts : 44 45 Chevalley Warning [Sene].
55 56 57 Polys irred sur $\mathbb{F}_q$ [FGN1]
62 Nombres de Bell.

I. Quelques outils de dénombrement [Bia]

1) Ensembles finis.

[Bia] 3,6.

Def 1 : On appelle cardinal d'un ensemble E la classe des ensembles en bijection avec E. On dit que E est fini s'il est en bijection avec un ensemble de la forme $[\![1,n]\!]$ pour $n\in\mathbb{N}^*$ (on notera alors n son cardinal).

Rq 2 : On doit adjoindre à la définition le cas de l'ensemble vide, par définition fini et de cardinal 0.

Prop 3 : Soient E et F deux sous-ensembles finis d'un ensemble S alors $E\cap F$ est fini et on a $|E\cup F| = |E|+|F|-|E\cap F|$.

Prop 4 : Si $(E_i)_{i\in[\![1,n]\!]}$ est une famille de sous-ensembles disjoints finis d'un ensemble S, alors $\left|\bigcup_{i=1}^n E_i\right| = \sum_{i=1}^n |E_i|$

Prop 5 : (Formule du crible) Si $(E_i)_{i\in[\![1,n]\!]}$ une famille de sous-ensembles finis. Alors on a

$$\left|\bigcup_{i=1}^n E_i\right| = \sum_{i=1}^n |E_i| - \sum_{1\le i<j\le n} |E_i\cap E_j| + \dots + (-1)^n \left|\bigcap_{i=1}^n E_i\right|$$
$$= \sum_{k=1}^n \sum_{1\le i_1<\dots<i_k\le n} (-1)^{k-1} |E_{i_1}\cap\dots\cap E_{i_k}|$$

Appl 6 : Il y a 684 nombres à 3 chiffres contenant au moins l'un des chiffres 0, 3, 6, 9.

Théo 7 : Le produit cartésien de p ensembles finis $A_1,\dots,A_p$ est fini, et de cardinal $\prod_{i=1}^p |A_i|$.

Théo 8 : Si E, F sont deux ensembles finis l'ensemble des fonctions de E vers F est un ensemble fini, de cardinal $|F|^{|E|}$

Ap 9. Comme l'ensemble des fonctions $E\to\{0,1\}$ est en bijection avec $\mathcal{P}(E)$, on a $|\mathcal{P}(E)| = 2^{|E|}$.

Rq 10 : On peut montrer qu'un ensemble quelconque E n'est jamais en bijection avec l'ensemble de ses parties, ce qui est clair pour un ensemble fini.

Appl 11 : Il y a $2^6 = 64$ signes possibles dans l'alphabet braille.

Appl 12 : En tirant p boules dans un ensemble de n boules, il y a n^p possibilités.

2) Arrangements, permutations et combinaisons.

Def 13 : Soient $n\in\mathbb{N}^*$ et $p\le n$ et E un ensemble de cardinal n, un p-arrangement est une injection $[\![1,p]\!]\hookrightarrow E$.
On peut de même définir un arrangement comme un sous-ensemble de E de cardinal p, ordonné.

Théo 14 : Le nombre de p-arrangements de E est $A_n^p = \frac{n!}{(n-p)!}$
(moralement, on choisit le premier élément, avec n choix, puis le second, avec $n-1$ choix, ...).

Appl 15 Dans un tirage sans remise, il y a A_n^p possibilités.

Def 16 : Dans le cas où $p=n$, on parle de permutation : une permutation est une injection de $[\![1,n]\!]$ dans E.

Cor 17 : Comme on parle d'ensembles finis, une telle injection est une bijection. Par composition on peut associer à toute permutation une unique bijection $E\to E$. On a donc $|\mathfrak{S}(E)| = n! = A_n^n$. On obtient le cardinal du groupe symétrique d'indice n.

Def 18 : On définit une p-combinaison de E comme un sous-ensemble de E à p éléments.

Rq 19 : On peut associer un sous-ensemble de E de cardinal p à une classe d'équivalence d'injections $[\![1,p]\!]\hookrightarrow E$ (on identifie les images). On obtient ainsi

Prop 20 : Le nombre de p-combinaisons de E est $\binom{n}{p} := \frac{n!}{p!(n-p)!}$

Prop 21 : Pour $n\ge1$ et $1\le p\le n$, on a
- $\binom{n}{p} = \binom{n}{n-p}$ — $\binom{n-1}{p}+\binom{n-1}{p-1} = \binom{n}{p}$ (Formule de Pascal).
- $\binom{n}{p} = \frac{n}{p}\binom{n-1}{p-1} = \frac{n}{n-p}\binom{n-1}{p} = \frac{n-p+1}{p}\binom{n}{p-1}$

Appl22 : Une course comportant 20 chevaux admet 1140 tiercés (dans le désordre)

Prop23 : Soit A un anneau, $a, b \in A$ qui commutent et $n \in \mathbb{N}$, on a

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

Cor24 : On a $\sum_{k=0}^{n}\binom{n}{k} = 2^n$, on retrouve le cardinal de $\mathcal{P}(E)$.

Appli25 : La formule $(q+1)^n = \sum_{n=0}^{n}\binom{n}{k} q^k$ permet de retrouver les formules

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}, \quad \sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}, \quad \sum_{k=1}^{n} k^3 = \left(\frac{n(n+1)}{2}\right)^2$$

Appl26 : Le nombre σ_p^n de surjections $[\![1,n]\!] \to [\![1,p]\!]$ est

$$\sigma_p^n = \sum_{k=0}^{p}(-1)^{p-k}\binom{p}{k} k^n.$$

Appli27 : Le nombre de dérangements d'un ensemble à n éléments est

$$d_n = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}.$$

3) Autres principes.

Prop28 : (Lemme des Bergers) Soient E, F deux ensembles finis, $\varphi : E \to F$ une application, si $\forall x \in B \; |\varphi^{-1}(x)| = n$, alors $|A| = n|B|$

Appl29 : (Formule de Lagrange) Si G est un groupe fini de cardinal n, et H un sous groupe de G de cardinal p, on a $n = p[G:H]$, en particulier, p divise n.

Prop30 (Principe du double comptage) Soient E, F deux ensembles finis P une propriété sur $E \times F$, on a

$$|\{(x,y) \in E\times F \,/\, P(x,y)\}| = \sum_{x \in E} |\{y \in F \,/\, P(x,y)\}| = \sum_{y \in F} |\{x \in E \,|\, P(x,y)\}|$$

[Gou] 43-44

Appl31 (Formule de Burnside) Si $G \circlearrowright X$, G fini de cardinal n, X de cardinal p fini, on a

$$|X/G| = \frac{1}{|G|}\sum_{g \in G} |X^g| = \frac{1}{|G|}\sum_{g \in G} |\{x \in X \,|\, g.x = x\}|.$$

Ex32 : Avec 4 perles bleues, 3 blanches et 2 vertes, on peut faire 76 colliers.

Prop33 (Principe des tiroirs) Si k objets sont rangés dans n tiroirs alors au moins un des tiroirs contient $\lceil \frac{k}{n} \rceil$ objets.

Ex34 : Parmi trois personnes sur terre, deux au moins sont dans le même hémisphère.

II. Dénombrement en algèbre et théorie des nombres.

1) Théorie des groupes. [Ulm]

On a déjà vu le théorème de Lagrange et la formule de Burnside. On fixe ici G fini agissant sur X fini, on a

Théo35 (Formule des orbites) Pour $x \in X$, on a $|O(x)| = |G|/|Stab_G(x)|$, et donc $|X| = \sum_{x \in C} |O(x)|$. où C est un ensemble de représentants des orbites.

App36 : Soit $m(G)$ la proportion de couples (x,y) de G^2 commutant, on a $m(G) \leq \frac{5}{8}$ si G est non abélien.

App37 Le nombre moyen de points fixes de $\sigma \in \mathfrak{S}_n$ est 1.

Prop38 Pour p un nombre premier, G un p-groupe, alors $|X^G| \equiv |X| \, [p]$

Appl39 : Le centre d'un p-groupe est non trivial, ainsi un groupe d'ordre p ou p^2 est non trivial.

2) Corps finis. [Perr]

On suppose ici p premier et $n \in \mathbb{N}$, on pose $q = p^n$, on a

Théo40 : On a les cardinaux suivants :

- $|GL_n(\mathbb{F}_q)| = \prod_{i=0}^{n-1}(q^n - q^i) = q^{\frac{n(n-1)}{2}} \prod_{i=0}^{n-1}(q^{n-i}-1)$
- $|SL_n(\mathbb{F}_q)| = |PGL_n(\mathbb{F}_q)| = |GL_n(\mathbb{F}_q)|/q-1.$
- $|PSL_n(\mathbb{F}_q)| = |SL_n(\mathbb{F}_q)|/pgcd(n, q-1).$
- $|\mathbb{P}^1(\mathbb{F}_q)| = q+1.$

Appli41 : L'ensemble des matrices triangulaires supérieures à diagonale 1 forme un p-sous groupe de Sylow de $GL_n(\mathbb{F}_p)$.

Appli42 : Tout groupe fini admet des p-Sylow.

Appli43 (Isomorphismes exceptionnels)

- $GL_2(\mathbb{F}_2) \simeq SL_2(\mathbb{F}_2) \simeq PSL_2(\mathbb{F}_2) \simeq \mathfrak{S}_3$
- $PGL_2(\mathbb{F}_3) \simeq \mathfrak{S}_4$, $PSL_2(\mathbb{F}_3) \simeq \mathfrak{A}_4$
- $PGL_2(\mathbb{F}_4) \simeq PSL_2(\mathbb{F}_4) \simeq \mathfrak{A}_5$
- $PGL_2(\mathbb{F}_5) \simeq \mathfrak{S}_5$, $PSL_2(\mathbb{F}_5) \simeq \mathfrak{A}_5$.

[Serre]

Théo44 (Chevalley Warning) Soit $(f_\alpha)_{\alpha\in A} \in \mathbb{F}_q[X_1,\dots,X_n]$ une famille de polynômes à n variables telle que $\sum_{\alpha\in A} d^\circ f_\alpha < n$ et soit V l'ensemble de leurs zéros communs dans $\mathbb{F}_q^n$. alors $|V| \equiv 0\ [p]$ DVP

Cor45: (Erdős Ginzburg Ziv) Parmi $2n-1$ entiers $a_1,\dots,a_{2n-1}$, on peut en choisir n dont la somme est divisible par n.

3) Fonctions multiplicatives.

[Perrin]

Déf46: On dit qu'une fonction arithmétique (fonction $\mathbb{N}^* \to \mathbb{C}$) est multiplicative si $m \wedge n = 1 \Rightarrow \varphi(mn) = \varphi(m)\varphi(n)$.

Déf47: Pour $n\in\mathbb{N}^*$, on pose $\varphi(n)$ le nombre d'entiers de $[\![1,n]\!]$ premiers avec n, c'est l'indicatrice d'Euler.

Ex48: Si p est premier, $\varphi(p)=p-1$, et $\varphi(p^\alpha)=p^{\alpha-1}(p-1)$, $\alpha\in\mathbb{N}^*$.

Prop49: φ est multiplicative, si $2\le n = p_1^{\alpha_1}\cdots p_r^{\alpha_r}$ est la décomposition de n en produit de facteurs premiers, on a $\varphi(n) = n\prod_{i=1}^{r} \left(1-\frac{1}{p_i}\right)$.

Prop50: Pour $n\geq 2$, $n=\sum_{d|n}\varphi(d)$

Appl51: Si K est un corps fini, K^* est un groupe cyclique.

Déf52: Pour $n \geq \mathbb{N}^*$, on définit $\mu(n)\in\{0,\pm1\}$ par $\mu(1)=1$, $\mu(n)=0$ si n est divisible par un carré, et $\mu(p_1\cdots p_r)=(-1)^r$ si les p_i sont premiers deux à deux distincts.

Ex53: $\mu(42)=\mu(2\times3\times7)=-1$.

Prop54: La fonction μ est multiplicative, pour $n\geq2$ et $\sum_{d|n}\mu(d)=0$

Théo55: Soient $f:\mathbb{N}^*\to\mathbb{R}$, $g:=\sum_{d|n} f(d)$, alors on a la formule d'inversion de Möbius. $\forall n\geq1,\ f(n)=\sum_{d|n}\mu\left(\frac{n}{d}\right)g(d)$. DVP

Appli56: Pour q primaire, on a, par $P_q(d)$ l'ensemble des polynômes irréductibles de deg d unitaires sur $\mathbb{F}_q$, on a $X^{q^n}-X=\prod_{d|n}\prod_{P\in P_q(d)} P(X)$. Si $I(n,q)=|P_q(d)|$, on a

$$I(n,q)=\frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right) q^d$$

équivalent à $\frac{q^n}{n}$

Cor57: Il existe des polynômes irréductibles de tout degré sur $\mathbb{F}_q$.

III Séries entières et séries formelles.

1) Séries formelles.

[FGN1]

Déf58: Soit $(a_n)\in K^{\mathbb{N}}$. On définit sa série génératrice par $G(S):=\sum_{n\geq0} a_n X^n \in K[[X]]$.

Appli59 Partition d'un entier en parts fixées. Soient $a_1,\dots,a_k\in\mathbb{N}^*$, premiers entre eux dans leur ensemble. Pour $n\geq1$, on note

$$u_n = \mathrm{Card}\{(x_1,\dots,x_k)\in\mathbb{N}^k \mid a_1x_1+\dots+a_kx_k=n\}.$$

Alors on a $u_n \underset{n\to\infty}{\sim} (a_1\cdots a_k)^{-1}\frac{n^{k-1}}{(k-1)!}$.

Appl60: (Nombres de Catalan) Si C_n désigne le nombre de parenthésages possibles d'un produit de n termes. Alors $C_n=\sum_{k=1}^{n-1} C_k C_{n-k}$. On obtient alors $C_n=\frac{1}{n}\binom{2n-2}{n-1}$.

Appl61: Il y a $\sum_{p+2q=n}\frac{n!}{2^q\, p!\, q!}$ involutions d'un ensemble à n éléments.

2) Séries entières

Prop62 (Nombres de Bell) Pour $n\in\mathbb{N}^*$, on note B_n le nombre de partitions distinctes de $[\![1,n]\!]$, avec par convention $B_0=1$. Alors

(i) La série entière $\sum \frac{B_n}{n!} z^n$ a un rayon de convergence $R>0$ et sa somme vérifie $\forall z\in]-R,R[\quad f(z)=e^{e^z-1}$ DVP

(ii) On a $B_k=\frac{1}{e}\sum_{n=0}^{\infty}\frac{n^k}{n!}$