

I. Notion de dénombrement et de combinatoire

[Tau07, ChII, p5]

I. A. Bijections entre cardinaux

Ensemble fini, exemples, cardinal, $\text{card}(F) \leq \text{card}(E)$ si $F \subset E$, deux ensembles de même cardinal sont en bijection

Union d'ensembles disjoints finis, ensemble privé d'une partie.

Exemple : pour $n \in \mathbb{N}^*$, on appelle dérangement de n une permutation de $\llbracket 1, n \rrbracket$ sans point fixe. On note d_n le nombre de dérangements de n . On a $n! = \sum_{k=0}^n \binom{n}{k} d_k$

Cardinal de $A \cup B$ dans le cas général, de $A \times B$, lemme des bergers

Cardinal de l'ensemble des fonctions (injectives, surjectives) de E dans F

Parties de E

I. B. Coefficients binomiaux et combinatoire

Définition, formules classiques (somme des coefficients binomiaux, formule de PASCAL, de VANDERMONDE)

II. Dénombrement en algèbre

II. A. Dénombrement sur un corps fini

[Rom17, §13.6–7, p429–435] [Per96, §III.2/IV.5, p72/105]

Soit $p \in \mathcal{P}$ et $q = p^n$ où $n \in \mathbb{N}^*$. On note $\mathbb{F}_q$ le corps à q éléments.

Cardinaux de $\mathcal{GL}_n(\mathbb{F}_q)$, $\mathcal{SL}_n(\mathbb{F}_q)$, $\mathcal{PGL}_n(\mathbb{F}_q)$, $\mathcal{PSL}_n(\mathbb{F}_q)$

On note $\mathbb{F}_q^2 = \{x^2 \mid x \in \mathbb{F}_q\}$ et $\mathbb{F}_q^{*2} = \mathbb{F}_q^2 \cap \mathbb{F}_q^*$.

PROPOSITION 1. Si $p = 2$, alors $\mathbb{F}_q^2 = \mathbb{F}_q$. Sinon, on a $|\mathbb{F}_q^2| = \frac{q+1}{2}$.

APPLICATION 2. Pour $a, b \in \mathbb{F}_p^*$ et $c \in \mathbb{F}_p$, $ax^2 + by^2 = c$ admet des solutions dans $\mathbb{F}_p^2$.

On aimerait savoir rapidement si un entier a donné est un carré modulo p , donc savoir si $x^2 \equiv a \pmod{p}$ admet ou non une solution entière.

DÉFINITION 3. [SYMBOLE DE LEGENDRE]

Soit $a \in \mathbb{Z}$, on appelle symbole de LEGENDRE (de a modulo p) l'entier :

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } x^2 \equiv a \pmod{p} \text{ est résoluble et } p \nmid a \\ 0 & \text{si } p \mid a \\ -1 & \text{sinon} \end{cases}$$

On suppose dans la suite p impair.

PROPOSITION 4. On a $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$ pour tout $a \in \mathbb{Z}$.

EXEMPLE 5. -1 est un carré modulo q si et seulement si $q \equiv 1 \pmod{4}$.

THÉORÈME 6. [LOI DE RÉCIPROCITÉ QUADRATIQUE]

Soient $p \neq q$ des nombres premiers impairs. Alors $\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}}$.

PROPOSITION 7. Pour p premier impair, on a $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. Ainsi 2 est un carré modulo p si et seulement si $p \equiv \pm 1 \pmod{8}$.

EXEMPLE 8. $\left(\frac{26}{307}\right) = \left(\frac{2}{307}\right) \left(\frac{13}{307}\right) = -(-1)^{\frac{13-1}{2} \frac{307-1}{2}} \left(\frac{307}{13}\right) = -\left(\frac{8}{13}\right) = -\left(\frac{2}{13}\right) \left(\frac{4}{13}\right) = -1$
Ainsi 26 n'est pas un carré modulo 307.

II. B. Actions de groupes

[Rom17, §1.6–10/5.6, p19/148]

Soit $(G, \cdot)$ un groupe et X un ensemble.

DÉFINITION 9. [ACTION D'UN GROUPE SUR UN ENSEMBLE]

On dit que G opère à gauche sur X si on a une application $G \times X \longrightarrow X$, $(g, x) \longmapsto g.x$ telle que $\forall g, h \in G, \forall x \in X, g.(h.x) = (gh).x$ et $\forall x \in X, 1.x = x$.

On considère une action de G sur X .

EXEMPLE 10.

- G opère sur lui-même par translation à gauche ($g.h = gh$), par conjugaison ($g.h = ghg^{-1}$),
- $\mathfrak{S}(X)$ opère naturellement sur X : $\sigma.x = \sigma(x)$.

DÉFINITION 11. [ORBITES, TRANSITIVITÉ, FIDÉLITÉ]

- Pour $x \in X$, on appelle orbite de x et on note $O(x)$ l'ensemble $G.x = \{g.x \mid x \in X\}$. On note $\mathcal{O}$ l'ensemble des orbites de X . C'est une partition de X .
- On dit que l'action est transitive s'il n'y a qu'une seule orbite pour l'action de G sur X , c'est-à-dire si $\forall x \in X, O(x) = X$.

DÉFINITION 12. [STABILISATEUR, ACTION LIBRE]

On appelle stabilisateur de $x \in X$ le groupe $\text{Stab}(x) = \{g \in G \mid g.x = x\}$.

On dit que G opère librement sur X si $\text{Stab}(x) = \{e\}$ pour tout $x \in X$.

PROPOSITION 13. Soit $x \in X$. L'application $g \in G \mapsto g.x \in O(x)$ a pour noyau $\text{Stab}(x)$. L'application quotient est alors une bijection de $G/\text{Stab}(x)$ dans $O(x)$. En particulier, si $|G| < +\infty$, on a $\forall x \in X, |O(x)| = [G : \text{Stab}(x)] = \frac{|G|}{|\text{Stab}(x)|}$.

APPLICATION 14. [CLASSES DE CONJUGAISONS DE $\mathfrak{S}_n$]

Deux permutations de $\mathfrak{S}_n$ sont conjuguées si et seulement si elles ont même type.

Le nombre de classes de conjugaison est le nombre de partitions de n .

Calcul du cardinal de la classe de conjugaison associée au type $(\ell_1, \dots, \ell_m)$. Deux calculs proposés, où l'on note $p_k = \text{card}(\{i \mid \ell_i = k\})$:

$$\left(\prod_{i=1}^m \binom{n - \sum_{j < i} \ell_j}{\ell_i} (\ell_i - 1)! \right) \times \left(\prod_{k=1}^n \frac{1}{p_k!} \right) = \frac{n!}{\prod_{k=1}^n k^{p_k} p_k!}$$

Dans la suite de cette partie on suppose G et X finis.

COROLLAIRE 15. [ÉQUATION AUX CLASSES]

Si $|G| < +\infty$, choisissons pour chaque orbite O un représentant x_O . Alors on a :

$$|X| = \sum_{O \in \mathcal{O}} |O| = \sum_{O \in \mathcal{O}} \frac{|G|}{|\text{Stab}(x_O)|}$$

APPLICATION 16. [CARDINAL DE $\mathcal{D}_n(\mathbb{F}_q)$]

Soit $n \in \mathbb{N}, q = p^r$ où p premier, $r \neq 0$. Soit $\mathcal{D}_n(\mathbb{F}_q)$ l'ensemble des matrices diagonalisables de $\mathbb{F}_q$. Alors en posant $|\mathcal{GL}_0(\mathbb{F}_q)| = 1$, on a :

$$|\mathcal{D}_n(\mathbb{F}_q)| = \sum_{n_1 + \dots + n_q = n} \frac{|\mathcal{GL}_n(\mathbb{F}_q)|}{\prod_{i=1}^q |\mathcal{GL}_{n_i}(\mathbb{F}_q)|}$$

COROLLAIRE 17. [FORMULE DE BURNSIDE]

$$|\mathcal{O}| = \frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g)|$$

APPLICATION 18. On peut colorier les 6 faces (toutes identiques) d'un cube avec 3 couleurs de 57 manières différentes.

III. Dénombrement en analyse

III. A. Utilisation des probabilités

[Ouv08]

Lien entre probabilité uniforme sur un ensemble fini et cardinal d'une partie

Application à la probabilité de retour en 0 au bout de $2n$ pas de la marche aléatoire simple $\rightarrow$ application à la récurrence/transience

Formule du crible, nombre de dérangements

APPLICATION 19. On a $d_n = n! \sum_{k=0}^n \frac{(-1)^k}{k!}$.

III. B. Séries génératrices

[FGN07, §1.2–6, p6] [Rom17, Ch2, p53–55/73]

Série génératrice ordinaire, exponentielle

Équivalent du nombre de solutions S_n de $\sum \alpha_i n_i = n$

[Gou08, §4.4, p249]

Idee : relation de récurrence lors d'un dénombrement $\rightarrow$ introduction de la série génératrice ordinaire ou exponentielle pour obtenir une équation fonctionnelle, différentielle, et déterminer la fonction associée. On vérifie que le rayon de convergence est positif, puis on identifie les coefficients

COROLLAIRE 20. Le nombre de permutations de $\mathfrak{S}_n$ ayant exactement r points fixes est $\binom{n}{r} d_{n-r} = \frac{n!}{r!} \sum_{k=0}^{n-r} \frac{(-1)^k}{k!}$.

APPLICATION 21. En utilisant un déterminant circulant, on montre qu'il y a plus (resp. moins) de dérangements impairs que de dérangements pairs dans $\mathfrak{S}_n$ lorsque n est pair (resp $n > 1$ impair).

Nombres de CATALAN, nombres de BELL

COMMENTAIRES

Il faut aller piocher dans plusieurs références pour cette leçon. Voir aussi [FGN07, BMP05].

QUESTIONS

Q Questions autour de la loi de réciprocité quadratique : où intervient l'hypothèse p et q impairs ? Caractérisation des carrés, à la fin comment passer de l'inégalité modulo p à celle dans $\mathbb{Z}$, réduction des formes quadratiques en caractéristique différente de 2. Que se passe-t-il si $p = 2$? À quoi sert la loi de réciprocité quadratique ? À quoi ça sert de savoir si un élément est un carré dans $\mathbb{F}_q$?

Q Quelle est la probabilité que deux entiers soient premiers entre eux ?

R $6/\pi^2$.

Q Soit $\mathcal{H}_{d,n}$ l'ensemble des polynômes homogènes de degré d à n variables. Quelle est sa dimension ?

R Une base de $\mathcal{H}_{d,n}$ est $(X_{i_1} \dots X_{i_d})_{i_1, \dots, i_d \in \llbracket 1, n \rrbracket}$, ou encore $(X_1^{\alpha_1} \dots X_n^{\alpha_n})_{\sum_i \alpha_i = d}$.

On cherche donc le nombre de $(\alpha_i)_i$ tels que $\sum_i \alpha_i = d$.

Prenons d points alignés, que l'on veut séparer en n morceaux. Pour cela on rajoute $n - 1$ points à ces points aux endroits de séparation. Finalement la dimension est :

$$\binom{d+n-1}{n-1}$$

Q Montrer que $\varphi(n) = \sum_{d|n} \frac{\mu(d)}{d}$. Ou plutôt montrer que si $g(n) = \sum_{d|n} f(d)$ alors $f(n) = \sum_{d|n} g(d) \mu(n/d)$.

Q Dénombrer les polynômes de degré 3 à 3 variables.

Q Dénombrer les permutations de $\mathfrak{S}_n$ sans point fixe (voir aussi la formule de PASCAL dans le [Rom17]).

Q Sur $\mathfrak{S}_n$, on dit qu'une permutation σ est un zig-zag si pour $i \in \llbracket 1, n-1 \rrbracket$, $\sigma(i) \notin \llbracket \sigma(i-1), \sigma(i+1) \rrbracket$. Montrer qu'il y a autant de zig-zag descendants qu'ascendants (faire une réflexion ...). Donner une relation de récurrence sur le cardinal des zig-zags (on regarde les ascendants ...).

Q Interpréter de manière combinatoire la formule du triangle de PASCAL.

Q Dénombrer le nombre de mots bien parenthésés de longueur $2n$?

R On trouve les nombres de CATALAN. On peut par exemple utiliser les chemins sous-diagonaux pour trouver la relation de récurrence $c_{n+1} = \sum_{d=0}^n c_d c_{n-d}$.

Q Combien y a-t-il de droites / de plans dans $\mathbb{F}_q^n$?

BIBLIOGRAPHIE

[BMP05] V. BECK, J. MALICK et G. PEYRÉ : *Objectif Agrégation*. H&K, 2^{ème} édition, 2005.

[FGN07] S. FRANCINO, H. GIANELLA et S. NICOLAS : *Oraux X-ENS - Algèbre 1*. Cassini, 2007.

[Gou08] X. GOURDON : *Les maths en tête - Analyse*. Ellipses, 2^{ème} édition, 2008.

[Ouv08] J.-Y. OUVRARD : *Probabilités : Tome 1*. Cassini, 2^{ème} édition, 2008.

[Per96] D. PERRIN : *Cours d'algèbre*. Ellipses, 1996.

[Rom17] J.-E. ROMBALDI : *Mathématiques pour l'agrégation : Algèbre et géométrie*. De Boeck, 2017.

[Tau07] P. TAUVEL : *Mathématiques générales pour l'agrégation*. Masson, 2007.