MÉTHODES COMBINATOIRES ET PROBLÈMES DE DÉNOMBREMENT

Leçon 190

HOSTEIN Matthias
Préparation à l'agrégation
Université de Rennes
Année 2023 - 2024

Table des matières

Introduction historique : Pascal et le Chevalier de Méré

Le dénombrement en mathématiques est une discipline exigeante qui nécessite beaucoup de soin dans les raisonnements. Les techniques de dénombrement sont notamment utilisées pour décrire le hasard au XVII^{e} siècle, époque où les jeux de dés et de cartes étaient très populaires, comme en témoigne la correspondance entre Blaise Pascal et le Chevalier de Méré. Le chevalier de Méré posait ce paradoxe à Pascal : il doit être aussi avantageux de parier sur l'apparition d'au moins un 6 en lançant 4 fois un dé (à 6 faces et bien équilibré), que de parier sur l'apparition d'au moins un double 6 en lançant 24 fois 2 dés ! Cependant, il a remarqué par son expérience aux jeux de dés, qu'il était en fait plus avantageux de parier sur le premier cas que sur le second. Comment cela s'explique-t-il ? Pascal répond à cette question en *dénombrant* les possibilités favorables dans les deux jeux et en divisant par le nombre total de possibilités, et il trouve les résultats suivants :

— Probabilité de gagner au premier jeu : $1 - \left(\frac{5}{6}\right)^4 \approx 0,51774691358$;

— Probabilité de gagner au second jeu : $1 - \left(\frac{35}{36}\right)^{24} \approx 0,49140387613$!

Les arguments « d'homothétie » ne sont donc clairement pas valables en combinatoire ! La *modélisation* du problème de hasard du chevalier de Méré n'était pas bonne. Pascal disait d'ailleurs de lui, dans une lettre à Pierre de Fermat qu'il « avait très bon esprit mais n'était pas géomètre ». Essayons donc d'être un peu plus rigoureux que le chevalier de Méré en étudiant correctement les notions clefs de la combinatoire et en analysant rigoureusement quelques problèmes de dénombrement.

1 Cardinaux et dénombrements élémentaires [Gou21]

1.1 Notion de cardinal d'un ensemble fini

La notion de « cardinal » d'un ensemble est ce qui va nous permettre de dire *combien* d'éléments sont dans l'ensemble. L'outil principal permettant de définir cet objet est la notrion de *bijection*.

Définition 1.1 (Ensemble fini)**.** On dit qu'un ensemble E est *fini* si $E = \emptyset$ ou s'il existe $n \in \mathbb{N}^*$ et une bijection $f : E \longrightarrow [\![1, n]\!]$.

À ce stade, on serait tenté de dire que n est le nombre d'éléments de E. Cependant, ce n n'est pas forcément unique ! Il faut donc prouver cette unicité :

Lemme 1.2. Soient $p, n \in \mathbb{N}^*$

1. S'il existe une injection $g : [\![1, p]\!] \longrightarrow [\![1, n]\!]$, alors $p \leqslant n$.
2. S'il existe une bijection $h : [\![1, p]\!] \longrightarrow [\![1, n]\!]$, alors $p = n$.

De ce lemme se déduit facilement le résultat suivant :

Proposition 1.3. Si E est un ensemble fini non vide, l'entier $n \in \mathbb{N}^*$ tel que E soit en bijection avec $[\![1, n]\!]$, est unique et est appelé *cardinal* de E, noté $|E|$, $\#E$ ou encore $\mathrm{Card}(E)$. On dira par convention que $|\emptyset| = 0$.

On peut donc prouver quelques résultats sur des ensembles finis quelconques :

Proposition 1.4 (Principe des tiroirs)**.** Si E est un ensemble fini de cardinal n et F est un ensemble fini de cardinal p, et s'il existe une injection $F \hookrightarrow E$, alors $p \leqslant n$.

Remarque 1.1.1 (Où sont les tiroirs ?)**.** *Cette propriété tient son nom de la formulation contraposée : si E et F sont des ensembles finis de cardinaux respectifs n et p avec $p > n$, alors aucune application $F \longrightarrow E$ n'est injective. En particulier, si vous avez p chaussettes que vous voulez ranger dans n tiroirs différents avec $p > n$, alors au moins un tiroir contiendra au moins deux chaussettes ! On prouvera un résultat plus fort dans la section suivante portant sur le calcul de cardinaux de réunions, produits,... d'ensembles finis.*

Application 1.1.1 (Théorème d'approximation de Dirichlet)**.** *Soient $\alpha \in \mathbb{R}$ et $N \in \mathbb{N}^*$. Il existe alors $(p, q) \in \mathbb{Z} \times [\![1, N]\!]$ tel que :*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{qN}.$$

On peut augmenter en généralité les résultats précédents :

Proposition 1.5. Soient E et F des ensembles.

1. Si F est fini et s'il existe une injection $f : E \longrightarrow F$, alors E est fini et $|E| \leqslant |F|$, avec égalité si et seulement si f est une bijection.
2. Si E est fini et s'il existe une surjection $g : E \longrightarrow F$, alors F est fini et $|F| \leqslant |E|$, avec égalité si et seulement si g est une bijection.
3. En particulier, si E et F sont finis et de même cardinal alors toute application $f : E \longrightarrow F$ est injective si et seulement si elle est surjective si et seulement si elle est bijective.
4. En particulier également, si E est fini et qu'il existe une bijection $E \longrightarrow F$, alors F est fini et $|E| = |F|$.

On a alors l'un des principes phares du dénombrement : pour dénombrer un ensemble donné, il est judicieux d'essayer de le mettre en bijection avec un ensemble plus simple à dénombrer ou bien dont on connaît déjà le cardinal.

1.2 Cardinaux et opérations ensemblistes

Une autre méthode pour dénombrer un ensemble est de le partitionner en sous-ensembles qu'on pourrait comprendre plus facilement. Pour comprendre le lien entre le cardinal d'une union d'ensembles finis et le cardinal des ensembles qui composent cette union, un outil pratique à étudier est la notion de fonction indicatrice :

Définition 1.6 (Fonction indicatrice)**.** Soit E un ensemble et $A \subset E$. On appelle alors *fonction indicatrice* de l'ensemble A l'application :

$$\begin{array}{rccl} \mathbb{1}_A & : & E & \longrightarrow & \{0,1\} \\ & & x & \longmapsto & \begin{cases} 0 & \text{si} \quad x \notin A \\ 1 & \text{si} \quad x \in A. \end{cases} \end{array}$$

La fonction indicatrice permet de déterminer le cardinal d'un certain sous-ensemble fini d'un ensemble :

Proposition 1.7. Soit E un ensemble et $A \subset E$ un ensemble fini. Alors :

$$|A| = \sum_{x \in E} \mathbb{1}_A(x).$$

Couplé avec les formules liant les fonctions indicatrices et les opérations ensemblistes suivantes :

Proposition 1.8. Soit E un ensemble et A, B deux sous-ensembles de E. On a alors :

1. $\mathbb{1}_{A^c} = 1 - \mathbb{1}_A$,
2. $\mathbb{1}_{A \cap B} = \mathbb{1}_A \mathbb{1}_B$,
3. $\mathbb{1}_{A \cup B} = \mathbb{1}_A + \mathbb{1}_B - \mathbb{1}_{A \cap B}$,
4. $\mathbb{1}_{A \setminus B} = \mathbb{1}_A - \mathbb{1}_{A \cap B}$

on obtient les relations sur les cardinaux :

Proposition 1.9. Soit E un ensemble et A, B deux sous-ensembles finis de E. On a alors :

1. Si E est fini, alors A^c est fini et on a : $|A^c| = |E| - |A|$,
2. $A \setminus B$ est fini et : $|A \setminus B| = |A| - |A \cap B|$
3. $A \cup B$ est fini et : $|A \cup B| = |A| + |B| - |A \cap B|$.

On utilisera souvent la relation 3. dans le cas particulier où A et B sont disjoints : dans ce cas, on obtient : $|A \sqcup B| = |A| + |B|$ et ce calcul se généralise pour une famille finie d'ensembles disjoints.

Application 1.2.1 (Principe des tiroirs amélioré)**.** *Soient X et Y deux ensembles finis non vides de cardinaux respectifs n et m. Alors pour tout $f : X \longrightarrow Y$, il existe au moins un élément $y \in Y$ tel que :*

$$\left|f^{-1}(\{y\})\right| \geqslant \frac{n}{m}.$$

Une autre application importante est la définition de la probabilité uniforme sur un ensemble fini :

Application 1.2.2 (Probabilité uniforme)**.** *Soit E un ensemble fini. Le couple $(E, \mathscr{P}(E))$ munit E d'une structure d'espace mesurable et la fonction :*

$$\begin{array}{rccc} \mathbb{P} & : & \mathscr{P}(E) & \longrightarrow & [0,1] \\ & & A & \longmapsto & \dfrac{|A|}{|E|} \end{array}$$

est une probabilité sur E, appelée « probabilité uniforme » sur E.

La relation 3. dans toute sa généralité a également son importance pour prouver par exemple que l'intersection $A \cap B$ n'est pas vide, et en voici une application dans le cadre des formes quadratiques sur un corps fini :

Application 1.2.3 (Une forme quadratique non-dégénérée sur $\mathbb{F}_q^2$ représente toujours 1)**.** *Soient $\mathbb{F}_q$ un corps fini de cardinal q et Q une forme quadratique non-dégénérée sur $\mathbb{F}_q^2$. Alors Q représente 1. C'est-à-dire qu'il existe $(x, y) \in \mathbb{F}_q^2$ tel que $Q(x, y) = 1$.*

Cependant, il est également très utile parfois de connaître une formule généralisant la formule 3 de la proposition 1.9 pour une union finie quelconque d'ensembles finis : c'est la formule du *crible de Poincaré* :

Théorème 1.10 (Crible de Poincaré)**.** Soient E un ensemble et $A_1, \ldots, A_n$ des sous-ensembles finis de E. On a alors :

$$\mathbb{1}_{\bigcup_{i=1}^n A_i} = \sum_{k=1}^{n} (-1)^{k-1} \left(\sum_{1 \leqslant i_1 < \ldots < i_k \leqslant n} \mathbb{1}_{A_{i_1}} \ldots \mathbb{1}_{A_{i_k}} \right).$$

En particulier :

$$\left| \bigcup_{i=1}^{n} A_i \right| = \sum_{k=1}^{n} (-1)^{k-1} \left(\sum_{1 \leqslant i_1 < \ldots < i_k \leqslant n} \left| \bigcap_{j=1}^{k} A_{i_j} \right| \right).$$

Cette formule peut se prouver par récurrence, mais les calculs deviennent vite fastidieux. Elle est cependant très agréable à prouver en développant simplement le produit suivant :

$$\mathbb{1}_{\bigcap_{i=1}^n A_i^c} = \prod_{i=1}^{n} (1 - \mathbb{1}_{A_i}).$$

Application 1.2.4 (Nombre de couples d'entiers premiers entre eux [FGN07])**.** *Soit $A_n := \left\{(a, b) \in [\![1, n]\!]^2 \mid a \wedge b = 1\right\}$. En notant $p_1, \ldots, p_k$ les nombres premiers compris entre 1 et n, et en notant :*

$$\forall i \in [\![1, k]\!], \quad U_i := \left\{(a, b) \in [\![1, n]\!]^2 \mid p_i \mid a \text{ et } p_i \mid b\right\}$$

on a :

$$|A_n| = n^2 - \left|\bigcup_{i=1}^{k} U_i\right| = n^2 - \sum_{j=1}^{n}(-1)^{j-1}\left(\sum_{1\leqslant i_1<\ldots<i_j\leqslant n}\left|\bigcap_{m=1}^{j} U_{i_m}\right|\right) = \sum_{d=1}^{n}\mu(d)\left\lfloor\frac{n}{d}\right\rfloor^2$$

où μ est la fonction de Möbius, que nous introduirons en partie 2.

On a calculé le cardinal d'une union d'ensembles. Mais qu'en est-il du produit cartésien ? C'est tout simplement le produit des cardinaux, comme le montrent les résultats ci-dessous :

Lemme 1.11. Soient $p, q \in \mathbb{N}^*$. L'application :

$$\begin{array}{rccc} \varphi & : & [\![1,p]\!]\times[\![1,q]\!] & \longrightarrow & [\![1,pq]\!] \\ & & (a,b) & \longmapsto & a+p(b-1) \end{array}$$

est une bijection. En particulier :

$$|[\![1,p]\!]\times[\![1,q]\!]| = pq.$$

Proposition 1.12. Soient E_1 et E_2 deux ensembles finis. Alors le produit cartésien $E_1 \times E_2$ est un ensemble fini et :

$$|E_1 \times E_2| = |E_1| \times |E_2|.$$

De même, si $E_1, \ldots, E_n$ sont des ensembles finis, alors le produit cartésien $\prod_{i=1}^{n} E_i$ est fini et :

$$\left|\prod_{i=1}^{n} E_i\right| = \prod_{i=1}^{n} |E_i|.$$

On peut alors commencer à dénombrer quelques objets mathématiques bien connus.

1.3 Premiers décomptes

Proposition 1.13 (Nombre de p-listes)**.** Soit $p \in \mathbb{N}^*$. Une *p-liste* d'éléments d'un ensemble E est un élément de E^p. Si E est un ensemble fini, il y a alors $|E|^p$ p-listes de E.

Exemple 1.3.1 (Probabilité de faire un double 6)**.** *On lance deux dés à 6 faces équilibrés. Il y a $6 \times 6 = 36$ issues possibles pour ce lancer de dés, qui correspondent aux 2-listes de $[\![1,6]\!]$. Étant donné que seule une issue correspond à un double 6, la probabilité d'obtenir un double 6 est de $\frac{1}{36}$.*

Remarque 1.3.1 (Ça existe une 0-liste ?)**.** *On peut définir, lorsque E est fini non vide, que E^0 a un unique élément, qui est la liste vide $()$. Ainsi, la formule reste vraie lorsque $p = 0$.*

En général, les p-listes correspondent aux issues d'expériences nécessitant d'effectuer des tirages *avec remise*. Les issues correspondant à des tirages *sans remise* sont plutôt des *p-arrangements* :

Proposition 1.14 (Nombre de p-arrangements)**.** Soient E un ensemble et $p \in \mathbb{N}^*$. On appelle *p-arrangement* de E toute p-liste de E constituée d'éléments distincts. Ce sont donc des éléments de l'ensemble :

$$\mathscr{A}_p(E) := \{(x_1, \ldots, x_p) \in E^p \mid \forall i \neq j, \quad x_i \neq x_j\}.$$

Si E est un ensemble fini de cardinal n, alors le nombre de p-arrangements possibles de E est égal à :

$$A_p^n := \begin{cases} \dfrac{n!}{(n-p)!} & \text{si } p \leqslant n \\ 0 & \text{sinon.} \end{cases}$$

Remarque 1.3.2 (Dénombrer en étudiant les *choix possibles*)**.** *La technique de dénombrement ici à l'œuvre est sans doute l'une des plus emblématiques : combien de choix possibles pour le premier élément x_1 de la liste ? Autant que d'éléments de E : n. Combien de choix possibles pour x_2 ? On peut en choisir $n-1$ au total car x_2 doit être différent de x_1, que l'on a choisi préalablement. Combien de choix pour x_3 ? $n-2$ puisque x_3 doit être différent de x_1 et x_2. On peut répéter ce raisonnement jusqu'à x_p qui peut être choisi parmi $n-p+1$ éléments de E. On a donc au total $n\times(n-1)\times(n-2)\times\ldots\times(n-p+1)$ choix de p-arrangements possibles. En fait, ce raisonnement est implicitement une construction de bijection entre l'ensemble des p-arrangements et le produit $[\![1,n]\!]\times[\![1,n-1]\!]\times\ldots\times[\![1,n-p+1]\!]$. C'est ce principe qui est utilisé le plus fréquemment pour démontrer le résultat suivant :*

Proposition 1.15 (Cardinal des familles libres d'un espace vectoriel sur un corps fini)**.** Soient p un nombre premier, $q=p^n$ une certaine puissance de p, $d\in\mathbb{N}^*$ et $r\in[\![1,d]\!]$. Notons $L_{r,d}$ l'ensemble des familles libres de $\mathbb{F}_q^d$ à r éléments. Alors on a :

$$|L_{r,d}|=\prod_{i=0}^{r-1}\left(q^n-q^i\right).$$

Un corollaire immédiat de ce résultat est le suivant :

Corollaire 1.16 (Cardinal du groupe général linéaire sur un corps fini)**.** Soient p un nombre premier, $q=p^n$ une certaine puissance de p et $d\in\mathbb{N}^*$. Alors :

$$|\mathrm{GL}_d(\mathbb{F}_q)|=q^{\frac{d(d-1)}{2}}\prod_{i=1}^{d}\left(q^i-1\right).$$

Remarque 1.3.3. *On montrera la formule du cardinal de $L_{r,d}$ à partir de la formule du cardinal de $\mathrm{GL}_d(\mathbb{F}_q)$ via la relation orbite-stabilisateur dans notre développement 1.*

Application 1.3.1 (Un p-Sylow de $\mathrm{GL}_d(\mathbb{F}_p)$)**.** *Si p est un nombre premier et $d\in\mathbb{N}^*$, alors l'ensemble U formé des matrices triangulaires supérieures de taille d à coefficients dans $\mathbb{F}_p$ dont les coefficients diagonaux sont égaux à 1 est un p-Sylow de $\mathrm{GL}_d(\mathbb{F}_p)$.*

Donnons peut-être un dernier exemple de l'utilisation de cette méthode de dénombrement dans le cadre du groupe symétrique :

Proposition 1.17 ([Per96])**.** Soient $n\in\mathbb{N}^*$, $(k_1,\ldots,k_n)\in\mathbb{N}^n$ tels que $\sum_{i=1}^{n}ik_i=n$ et $\sigma\in\mathfrak{S}_n$ de *type cyclique* $(k_1,k_2,\ldots,k_n)$, c'est-à-dire que σ possède, dans sa décomposition en produits de cycles à supports disjoints k_i i-cycles pour tout $i\in[\![1,n]\!]$. Alors, en notant $Z(\sigma)$ le *centralisateur* de σ, on a :

$$|Z(\sigma)|=\prod_{i=1}^{n}i^{k_i}k_i!$$

Application 1.3.2 (Les automorphismes de $\mathfrak{S}_n$)**.** *Pour $n\neq 6$, les automorphismes de groupes de $\mathfrak{S}_n$ sont tous intérieurs.*

On peut également s'intéresser à des expériences de tirages sans remise, mais dans lesquelles l'ordre de tirage n'est pas pris en compte. Par exemple, si on tire trois nombres dans $[\![1,90]\!]$ sans remise, les issues $(1,8,72)$ et $(72,1,8)$ sont considérées comme étant les mêmes : on parle alors de p-combinaisons.

Proposition 1.18 (Nombre de p-combinaisons)**.** Soient E un ensemble fini de cardinal n et $p \in \mathbb{N}^*$. On appelle p-combinaison de E tout sous-ensemble de E de cardinal p. Le nombre p-combinaisons est souvent noté $\binom{n}{p}$, lu « p parmi n ». On a alors :

$$\binom{n}{p} = \frac{A_p^n}{p!} = \begin{cases} \dfrac{n!}{p!(n-p)!} & \text{si } p \leqslant n \\ 0 & \text{sinon.} \end{cases}$$

Remarque 1.3.4.

1. *Les tirages sans remise dans lequel l'ordre de tirage ne compte pas correspondent bien à des sous-ensembles de E plutôt qu'à des listes : $\{1, 8, 72\}$ et $\{72, 1, 8\}$ correspondent au même sous-ensemble de $[\![1, 90]\!]$.*
2. *Le lien entre A_p^n et $\binom{n}{p}$ peut s'observer en remarquant que la relation d'équivalence suivante sur $\mathscr{A}_p(E)$:*

$$(x_1, \dots, x_p)\mathscr{R}(y_1, \dots, y_p) \iff \exists \sigma \in \mathfrak{S}_p,\ \forall i \in [\![1, p]\!], \quad x_{\sigma(i)} = y_i \qquad (*)$$

permet d'identifier le quotient $\dfrac{\mathscr{A}_p(E)}{\mathscr{R}}$ et l'ensemble des p-combinaisons.

3. *On a montré un résultat fort : quel que soient $n \in \mathbb{N}$ et $p \leqslant n$, le nombre $\frac{n!}{p!(n-p)!}$ est un entier !*

On peut également s'intéresser aux expériences de tirage *avec remise* mais dans lequel l'ordre ne compte pas : on parle alors de p-combinaisons *avec répétitions.*

Proposition 1.19 (Nombre de p-combinaisons avec répétition)**.** On appelle p-combinaison avec répétition toute p-liste de E dans lequel l'ordre ne compte pas, c'est-à-dire un élément du quotient $\dfrac{E^p}{\mathscr{R}}$ où $\mathscr{R}$ est la relation d'équivalence $(*)$. Le nombre de p-combinaisons avec répétition est alors de $\binom{n+p-1}{p}$.

Avoir dénombré les p-listes, les p-arrangements et les p-combinaisons nous permet alors de dénombrer certains ensembles d'applications entre deux ensembles :

Proposition 1.20 (Nombre d'applications, d'applications injectives, d'applications (strictement) croissantes)**.** Soient E et F deux ensembles finis de cardinal respectifs p et n.

1. L'ensemble des applications de E vers F, noté F^E est fini, et : $\left|F^E\right| = n^p$.
2. L'ensemble des applications injectives de E vers F est fini et de cardinal A_p^n.
3. En particulier, le groupe symétrique $\mathfrak{S}(E)$ est fini et : $|\mathfrak{S}(E)| = p!$.
4. L'ensemble des applications strictement croissantes de $[\![1, p]\!]$ dans $[\![1, n]\!]$ est fini et de cardinal $\binom{n}{p}$.
5. L'ensemble des applications croissantes de $[\![1, p]\!]$ dans $[\![1, n]\!]$ est fini et de cardinal $\binom{n+p-1}{p}$.

Le point 1 de cette dernière propriété permet de dénombrer les parties d'un ensemble E :

Corollaire 1.21 (Nombres de parties)**.** Soit E un ensemble fini de cardinal n.

1. $\mathscr{P}(E)$ est fini et : $|\mathscr{P}(E)| = 2^n$.
2. En particulier, on a la formule :

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n.$$

La preuve du point 1. de ce corollaire est encore une jolie application des fonctions indicatrices : l'application

$$\begin{array}{ccc} \mathscr{P}(E) & \longrightarrow & \{0,1\}^E \\ A & \longmapsto & \mathbb{1}_A \end{array}$$

est en fait une bijection. On a également d'autres formules invoquant des coefficients binomiaux :

Proposition 1.22. Soient $n, p \in \mathbb{N}$. On a :

1. Si $p \in [\![0, n]\!]$, alors $\binom{n}{p} = \binom{n}{n-p}$.
2. Si $p, n \geqslant 1$, on a la formule de Pascal : $\binom{n}{p} = \binom{n-1}{p-1} + \binom{n-1}{p}$.
3. Si $p, n \geqslant 1$, on a la formule dite du *capitaine* : $\binom{n}{p} = \frac{n}{p}\binom{n-1}{p-1}$.

Avant d'énoncer d'autres formules utiles invoquant les coefficients binomiaux, énonçons une application de la formule du capitaine :

Application 1.3.3 (Relation de divisibilité entre un nombre premier et les coefficients binomiaux)**.** *Soit p un nombre premier. On a alors :*

$$\forall k \in [\![1, p-1]\!], \quad p \mid \binom{p}{k}.$$

Les formules suivantes s'avèrent également très utiles :

Proposition 1.23. Soient $m, n, p \in \mathbb{N}$.

1. On a la formule de Vandermonde :
$$\sum_{k=0}^{p} \binom{n}{k}\binom{m}{p-k} = \binom{m+n}{p}.$$
2. Soient A une algèbre et $a, b \in A$ deux éléments qui commutent. On a la formule du *binôme de Newton* :
$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

De la formule de Vandermonde découlent des cas particuliers intéressants :

Exemple 1.3.2. — *Si $m, n \in \mathbb{N}$, on a :*

$$\sum_{k=0}^{n} \binom{n}{k}\binom{m}{k} = \binom{m+n}{m}.$$

— *En particulier :*

$$\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}.$$

La formule du binôme de Newton, couplée à l'application 1.3.3 permet de montrer les faits suivants :

Application 1.3.4 (Le Frobenius est un morphisme)**.** *Si A est un anneau de caractéristique p première, alors l'application :*

$$\begin{array}{ccc} A & \longrightarrow & A \\ x & \longmapsto & x^p \end{array}$$

est un morphisme d'anneaux. Dans le cas où A est un corps, il est souvent appelé morphisme de Frobenius.

Application 1.3.5 (Une preuve élémentaire du petit théorème de Fermat)**.** *Une jolie application de ce fait est une preuve élémentaire du petit théorème de Fermat par récurrence : si $a \in \mathbb{N}$, alors $a^p \equiv a\ [p]$. L'initialisation en $a = 0$ est claire et pour l'hérédité, il suffit de constater :*

$$(a+1)^p \equiv a^p + 1 \equiv a + 1\ [p].$$

On a également une formule généralisant le binôme de Newton, basée sur le coefficient *multinomial* :

Proposition 1.24 (Nombre de partitions par des ensembles de cardinal prescrit)**.** Soient E un ensemble fini non vide de cardinal n, $p \in \mathbb{N}^*$ et $(i_1, \dots, i_p) \in \mathbb{N}^p$ tels que :

$$\sum_{k=1}^{p} i_k = n.$$

Alors le nombre de partitions ordonnées $(A_1, \dots, A_p)$ de E telles que pour tout $k \in [\![1, p]\!]$, $|A_k| = i_k$ est égal à :

$$\binom{n}{i_1, \dots, i_p} := \frac{n!}{\prod_{k=1}^{p} i_k!}$$

On a alors :

Proposition 1.25 (Formule du multinôme)**.** Soient A une algèbre et $a_1, \dots, a_p \in A$ p éléments commutant deux à deux. Alors, pour tout $n \in \mathbb{N}^*$, on a :

$$\left(\sum_{i=1}^{p} a_i\right)^n = \sum_{\substack{(i_1,\dots,i_p)\in\mathbb{N}^p \\ i_1+\dots+i_p=n}} \left(\binom{n}{i_1, \dots, i_p} \prod_{k=1}^{p} a_k^{i_k}\right).$$

2 Techniques algébriques de dénombrement : séries génératrices et formules d'inversion [Gou21] [Ten22] [Goz97]

Motivations

La section précédente nous a permis de revoir les techniques élémentaires de dénombrement, en les appliquant sur des objets mathématiques connus. Cependant, certaines formules prouvées dans la section précédente peuvent être prouvées d'une autre façon. Prenons un exemple parlant : la formule de Vandermonde, citée en proposition 1.23 peut se prouver en trois coups de cuillère à pot en remarquant le fait suivant :

$$\forall n \in \mathbb{N}, \quad (1+X)^n = \sum_{k=0}^{n} \binom{n}{k} X^k,$$

et donc, en identifiant les coefficients devant X^p dans l'égalité :

$$(1+X)^n (1+X)^m = (1+X)^{m+n},$$

on obtient la formule de Vandermonde. Cette propriété remarquable des polynômes disant qu'une égalité de polynômes entraîne une identification des coefficients est ce qui motive la définition des séries génératrices.

2.1 Séries génératrices

Définition 2.1 (L'algèbre des séries formelles)**.** Soit $(A, +, \times)$ un anneau commutatif unitaire et soit $(a_n)_{n\in\mathbb{N}} \in A^{\mathbb{N}}$. On appelle *série formelle* ou *série génératrice* assoicée à la suite (a_n) l'expression :

$$\sum_{n\geqslant 0} a_n X^n$$

où X est une inconnue. L'ensemble des séries formelles, noté $A[\![X]\!]$ est muni de la structure de A-algèbre suivante :

$$\forall (a_n)_{n\in\mathbb{N}}, (b_n)_{n\in\mathbb{N}} \in A^{\mathbb{N}}, \quad \left(\sum_{n\geqslant 0} a_n X^n\right) +_{A[\![X]\!]} \left(\sum_{n\geqslant 0} b_n X^n\right) := \sum_{n\geqslant 0} (a_n + b_n) X^n,$$

$$\forall (a_n)_{n\in\mathbb{N}}, (b_n)_{n\in\mathbb{N}} \in A^{\mathbb{N}}, \quad \left(\sum_{n\geqslant 0} a_n X^n\right) \times_{A[\![X]\!]} \left(\sum_{n\geqslant 0} b_n X^n\right) := \sum_{n\geqslant 0} \left(\sum_{k=0}^{n} a_k b_{n-k}\right) X^n,$$

$$\forall (a_n)_{n\in\mathbb{N}} \in A^{\mathbb{N}},\ \forall a \in A, \quad a \cdot_{A[\![X]\!]} \left(\sum_{n\geqslant 0} a_n X^n\right) := \sum_{n\geqslant 0} (a \times a_n) X^n.$$

On a alors que deux séries formelles sont égales si et seulement si la suite de leurs coefficients est la même.

Remarque 2.1.1. *Le X dans les séries formelles est simplement une variable muette, qui permet de mimer une série entière ou un polynôme, bien qu'il n'y ait aucune notion de convergence ici. On pourrait définir les séries formelles comme la A-algèbre $A^{\mathbb{N}}$ munie des lois $+,\times$ et $\cdot$ comme définies plus haut.*

On peut définir quelques opérations sur les séries génératrices comme en analyse :

Définition 2.2 (Dérivation, évaluation, composition)**.** Soient A un anneau commutatif unitaire et $S, T \in A[\![X]\!]$, dont les suites associées seront notées respectivement $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$. On définit alors :

1. la dérivée formelle S' par la formule :
$$S' = \sum_{n\geqslant 1} n a_n X^{n-1} = \sum_{n\geqslant 0} (n+1) a_{n+1} X^n.$$
2. les dérivées formelles d'ordre $k \in \mathbb{N}$ de S, notées $S^{(k)}$ par la formule de récurrence :
$$\begin{cases} S^{(0)} &= S \\ S^{(k+1)} &= \left(S^{(k)}\right)', \quad \forall k \in \mathbb{N}. \end{cases}$$
3. l'évaluation en 0 : $S(0) := a_0$,
4. si $T(0) = 0$, la composition $S \circ T$: pour tout $n \in \mathbb{N}$, T^n est une série formelle associée à une certaine suite notée $\left(b_k^{(n)}\right)_{k\in\mathbb{N}}$. Cette suite vérifie :
$$\forall k \leqslant n, \quad b_k^{(n)} = 0 \quad \text{et} \quad \forall k \in \mathbb{N}, \quad b_k^{(0)} = \delta_{0,k}.$$
On définit alors :
$$S \circ T = \sum_{k\geqslant 0} \left(\sum_{n=0}^{k} a_n b_k^{(n)}\right) X^k.$$

Exemple 2.1.1. *Si A est un corps de caractéristique 0, la série génératrice associée à la suite $\left(\frac{1}{n!}\right)_{n\in\mathbb{N}}$ est notée* exp *et s'écrit donc :*

$$\exp(X) = \sum_{n\geqslant 0} \frac{1}{n!} X^n.$$

Étudions l'intérêt des séries génératrices avec quelques exemples parlants :

Application 2.1.1 (Les nombres de Bell)**.** *Soit $n \in \mathbb{N}^*$. On note B_n le nombre de partitions de $[\![1, n]\!]$. On pose $B_0 = 1$ par convention. Alors $(B_n)_{n\in\mathbb{N}}$ vérifie la relation de récurrence :*

$$\forall n \in \mathbb{N}, \quad B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_k.$$

La série génératrice F associée à la suite $\left(\dfrac{B_n}{n!}\right)_{n\in\mathbb{N}}$ vérifie l'équation suivante :

$$F' = \exp(X)F$$

et donc :

$$F = \exp \circ(\exp(X) - 1).$$

Ainsi, on a :

$$\forall n \in \mathbb{N}, \quad B_n = \frac{1}{e} \sum_{k=0}^{+\infty} \frac{m^n}{m!}.$$

Dans la preuve de ce résultat, on fait le lien entre les séries entières et les séries formelles ainsi : l'équation différentielle :

$$\left\{ \begin{array}{rcl} f' & = & \exp(x)f, \quad \forall x \in \mathbb{R} \\ f(0) & = & 1 \end{array} \right.$$

admet comme unique solution la fonction f telle que :

$$\forall x \in \mathbb{R}, \quad f(x) = \exp(\exp(x) - 1).$$

Ainsi, les coefficients de F sont les mêmes que les coefficients du développement en série entière de f, que l'on sait calculer ! On obtient donc ce résultat, appelé *formule de Dobinski*.

Les séries génératrices peuvent également servir dans l'étude des nombres de Catalan :

Application 2.1.2 (Les nombres de Catalan)**.** *Soit $n \in \mathbb{N}$. On appelle mot de Dyck de longueur $2n$ toute $2n$-liste $w = (w_1, \ldots, w_{2n})$ de $\{0, 1\}$ telle que :*

- *w contient autant de 1 que de 0,*
- *Tout préfixe de w contient plus de 1 que de 0, c'est-à-dire :*

$$\forall p \leqslant 2n, \quad |\{i \in [\![1, p]\!] \mid w_i = 1\}| \geqslant |\{i \in [\![1, p]\!] \mid w_i = 0\}|.$$

Par convention, le mot vide $()$ est un mot de Dyck de longueur 0. Le nombre de mots de Dyck de longueur $2n$ est appelé n-ième nombre de Catalan, noté C_n. On a alors :

1. *Pour tout $n \in \mathbb{N}$: $C_{n+1} = \sum_{k=0}^{n} C_k C_{n-k}$.*
2. *La série formelle S associée à la suite $(C_n)_{n\in\mathbb{N}}$ vérifie : $XS(X)^2 = S(X) - 1$.*
3. *Pour tout $n \in \mathbb{N}$, on a : $C_n = \dfrac{1}{n+1}\binom{2n}{n}$.*

On peut représenter graphiquement un mot de Dyck w de taille $2n$ par la fonction :

$$\begin{array}{rcccl} f_w & : & [\![0, 2n]\!] & \longmapsto & \mathbb{N} \\ & & k & \longmapsto & \left\{ \begin{array}{rcl} 0 & \text{si} & k = 0 \\ f_w(k-1) + 1 & \text{si} & w_{k-1} = 1 \text{ et } k \geqslant 1 \\ f_w(k-1) - 1 & \text{si} & w_{k-1} = 0 \text{ et } k \geqslant 1 \end{array} \right. \end{array}$$

de sorte que l'ensemble des mots de Dyck de taille $2n$ puisse être mis en bijection avec l'ensemble des fonctions $f : [\![0, 2n]\!] \longrightarrow \mathbb{N}$ telles que :

1. $\forall k \in [\![1, 2n]\!], \quad |f(k) - f(k-1)| = 1,$
2. $f(0) = f(2n) = 0$ (il y a autant de 1 que de 0).

Le fait que f soit à valeurs dans $\mathbb{N}$ traduit le fait que tout préfixe d'un mot de Dyck a plus de 1 que de 0. En figure 1 on trouvera un exemple de telle représentation graphique.
Détaillons un autre exemple parlant d'utilisation des séries génératrices, que l'on peut retrouver sur la chaîne YouTube de l'excellent 3Blue1Brown [3Bl] :

Application 2.1.3 (Nombre de sous-ensembles dont la somme des éléments est divisible par un entier fixé)**.** *Soient $n, k \in \mathbb{N}^*$ et P le polynôme :*

$$P = \prod_{i=1}^{n} (1 + X^i).$$

Alors, si on note $\left(a_0, a_1, \ldots, a_{\frac{n(n+1)}{2}}\right)$ les coefficients de P, on a que le nombre $D_{n,k}$ de sous-ensembles de $[\![1, n]\!]$ dont la somme des éléments est divisible par k vérifie :

$$D_{n,k} = \sum_{i=0}^{\left\lfloor \frac{n(n+1)}{2k} \right\rfloor} a_{ki} = \frac{1}{k} \left(\sum_{i=0}^{k-1} P\left(\zeta_k^i\right) \right)$$

où $\zeta_k := e^{\frac{2i\pi}{k}}$.

Dans la preuve de ce résultat, on utilise en fait un résultat central et assez profond qui justifie l'introduction de ce polynôme P pour résoudre ce problème :

Proposition 2.3. Soit $n \in \mathbb{N}^*$. Si P désigne le même polynôme que dans l'application précédente, c'est-à-dire :

$$P = \prod_{i=1}^{n} (1 + X^i),$$

alors en notant $\left(a_0, a_1, \ldots, a_{\frac{n(n+1)}{2}}\right)$ ses coefficients, on a :

$$\forall i \in \left[\!\left[0, \frac{n(n+1)}{2}\right]\!\right], \quad a_i = \left| \left\{ J \subset [\![1, n]\!] \;\middle|\; \sum_{j \in J} j = i \right\} \right|.$$

Exemple 2.1.2. *Pour $n = 2000$ et $k = 5$, on a :*

$$D_{2000,5} = \frac{1}{5} \left(2^{2000} + 4 \left(\prod_{i=1}^{5} (1 + \zeta_5^i) \right)^{400} \right) = \frac{1}{5} \left(2^{2000} + 4 \times (-2)^{400} \right) = 2^{402} \times \underbrace{\frac{1 + 2^{1598}}{5}}_{\in \mathbb{Z}}.$$

Citons enfin dans cette section des exemples de fonctions génératrices qui vont nous servir dans la preuve du développement 2 :

Définition 2.4 (Factorielles croissante et décroissante)**.** On définit la *n-ième factorielle décroissante* et la *n-ième factorielle croissante*, notées respectivement $X^{\underline{n}}$ et $X^{\overline{n}}$ par les formules de récurrence suivantes :

$$\begin{cases} X^{\underline{0}} = X^{\overline{0}} &= 1, \\ X^{\underline{n+1}} &= (X - n) X^{\underline{n}}, \quad \forall n \in \mathbb{N}, \\ X^{\overline{n+1}} &= (X + n) X^{\overline{n}}, \quad \forall n \in \mathbb{N}. \end{cases}$$

On peut alors définir les *nombres de Stirling de première et de deuxième espèces :*

Définition 2.5 (Nombres de Stirling de première espèce)**.** Soient $n \in \mathbb{N}$, $k \in [\![0, n]\!]$. $X^{\underline{n}}$ est un polynôme et on note $s(n,k)$ les nombres entiers tels que :

$$X^{\underline{n}} = \sum_{k=0}^{n} s(n,k) X^k.$$

Définition 2.6 (Nombres de Stirling de deuxième espèce)**.** Pour $n \in \mathbb{N}$ et $k \in [\![0, n]\!]$, on définit les *nombres de Stirling de deuxième espèce*, notés $S(n,k)$ comme les entiers vérifiant :

$$X^n = \sum_{k=0}^{n} S(n,k) X^{\underline{k}}.$$

Un avantage des séries génératrices, qu'on a pu voir à l'œuvre avec les nombres de Bell (application 2.1.1) et de Catalan (application 2.1.2) et qui sera de nouveau mis en évidence dans les propositions ci-dessous, est qu'elles permettent de compactifier les relations de récurrences que suit la suite des coefficients de ces séries. On peut alors en déduire des liens avec le dénombrement de familles d'objets dont le cardinal peut suivre la même relation de récurrence.

Proposition 2.7 (Nombres de Stirling de première espèce et nombre de cycles d'une permutation)**.** Soient $n, k \in \mathbb{N}^*$ et notons $\mathfrak{S}_{n,k}$ l'ensemble des permutations de $\mathfrak{S}_n$ s'écrivant comme produits de k cycles à supports disjoints et $C(n,k)$ son cardinal. Alors $C(n,k) = |s(n,k)|$.

Cette proposition sera prouvée dans le développement 2.

Proposition 2.8 (Nombres de Stirling de deuxième espèce et partitions)**.** Le nombre de Stirling $S(n,k)$ est égal au nombre de façons de partitionner $[\![1, n]\!]$ en exactement k sous-ensembles. En particulier, si B_n désigne le n-ième nombre de Bell (cf. application 2.1.1) on a :

$$\forall n \in \mathbb{N}, \quad \sum_{k=0}^{n} S(n,k) = B_n.$$

Les séries génératrices en probabilités

La notion de série génératrice existe également en probabilités :

Définition 2.9 (Série génératrice associée à une variable aléatoire discrète)**.** Soient $(\Omega, \mathscr{A}, \mathbb{P})$ un espace probabilisé et $Y : \Omega \longrightarrow \mathbb{N}$ une variable aléatoire discrète. On appelle *série génératrice* associée à la variable Y la série entière G_Y définie ainsi :

$$\begin{array}{rccl} G_Y & : & \overline{\mathbb{D}}(0,1) & \longrightarrow & \mathbb{R} \\ & & z & \longmapsto & \displaystyle\sum_{n=0}^{+\infty} \mathbb{P}(Y=n) z^n = \mathbb{E}\left(z^Y\right). \end{array}$$

Remarque 2.1.2. *Étant donné que la série* $\displaystyle\sum_{n \geqslant 0} \mathbb{P}(Y = k)$ *converge et est de somme* 1*, on a déjà que* G_Y *est holomorphe sur* $\mathbb{D}(0,1)$*, continue sur* $\overline{\mathbb{D}}(0,1)$ *et que* $G_Y(1) = 1$*.*

On peut alors faire le lien entre l'*intégrabilité* de la variable Y et la *régularité* de la fonction génératrice en 1.

Proposition 2.10. Soient $(\Omega, \mathscr{A}, \mathbb{P})$ un espace probabilisé et $Y : \Omega \longrightarrow \mathbb{N}$ une variable aléatoire discrète. Alors Y admet un moment d'ordre k si et seulement si la fonction $G_Y^{(k)}$, définie sur $\mathbb{D}(0,1)$ est définie et continue sur $\overline{\mathbb{D}}(0,1)$. Dans ce cas, on a :

$$\mathbb{E}\left(Y^k\right) = \sum_{i=0}^{k} S(k,i) G_Y^{(i)}(1),$$

où les nombres $S(k,i)$ sont les nombres de Stirling de deuxième espèce, introduits en définition 2.6.

Cette propriété sera utile pour un calcul d'espérance dans le développement 2.

2.2 Inverser pour dénombrer

Parfois, dans des problèmes de dénombrement, on est amené à avoir des formules du type :

$$\underbrace{d_1}_{\text{connu}} = F\ \underbrace{(d_2)}_{\text{inconnu}}\ .$$

C'est-à-dire que l'on peut exprimer le cardinal d_1 d'un ensemble connu en fonction du cardinal d_2 que l'on voudrait déterminer. Il existe dans certains cas des moyens d'inverser la fonction F pour connaître le cardinal d_2. Nous en détaillerons 2 : l'inversion de Pascal et l'inversion de Möbius :

2.2.1 Inversion de Pascal

Proposition 2.11 (Inversion de Pascal)**.** Soient $n \in \mathbb{N}$, A un anneau commutatif unitaire et $(a_0, \ldots, a_n), (b_0, \ldots, b_n) \in A^n$. Alors on a :

$$\left(\forall k \in [\![0,n]\!], \quad a_k = \sum_{i=0}^{k} \binom{k}{i} b_i\right) \iff \left(\forall k \in [\![0,n]\!], \quad b_k = \sum_{i=0}^{k} (-1)^{k-i} \binom{k}{i} a_i\right).$$

De cette formule d'inversion peuvent se déduire plusieurs résultats de dénombrement :

Application 2.2.1 (Nombre de dérangements, nombre d'applications surjectives)**.** *Soient E et F deux ensembles finis de cardinal respectif n et p. Alors :*

1. *Le nombre d'applications surjectives de E dans F noté $s_{p,n}$ vérifie :*

$$p^n = \sum_{k=0}^{p} \binom{p}{k} s_{k,n}.$$

Ainsi :

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

2. *On appelle dérangement de E toute permutation de E sans points fixes. Le nombre de dérangements de E, noté d_n vérifie :*

$$n! = \sum_{k=0}^{n} \binom{n}{k} d_k.$$

Ainsi :

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

2.2.2 Inversion de Möbius [Goz97] [Ten22]

Proposition 2.12 (L'algèbre des fonctions arithmétiques)**.** Soit $\mathscr{A} := \mathscr{F}(\mathbb{N}^*, \mathbb{C})$ muni des lois $+$ et $\cdot$ usuelles et de la loi de convolution $*$ définie ainsi :

$$\forall n \in \mathbb{N}^*, \quad (f * g)(n) = \sum_{d \mid n} f(d) g\left(\frac{n}{d}\right).$$

Alors $\mathscr{A}$ est une $\mathbb{C}$-algèbre commutative unitaire intègre, d'unité $\mathbb{1}_{\{1\}}$ et dont les éléments inversibles sont les fonctions f telles que $f(1) \neq 0$.

Définition 2.13 (Fonction de Möbius)**.** Soit $\mu \in \mathscr{A}$ la fonction définie comme :

$$\forall n \in \mathbb{N}^*, \quad \mu(n) = \begin{cases} 1 & \text{si} \quad n = 1 \\ (-1)^k & \text{si} \quad n \text{ s'écrit, dans sa décomposition en facteurs premiers, } p_1 \dots p_k \\ 0 & \text{si} \quad p^2 \mid n \text{ pour un certain nombre premier } p. \end{cases}$$

Théorème 2.14. La fonction μ est inversible dans $\mathscr{A}$ et son inverse est la fonction constante égale à 1. C'est-à-dire que μ est caractérisé par les propriétés suivantes :

$$\begin{cases} \mu(1) & = & 1 \\ \displaystyle\sum_{d \mid n} \mu(d) & = & 0, \quad \forall n \geqslant 2. \end{cases}$$

Corollaire 2.15 (Formule d'inversion de Möbius)**.** Soient $f, g \in \mathscr{A}$ telles que $f(1) \neq 0$ et $g(1) \neq 0$. Alors :

$$\left(\forall n \in \mathbb{N}^*, \quad f(n) = \sum_{d \mid n} g(d)\right) \iff \left(\forall n \in \mathbb{N}^*, \quad g(n) = \sum_{d \mid n} \mu(d) f\left(\frac{n}{d}\right)\right).$$

Exemple 2.2.1 (L'indicatrice d'Euler)**.** *On sait que l'indicatrice d'Euler φ vérifie la relation :*

$$\forall n \in \mathbb{N}^*, \quad n = \sum_{d \mid n} \varphi(d).$$

On a donc une expression de φ :

$$\forall n \in \mathbb{N}^*, \quad \varphi(n) = \sum_{d \mid n} \mu(d) \frac{n}{d}.$$

Application 2.2.2 (Dénombrement des polynômes irréductibles sur $\mathbb{F}_p$)**.** *Soit p un nombre premier et $n \in \mathbb{N}^*$. On note $\mathscr{I}(p, n)$ l'ensemble des polynômes unitaires de degré n irréductibles dans $\mathbb{F}_p[X]$ et $I(p, n)$ son cardinal. On a alors :*

$$X^{p^n} - X = \prod_{d \mid n} \prod_{Q \in \mathscr{I}(p,d)} Q(X).$$

En particulier, on obtient :

$$p^n = \sum_{d \mid n} d I(p, d).$$

Ainsi, la formule d'inversion de Möbius permet de dire que :

$$I(p, n) = \frac{1}{n} \sum_{d \mid n} \mu(d) p^{\frac{n}{d}}.$$

3 Utilisation des actions de groupes [CG13] [CG15] [Exc] [Ber20]

La théorie des actions de groupes s'applique très bien au dénombrement : si on désire dénombrer les configurations possibles pour une certaine figure, alors il s'agit souvent de dénombrer le nombre d'orbites sous l'action d'un certain groupe et dans ce cas, la formule de Burnside permet de donner ce nombre d'orbites en fonction du nombre de points fixes des éléments du groupe. Dans d'autres cas, on s'intéressera au nombre d'éléments dans l'orbite d'un certain élément sous l'action d'un groupe et ainsi, la relation orbite-stabilisateur permet souvent de s'en sortir.

3.1 La relation orbite-stabilisateur et ses utilisations

Proposition 3.1 (Relation orbite-stabilisateur)**.** Soient G un groupe et X un ensemble sur lequel G agit. Alors, pour tout $x \in X$, en notant $G \cdot x$ l'orbite de x et G_x le stabilisateur de x sous l'action de G, l'application :

$$\begin{array}{ccc} G & \longrightarrow & G \cdot x \\ g & \longmapsto & g \cdot x \end{array}$$

passe au quotient en une bijection entre $\dfrac{G}{G_x}$ et $G \cdot x$. En particulier, si G et X sont finis, on a :

$$\forall x \in X, \quad \frac{|G|}{|G_x|} = |G \cdot x|.$$

Exemple 3.1.1 (Rotations du n-gone régulier)**.** *Soit $G = \mu_n(\mathbb{C})$ le groupe des racines complexes n-ièmes de l'unité. Alors G agit sur lui-même par translation à gauche :*

$$\forall (r, s) \in G^2, \quad r \cdot s = rs.$$

On interprète cette action comme étant le groupe des rotations du plan complexe de centre O l'origine et d'angle $\frac{2k\pi}{n}$ pour $k \in [\![0, n-1]\!]$, qui s'identifie donc à $\mu_n(\mathbb{C})$, agissant sur les sommets du n-gone régulier, dont les affixes sont les éléments de $\mu_n(\mathbb{C})$. Si $g \in G$ et $s \in G$, on appelle g-orbite de s l'orbite de s pour l'action précédente, restreinte à $\langle g \rangle$. On a alors :

$$|\langle g \rangle \cdot s| = \frac{|\langle g \rangle|}{|\langle g \rangle_s|} = |\langle g \rangle| = \mathrm{o}(g).$$

Exemple 3.1.2 (Nombre d'éléments qui sont conjugués à une permutation donnée)**.** *Soient $n \in \mathbb{N}^*$, $(k_1, \ldots, k_n) \in \mathbb{N}^n$ tels que $\sum_{i=1}^{n} i k_i = n$ et $\sigma \in \mathfrak{S}_n$ de type cyclique $(k_1, \ldots, k_n)$ (cf. proposition 1.17). Alors il y a exactement*

$$\frac{n!}{\prod_{i=1}^{n} i^{k_i} k_i!}$$

permutations conjuguées à σ.

Donnons deux applications de cette proposition 3.1 en combinatoire sur les corps finis :

Application 3.1.1 (Familles en somme directe et nombre de matrices diagonalisables sur les corps finis)**.**

1. *Soient $n, k \in \mathbb{N}^*$ et $(n_1, \ldots, n_k) \in \mathbb{N}^k$ tel que $\sum_{i=21}^{k} n_i = n$. Le nombre de familles $(E_1, \ldots, E_k)$ de sous-espaces vectoriels de $\mathbb{F}_q^n$ tels que :*

$$\bigoplus_{i=1}^{k} E_i = \mathbb{F}_q^n, \quad \text{et} \quad \forall i \in [\![1, k]\!], \quad \dim(E_i) = n_i$$

est égal à :

$$\frac{|\mathrm{GL}_n(\mathbb{F}_q)|}{\prod_{i=1}^{k}|\mathrm{GL}_{n_i}(\mathbb{F}_q)|}.$$

2. *Le cardinal de l'ensemble des matrices diagonalisables de $\mathscr{M}_n(\mathbb{F}_q)$ est alors :*

$$\sum_{\substack{(n_1,\dots,n_q)\in\mathbb{N}^q\\ n_1+\dots+n_q=n}}\left(\frac{|\mathrm{GL}_n(\mathbb{F}_q)|}{\prod_{i=1}^{q}|\mathrm{GL}_{n_i}(\mathbb{F}_q)|}\right).$$

La deuxième application faisant l'objet de notre premier développement :

Développement 1 (Cardinal du cône nilpotent [CG15])**.** Soient $\mathbb{F}_q$ un corps de cardinal q et $d\in\mathbb{N}^*$. On note $\mathscr{N}_d(\mathbb{F}_q)$ l'ensemble des matrices nilpotentes à coefficients dans $\mathbb{F}_q$ et $n_d(q)$ son cardinal. On a :

$$n_d(q)=q^{d(d-1)}.$$

On peut coupler cette relation orbite-stabilisateur avec le fait qu'un ensemble muni d'une relation d'équivalence est partitionné par ses classes d'équivalence pour avoir *l'équation aux classes* :

Proposition 3.2 (Équation aux classes)**.** Soient G un groupe fini et X un ensemble fini sur lequel G agit. Posons $\mathscr{R}$ un système de représentants de l'ensemble des orbites X/G. On a alors :

$$|X|=\sum_{x\in\mathscr{R}}\frac{|G|}{|G_x|}=\left|X^G\right|+\sum_{\substack{x\in\mathscr{R}\\ G_x\neq G}}\frac{|G|}{|G_x|}$$

où on a noté X^G l'ensemble des éléments $x\in X$ fixes par tous les éléments de G :

$$X^G:=\{x\in X\ \mid \forall g\in G,\quad g\cdot x=x\}.$$

Déduisons-en un résultat sur les rotations du n-gone (exemple 3.1.1) :

Exemple 3.1.3 (Nombre de g-orbites du n-gone régulier par rotation)**.** *On a vu dans l'exemple 3.1.1 que toutes les g-orbites avaient même cardinal : $\mathrm{o}(g)$. Par l'équation aux classes, on a donc :*

$$n=|\mu_n(\mathbb{C})|=\sum_{s\in\mathscr{R}}\mathrm{o}(g)=|\mathscr{R}|\times\mathrm{o}(g).$$

Ainsi, pour tout $g\in G=\mu_n(\mathbb{C})$, le nombre de g-orbites pour l'action de G sur le n-gone régulier est :

$$\frac{n}{\mathrm{o}(g)}.$$

On en trouvera une illustration dans le cas $n=6$ en figure 2.

L'équation aux classes a énormément d'applications en théorie des groupes. Citons-en quelques unes :

Application 3.1.2 (En théorie des groupes)**.**

1. *Si p est un nombre premier et si G est un p-groupe, alors son centre $Z(G)$ est non trivial.*
2. *Si G est un groupe fini, p un facteur premier de $|G|$, S un p-Sylow de G et H un sous-groupe de G, alors il existe $g\in G$ tel que $gSg^{-1}\cap H$ soit un p-Sylow de H. En particulier (en couplant ce résultat à l'application 1.3.1), tout groupe fini admet un p-Sylow.*
3. *Lemme de Cauchy : Soient G un groupe fini et p un facteur premier de $|G|$. Alors G admet un élément d'ordre exactement p.*

3.2 La formule de Burnside et ses utilisations

Là où la relation orbite-stabilisateur permettait de calculer les cardinaux des orbites sous une action de groupe, la formule de Burnside, elle, met l'accent sur le *nombre* de ces orbites. Notamment, cela permet de dégager le nombre de structures différentes, si on se permet d'identifier deux structures qui seraient dans la même orbite. Par exemple, si on a une roulette avec plusieurs couleurs, on est tous d'accord pour dire que si on la tourne, ça reste la même roulette et donc si on veut compter le nombre de roulettes différentes, on ne doit pas recompter ces roulettes qu'on a fait tourner.

Proposition 3.3 (Formule de Burnside)**.** Soient G un groupe fini et X un ensemble fini sur lequel G agit. On note X/G l'ensemble des orbites sous l'action de G et, pour $g \in G$, $\mathrm{Fix}(g)$ l'ensemble des points fixes sous l'action de g, c'est-à-dire :

$$\mathrm{Fix}(g) := \{x \in X \mid g \cdot x = x\}.$$

Alors, on a la relation :

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)|.$$

Cette formule peut être reformulée ainsi : le nombre d'orbites de X sous l'action de G est égal au nombre moyen de points fixes de l'action ! Nous la verrons particulièrement à l'œuvre dans la deuxième partie de notre deuxième développement :

Développement 2 (Quelques résultats sur les permuations suivant la loi unforme sur $\mathfrak{S}_n$ [Gou21], [Exc])**.** Soit $n \in \mathbb{N}^*$. On rappelle que, pour $k \in \mathbb{N}^*$, on note $s(n,k)$ le *nombre de Stirling de première espèce* et $S(n,k)$ le *nombre de Stirling de deuxième espèce*, définis en définitions 2.1 et 2.6.

1. Soit Σ une variable aléatoire suivant la loi $\mathscr{U}(\mathfrak{S}_n)$, et notons C la variable aléatoire comptant le nombre de cycles à supports disjoints apparaissant dans la décomposition de Σ. Alors, on a :

$$\forall t \in \mathbb{R}, \quad G_C(t) = \frac{t^{\overline{n}}}{n!},$$

plus précisément :

$$\forall k \in [\![1, n]\!], \quad \mathbb{P}(C = k) = \frac{|s(n,k)|}{n!}$$

et :

$$\mathbb{E}(C) = \sum_{k=1}^{n} \frac{1}{k}.$$

2. Si Σ est une variable aléatoire suivant la loi $\mathscr{U}(\mathfrak{S}_n)$, alors, en notant F la variable aléatoire comptant le nombre de points fixes de Σ, on a :

$$\forall k \in \mathbb{N}, \quad \mathbb{E}\left(F^k\right) = \sum_{i=0}^{n} S(k,i).$$

(avec, pour tout $k > n$, $S(n,k) = 0$). En particulier :

$$\forall k \leqslant n, \quad \mathbb{E}\left(F^k\right) = B_k$$

et donc, F a les mêmes n premiers moments que la loi de Poisson $\mathscr{P}(1)$.

Formule de Burnside et coloriages [Ber20]

Le but de cette section est d'étudier les *coloriages* possibles d'un ensemble X et de pouvoir les dénombrer efficacement. Lorsqu'on a face à nous une figure que l'on voudrait colorier avec un certain nombre de couleurs, alors, si on manipule cette figure dans l'espace, on obtiendra le même coloriage et donc on ne doit pas compter cette configuration *a priori* différente comme étant un nouveau coloriage. C'est là tout l'enjeu des problèmes de coloriages et les actions de groupes et notamment la formule de Burnside sont les outils idéaux pour traiter ce genre de problème.

Définition 3.4 (Coloriage)**.** Soient X un ensemble fini de cardinal n et soit $q \in \mathbb{N}^*$. On appelle *coloriage* de X en au plus q couleurs, ou q-coloriage de X, toute application :

$$X \longrightarrow [\![1, q]\!].$$

L'ensemble des coloriages de X en au plus q couleurs sera noté $\mathscr{C}(X, q)$.

À partir de maintenant, on regarde un groupe G agissant sur X un peu comme pour mimer l'action d'un humain sur une figure, comme par exemple faire tourner une roulette, ou retourner un collier. On veut donc trouver les coloriages qui sont équivalents selon cette action :

Lemme 3.5. Soit G un groupe agissant sur notre ensemble X de cardinal n et soit $q \in \mathbb{N}^*$. Alors l'application suivante définit une action de G sur $\mathscr{C}(X, q)$:

$$\begin{array}{rcl} G \times \mathscr{C}(X,q) & \longrightarrow & \mathscr{C}(X,q) \\ (g, f) & \longmapsto & g \cdot f : x \mapsto f\left(g^{-1} \cdot x\right) \end{array}$$

On a donc que l'action de G sur X induit naturellement une action de G sur les coloriages de X. Il est donc naturel d'identifier deux coloriages qui sont dans la même orbite :

Définition 3.6. Soit G un groupe agissant sur notre ensemble X de cardinal n, $q \in \mathbb{N}^*$. Rappelons que $\mathscr{C}(X, q)$ désigne l'ensemble des q-coloriages de X. On note alors $\mathscr{C}_G(X, q)$ l'ensemble des orbites de l'action de G sur $\mathscr{C}(X, q)$.

Pour calculer le cardinal de l'ensemble des coloriages modulo l'action de G, il s'avère judicieux de s'intéresser aux coloriages fixés par les éléments g du groupe et d'utiliser la formule de Burnside :

Lemme 3.7. Soient G un groupe fini agissant sur un ensemble X fini de cardinal n. On fixe également $q \in \mathbb{N}^*$. Soit $g \in G$. Alors un q-coloriage f de X est fixé par g, i.e. $g \cdot f = f$ si et seulement si f est constante en restriction à chaque orbite de l'action de $\langle g \rangle$ sur X, c'est-à-dire :

$$\forall m \in \mathbb{Z},\ \forall x \in X, \quad f\left(g^m \cdot x\right) = f(x).$$

En combinant ce lemme avec la formule de Burnside, on obtient donc :

Théorème 3.8. Soient G un groupe fini agissant sur un ensemble X fini de cardinal n, $q \in \mathbb{N}^*$ et, pour $g \in G$, soit $r(g)$ le nombre de g-orbites de X, c'est-à-dire :

$$r(g) := \left|X/\langle g \rangle\right|.$$

Le nombre d'orbites de l'action de G sur l'ensemble des q-coloriages $\mathscr{C}(X, q)$ est alors :

$$\left|\mathscr{C}_G(X, q)\right| = \frac{1}{|G|} \sum_{g \in G} q^{r(g)}.$$

Application 3.2.1 (Nombre de coloriages d'une roulette à n secteurs)**.** *On considère l'action de $G := \mu_n(\mathbb{C})$ sur lui-même par translation à gauche, comme en exemples 3.1.1 et 3.1.3. On a vu que pour $g \in G$, le nombre de g-orbites d'un sommet du n-gone régulier, assimilé ici à un des n secteurs d'une roulette, était de $\frac{n}{\mathrm{o}(g)}$. On a alors que le nombre de q-coloriages réellement différents d'une roulette à n secteurs est :*

$$\left|\mathscr{C}_G(\mu_n(\mathbb{C}), q)\right| = \frac{1}{n} \sum_{d \mid n} \varphi(d) q^{\frac{n}{d}}.$$

Application 3.2.2 (Nombre de colliers de n perles réalisables avec q couleurs de perles différentes)**.** *On considère l'action naturelle du groupe diédral D_n sur les sommets du n-gone régulier, identifié à $\mu_n(\mathbb{C})$. Rappelons que le groupe diédral est composé de n rotations d'angle $\frac{2k\pi}{n}$ pour $k \in [\![0, n-1]\!]$ et de n symétries orthogonales. On a alors des résultats différents selon la parité de n :*

— *Si $n = 2m+1$ avec $m \in \mathbb{N}$, alors le nombre de colliers de n perles réalisables avec q couleurs de perles différentes est :*

$$|\mathscr{C}_{D_n}(\mu_n(\mathbb{C}), q)| = \frac{1}{2n}\left(\sum_{d \mid n} \varphi(d) q^{\frac{n}{d}} + nq^{m+1}\right),$$

— *Si $n = 2m$ avec $m \in \mathbb{N}^*$, alors le nombre de colliers de n perles réalisables avec q couleurs de perles différentes est :*

$$|\mathscr{C}_{D_n}(\mu_n(\mathbb{C}), q)| = \frac{1}{2n}\left(\sum_{d \mid n} \varphi(d) q^{\frac{n}{d}} + mq^{m+1} + mq^{m}\right).$$

On trouvera en figure 3 les différentes configurations pour les orbites d'une réflexion selon la parité de n.

Annexes

A Figures

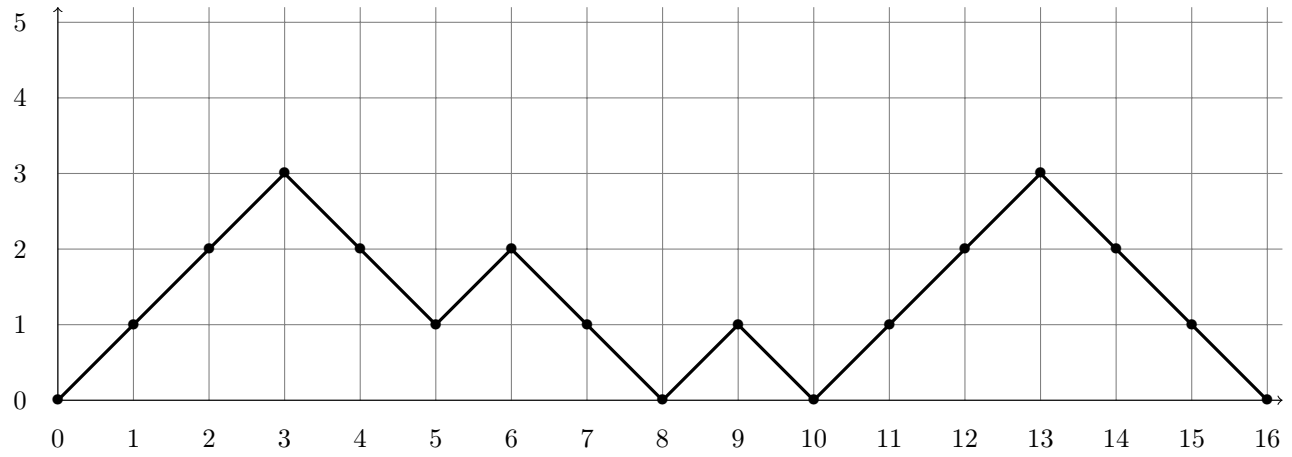
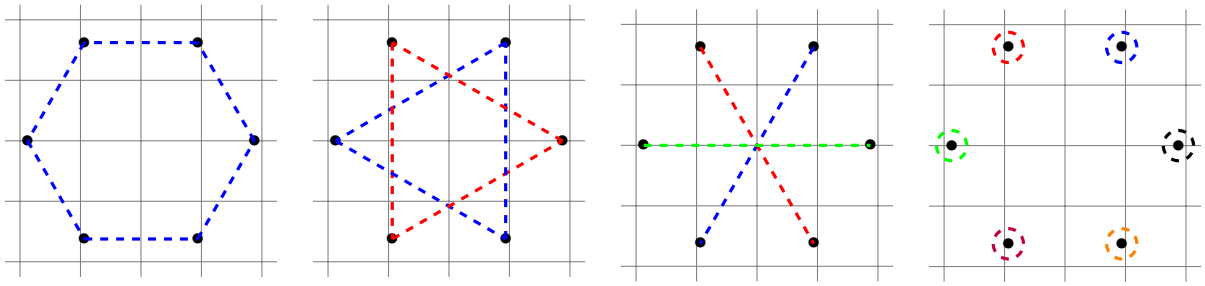


FIGURE 1 – Représentation graphique du mot de Dyck $(1,1,1,0,0,1,0,0,1,0,1,1,1,0,0,0)$



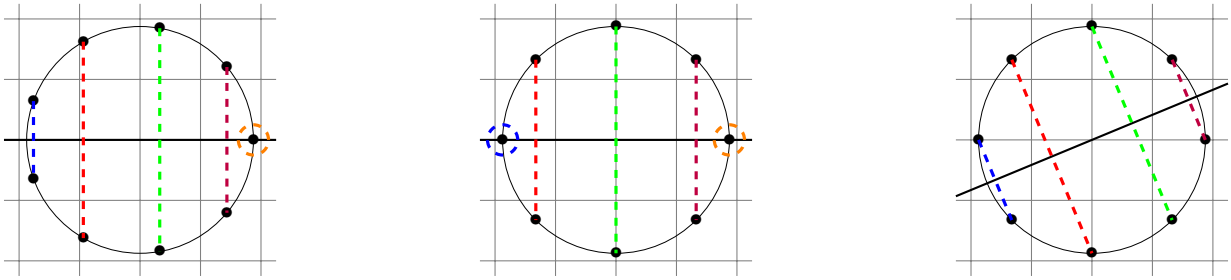
(a) $g = e^{\frac{i\pi}{3}}$, $o(g) = 6$
nombre d'orbites : 1

(b) $g = e^{\frac{2i\pi}{3}}$, $o(g) = 3$
nombre d'orbites : 2

(c) $g = e^{i\pi}$, $o(g) = 2$
nombre d'orbites : 3

(d) $g = 1$, $o(g) = 1$
nombre d'orbites : 6

FIGURE 2 – Les différentes g-orbites des sommets de l'hexagone régulier (roulette à 6 secteurs) sous l'action du groupe engendré par la rotation d'angle $\frac{\pi}{3}$, représentée par le nombre complexe $e^{\frac{i\pi}{3}}$.



(a) Réflexion d'un ennéagone régulier (collier à $9 = 2 \times 4 + 1$ perles) par rapport à un axe de symétrie.
Nombre d'orbites : $5 = 4 + 1$

(b) Réflexion d'un octogone régulier (collier à $8 = 2 \times 4$ perles) par rapport à un axe de symétrie contenant 2 points. Nombre d'orbites : $5 = 4 + 1$

(c) Réflexion d'un octogone régulier (collier à $8 = 2 \times 4$ perles) par rapport à un axe de symétrie ne contenant aucun points. Nombre d'orbites : 4

FIGURE 3 – Les différentes g-orbites des sommets d'un ennéagone régulier et d'un octogone régulier sous l'action des réflexions du groupe diédral.

B Démonstrations complètes des développements

B.1 Démonstration du développement 1

Remarque B.1.1 (En quoi le résultat du développement 1 est-il surprenant ?)**.** *Plusieurs estimations heuristiques de ce résultat peuvent être données. Par exemple, d'après le théorème de réduction de Jordan pour les endomorphismes nilpotents, tout élément de $\mathscr{N}_d(\mathbb{F}_q)$ est conjugué à une matrice de la forme :*

$$\begin{pmatrix} J_{d_1} & & \boldsymbol{O} \\ & \ddots & \\ \boldsymbol{O} & & J_{d_r} \end{pmatrix}$$

avec $\sum_{i=1}^{r} d_i = d$ et J_k le bloc de Jordan nilpotent de taille k. Or, si on était dans $\mathbb{R}$ par exemple, on pourrait dire que l'orbite de la matrice J_d par conjugaison serait dense dans $\mathscr{N}_d(\mathbb{R})$. Les matrices nilpotentes de taille d seraient donc « presque toutes » dans l'orbite de J_d. Si on extrapole ce résultat dans $\mathbb{F}_q$, on aurait donc :

$$n_d(q) \approx |\mathscr{O}_{J_d}| = \frac{|\mathrm{GL}_d(\mathbb{F}_q)|}{|Z(J_d)|}$$

où $Z(J_d)$ désigne le centralisateur de J_d. Dans notre discussion où on imagine que presque toutes les matrices sont inversibles, on peut imaginer $Z(J_d)$ comme étant le commutant de J_d. Or, étant donné que J_d est une matrice cyclique, son commutant est un espace vectoriel de dimension exactement égale à d. Ainsi, en approchant le cardinal de $\mathrm{GL}_d(\mathbb{F}_q)$ par q^{d^2}, on obtient :

$$n_d(q) \approx q^{d^2-d},$$

ce qui est exactement le résultat souhaité !

Une autre interprétation possible peut se faire en terme de variété. $\mathscr{N}_d(\mathbb{F}_q)$ peut se représenter comme étant le lieu des zéros de d applications polynômiales indépendantes sur $\mathscr{M}_d(\mathbb{F}_q)$: les coefficients du polynôme caractéristique ! En effet, une matrice de taille d est nilpotente si et seulement si son polynôme caractéristique est égal à X^d. Ainsi, si on était dans $\mathbb{R}$ par exemple, on pourrait dire que $\mathscr{N}_d(\mathbb{F}_q)$ serait une sous-variété de $\mathscr{M}_d(\mathbb{F}_q)$ de dimension $d^2 - d$ via la caractérisation par « équation ». Ainsi, en approximant le cardinal de $\mathscr{N}_d(\mathbb{F}_q)$ par celui d'un $\mathbb{F}_q$-espace vectoriel de dimension $d^2 - d$, on obtient :

$$n_d(q) \approx q^{d^2-d} \text{ !}$$

Démonstration du développement 1. Soient $e \in \mathbb{F}_q^d$ un vecteur non-nul et $N \in \mathscr{N}_d(\mathbb{F}_q)$. Ce vecteur engendre un sous-espace cyclique pour N, dont une base est :

$$\mathscr{F}_e = (e, Ne, \ldots, N^{r-1}e)$$

et telle que $N^r e = 0$. En effet, si $\pi_{N,e}$ désigne le polynôme minimal de N relativement au vecteur e, on a :

$$\pi_{N,e} \mid \pi_N \mid \chi_N = X^d.$$

Ainsi, il existe k entier naturel non-nul tel que :

$$\pi_{N,e} = X^k.$$

Or, $k \geqslant r$ car la famille $\mathscr{F}_e$ est libre : aucun élément de cette famille n'est nul. Or, par définition du sous-espace cyclique engendré par e, la famille $(e, Ne, \ldots, N^{r-1}e, N^r e)$ est liée, donc il existe P de degré r tel que $P(N)e = 0$. Ainsi, $\pi_{N,e}$ divise P, donc $k \leqslant r$. Donc $N^r e = \pi_{N,e}(N)e = 0$ par définition. Cela permet de justifier la définition suivante :

Définition B.1. Soient $N \in \mathscr{N}_d(\mathbb{F}_q)$ et $r \in [\![1, d]\!]$. On note $L_{r,d}$ l'ensemble des familles libres de $\mathbb{F}_q^d$ à r éléments. On dit que N *respecte* une famille $\mathscr{F} = (e_1, \dots, e_r) \in L_{r,d}$ si :

$$\forall i \in [\![1, r-1]\!], \quad Ne_i = e_{i+1}$$

avec $Ne_r = 0$.

Notons alors :

$$\tilde{\mathscr{N}_d} := \left\{ (N, \mathscr{F}) \in \mathscr{N}_d(\mathbb{F}_q) \times \bigsqcup_{r=1}^{d} L_{r,d} \mid N \text{ respecte } \mathscr{F} \right\}.$$

Un double décompte de $\tilde{\mathscr{N}_d}$ va nous permettre de trouver une relation de récurrence pour $n_d(q)$!

Décompte 1 : On dénombre d'abord selon la première composante, en notant π_1 la projection sur la première composante :

$$\tilde{\mathscr{N}_d} = \bigsqcup_{N \in \mathscr{N}_d(\mathbb{F}_q)} \pi_1^{-1}(\{N\}).$$

On a alors :

$$|\tilde{\mathscr{N}_d}| = \sum_{N \in \mathscr{N}_d(\mathbb{F}_q)} |\pi_1^{-1}(\{N\})|.$$

Un élément de $\pi_1^{-1}(\{N\})$ sera donc totalement déterminé par la donnée d'un vecteur e non-nul étant donné qu'il sera de la forme $(N, \mathscr{F}_e)$. Plus précisément, l'application :

$$\begin{array}{rcl} \pi_1^{-1}(\{N\}) & \longrightarrow & \mathbb{F}_q^d \setminus \{0\} \\ (N, (e_1, \dots, e_r)) & \longmapsto & e_1 \end{array}$$

est une bijection. Ainsi, on a :

$$\forall N \in \mathscr{N}_d(\mathbb{F}_q), \quad |\pi_1^{-1}(\{N\})| = q^d - 1.$$

D'où :

$$|\tilde{\mathscr{N}_d}| = n_d(q)\left(q^d - 1\right).$$

Décompte 2 : On dénombre ensuite selon la deuxième composante. On note alors π_2 la projection sur cette composante, de sorte qu'on ait :

$$|\tilde{\mathscr{N}_d}| = \sum_{r=1}^{d} \sum_{\mathscr{F} \in L_{r,d}} |\pi_2^{-1}(\{\mathscr{F}\})|.$$

Soit alors $\mathscr{F} \in L_{r,d}$ avec r fixé. Par le théorème de la base incomplète, on peut compléter cette famille en une base $\mathscr{B}$ de $\mathbb{F}_q^d$. Ainsi, $N \in \mathscr{N}_d(\mathbb{F}_q)$ respecte $\mathscr{F}$ si et seulement si, la matrice de son endomorphisme associé (que l'on notera encore N) dans la base $\mathscr{B}$ est :

$$\begin{pmatrix} J_r^T & M \\ \mathbf{O} & N_{d-r} \end{pmatrix}$$

où $M \in \mathscr{M}_{r,d-r}(\mathbb{F}_q)$ est une certaine matrice et $N_{d-r} \in \mathscr{N}_{d-r}(\mathbb{F}_q)$. En effet, par définition, N respecte $\mathscr{F}$ si et seulement si $\mathrm{Vect}(\mathscr{F})$ est stable par N et $N_{|\mathrm{Vect}(\mathscr{F})}$ a pour matrice dans la base $\mathscr{F}$ égal à J_r^T. Enfin, N doit être nilpotent, d'où le fait que la matrice N_{d-r} doive être nilpotente. On obtient donc :

$$|\tilde{\mathscr{N}_d}| = \sum_{r=1}^{d} \sum_{\mathscr{F} \in L_{r,d}} q^{r(d-r)} n_{d-r} = \sum_{r=1}^{d} |L_{r,d}| n_{d-r}(q) q^{r(d-r)}.$$

Il nous faut donc calculer le cardinal de $L_{r,d}$! Comment faire ? Considérons l'action suivante :

$$\begin{array}{rcl} \mathrm{GL}_d(\mathbb{F}_q) \times L_{r,d} & \longrightarrow & L_{r,d} \\ (M, (e_1, \dots, e_r)) & \longmapsto & (Me_1, \dots, Me_r). \end{array}$$

Cette action est transitive : en effet si $\mathscr{F}_1, \mathscr{F}_2 \in L_{r,d}$, alors le théorème de la base incomplète nous dit que l'on peut

compléter ces deux familles en bases $\mathscr{B}_1, \mathscr{B}_2$ de $\mathbb{F}_q^d$. En prenant M la matrice de passage de la base $\mathscr{B}_1$ à la base $\mathscr{B}_2$, on a bien que $M \cdot \mathscr{F}_1 = \mathscr{F}_2$. Ainsi :

$$|L_{r,d}| = |\mathscr{O}_{\mathscr{F}}|$$

pour un certain $\mathscr{F} \in L_{r,d}$. Le calcul du cardinal de cette orbite peut s'effectuer grâce à celui du stabilisateur associé via la relation orbite-stabilisateur. Si on complète $\mathscr{F}$ en une base $\mathscr{B}$ de $\mathbb{F}_q^d$, on a qu'une matrice M est dans le stabilisateur de $\mathscr{F}$ si et seulement si la matrice de l'endomorphisme canoniquement associé à M s'écrit, dans la base $\mathscr{B}$:

$$\begin{pmatrix} I_r & A \\ \mathbf{O} & B \end{pmatrix}$$

où $A \in \mathscr{M}_{r,d-r}(\mathbb{F}_q)$ et $B \in \mathrm{GL}_{d-r}(\mathbb{F}_q)$. En notant alors $g_k(q)$ le cardinal de $\mathrm{GL}_k(\mathbb{F}_q)$, on a donc, grâce à la relation orbite-stabilisateur :

$$|L_{r,d}| = \frac{g_d(q)}{q^{r(d-r)} g_{d-r}(q)}.$$

Ainsi :

$$|\tilde{\mathscr{N}_d}| = \sum_{r=1}^{d} n_{d-r}(q) \frac{g_d(q)}{g_{d-r}(q)}.$$

Combinons les décomptes : En regroupant les résultats des deux décomptes, on obtient :

$$n_d(q)\left(q^d - 1\right) = \sum_{r=1}^{d} n_{d-r}(q) \frac{g_d(q)}{g_{d-r}(q)}$$

i.e.

$$\frac{n_d(q)}{g_d(q)}\left(q^d - 1\right) = \sum_{r=0}^{d-1} \frac{n_r(q)}{g_r(q)}.$$

On en conclut :

$$\frac{n_d(q)}{g_d(q)}\left(q^d - 1\right) = \frac{n_{d-1}(q)}{g_{d-1}(q)} + \frac{n_{d-1}(q)}{g_{d-1}(q)}\left(q^{d-1} - 1\right),$$

c'est-à-dire :

$$\frac{n_d(q)}{g_d(q)} = \frac{q^{d-1}}{q^d - 1} \frac{n_{d-1}(q)}{g_{d-1}(q)}.$$

On a donc, par produit téléscopique :

$$\frac{n_d(q)}{g_d(q)} = \prod_{k=2}^{d} \left(\frac{q^{k-1}}{q^k - 1}\right) \underbrace{\frac{n_1(q)}{g_1(q)}}_{=\frac{1}{q-1}} = \frac{q^{\frac{d(d-1)}{2}}}{\prod_{k=1}^{d}\left(q^k - 1\right)} = \frac{q^{d(d-1)}}{g_d(q)}.$$

On en conclut :

$$n_d(q) = q^{d(d-1)}$$

ce qui termine la preuve ! □

B.2 Démonstration du développement 2

Démonstration. 1. **Étape 1 : $\sum_{k=0}^{n} |s(n,k)| x^k = x^{\overline{n}}$:**

En développant l'écriture de $x^{\underline{n}}$ et $x^{\overline{n}}$, on obtient :

$$x^{\underline{n}} = x(x-1)\dots(x-n+1), \quad x^{\overline{n}} = x(x+1)\dots(x+n-1).$$

Ainsi :

$$\forall x \in \mathbb{R}, \quad (-x)^{\underline{n}} = (-1)^n x^{\overline{n}}.$$

Ainsi, on obtient :

$$\forall x \in \mathbb{R}, \quad x^{\overline{n}} = \sum_{k=0}^{n} (-1)^{n-k} s(n,k) x^k.$$

Or, en notant $\tilde{s}(n,k)$ les entiers tels que :

$$x^{\overline{n}} = \sum_{k=0}^{n} \tilde{s}(n,k) x^k$$

on a :

$$\forall k \in [\![0,n]\!], \quad \tilde{s}(n,k) \geqslant 0$$

par somme et produits d'entiers positifs. On a donc :

$$\forall k \in [\![0,n]\!], \quad (-1)^{n-k} s(n,k) \geqslant 0$$

et donc :

$$x^{\overline{n}} = \sum_{k=0}^{n} |s(n,k)| x^k.$$

Étape 2 : Une relation de récurrence sur les $|s(n,k)|$:
On va utiliser la relation de récurrence sur la factorielle croissante afin de déduire une relation de récurrence sur les $|s(n,k)|$:

$$\sum_{k=0}^{n+1} |s(n+1,k)| x^k = x^{\overline{n+1}} = (x+n) \sum_{k=0}^{n} |s(n,k)| x^k = \sum_{k=1}^{n} \left(|s(n,k-1)| + n|s(n,k)| \right) x^k + |s(n,n)| x^{n+1}.$$

On en déduit donc :

$$\forall n \in \mathbb{N}^*, \quad \begin{cases} |s(n,0)| &= 0 \\ |s(n,n)| &= 1 \\ |s(n+1,k)| &= |s(n,k-1)| + n|s(n,k)|, \quad \forall k \in [\![1,n]\!]. \end{cases}$$

Étape 3 : Le nombre de permutations de $\mathfrak{S}_n$ s'écrivant comme produit de k cycles à supports disjoints vérifie la même relation de récurrence :
Disclaimer : Attention ! Ici, l'identité sera considérée comme étant un produit de n cycles à supports disjoints ! (on considère les 1-cycles comme étant des cycles à part entière).

Notons $\mathfrak{S}_{n,k}$ l'ensemble des permutations de $\mathfrak{S}_n$ s'écrivant comme produits de k cycles à supports disjoints et $C(n,k)$ son cardinal. On a :

$$C(n,0) = 0, \text{ et } C(n,n) = 1$$

car si $n \geqslant 1$, une permutation possède au moins 1 cycle dans sa décomposition et $id_{[\![1,n]\!]}$ est la seule permutation de $\mathfrak{S}_n$ s'écrivant comme produit de n cycles à supports disjoints. Pour passer du cran n au cran $n+1$, il faut distinguer les cas selon la présence de $n+1$ dans un cycle de longueur plus grande que 1 ou non. On écrit alors $\mathfrak{S}_{n+1,k}$ grâce à la partition suivante :

$$\mathfrak{S}_{n+1,k} = \bigsqcup_{m=1}^{n+1} \mathfrak{S}_{n+1,k}(m)$$

où on a noté :

$$\mathfrak{S}_{n+1,k}(m) = \{ \sigma \in \mathfrak{S}_{n,k} \mid \sigma(n+1) = m \}$$

Cas $m = n+1$: Si $\sigma(n+1) = n+1$, alors l'application de restriction à $[\![1,n]\!]$ devient une bijection entre $\mathfrak{S}_{n+1,k}(n+1)$ et $\mathfrak{S}_{n,k-1}$. En effet, si $\sigma \in \mathfrak{S}_{n+1,k}(n+1)$, alors sa restriction à $[\![1,n]\!]$ est une permutation et s'écrit nécessairement comme un produit de $k-1$ cycles à supports disjoints (puisque σ possède déjà le cycle $(n+1)$). Réciproquement, une permutation de $[\![1,n]\!]$ s'écrivant comme un produit de $k-1$ cycles à supports disjoints se voit naturellement comme un élément de $\mathfrak{S}_{n+1}$ s'écrivant comme produit de k cycles à supports

disjoints. D'où :

$$|\mathfrak{S}_{n+1,k}(n+1)| = C(n,k-1).$$

Cas $m \leqslant n$: Si $\sigma \in \mathfrak{S}_{n+1,k}(m)$, alors, il s'écrit :

$$\sigma = c \circ c_2 \circ \ldots \circ c_k$$

où $c = \begin{pmatrix} n+1 & m & i_3 & \ldots & i_r \end{pmatrix}$ désigne le cycle de σ dans sa décomposition contenant $n+1$. On a alors, en notant :

$$\sigma' = \begin{pmatrix} n+1 & m \end{pmatrix} \circ \sigma,$$

que $\sigma' \in \mathfrak{S}_{n+1,k}(n+1)$. Ainsi, $\sigma'_{|[\![1,n]\!]} \in \mathfrak{S}_n$. Notons cette restriction $f(\sigma)$. On a alors défini une application :

$$f \quad : \quad \mathfrak{S}_{n+1,k}(m) \quad \longrightarrow \quad \mathfrak{S}_n$$

Montrons qu'en réalité, $f(\sigma) \in \mathfrak{S}_{n,k}$ et que f est injective. Premièrement, on observe que le cycle c de σ est transformé en le cycle $c' = \begin{pmatrix} m & i_3 & \ldots & i_r \end{pmatrix}$ dans la décomposition de σ'. Plus concrètement, on a :

$$\sigma' = c' \circ c_2 \circ \ldots c_k$$

et, étant donné que tous les entiers apparaissant dans le support de σ' sont entre 1 et n, $f(\sigma)$ s'écrit exactement :

$$f(\sigma) = c' \circ c_2 \circ \ldots c_k.$$

Ainsi, $f(\sigma)$ possède exactement k cycles dans sa décomposition. Donc :

$$f(\sigma) \in \mathfrak{S}_{n,k}.$$

Enfin, f est injective. En effet, si $\sigma, \tau \in \mathfrak{S}_{n+1,k}(m)$ sont tels que $f(\sigma) = f(\tau)$, alors en écrivant :

$$\sigma = \begin{pmatrix} n+1 & m & i_3 & \ldots & i_r \end{pmatrix} \circ c_2 \circ \ldots \circ c_k$$

et :

$$\tau = \begin{pmatrix} n+1 & m & j_3 & \ldots & j_s \end{pmatrix} \circ \tilde{c}_2 \circ \ldots \circ \tilde{c}_k$$

on a, d'après le calcul précédent :

$$f(\sigma) = \begin{pmatrix} m & i_3 & \ldots & i_r \end{pmatrix} \circ c_2 \circ \ldots \circ c_k$$

et :

$$f(\tau) = \begin{pmatrix} m & j_3 & \ldots & j_s \end{pmatrix} \circ \tilde{c}_2 \circ \ldots \circ \tilde{c}_k.$$

Ainsi, $c_i = \tilde{c}_i$ pour tout $i \in [\![2,k]\!]$, $s = r$ et $j_l = i_l$ pour tout $l \in [\![3,r]\!]$, donc $\sigma = \tau$. On a donc montré que f effectuait une bijection entre $\mathfrak{S}_{n+1,k}(m)$ et $\mathfrak{S}_{n,k}$ pour tout $m \in [\![1,n]\!]$. On a donc :

$$C(n+1,k) = |\mathfrak{S}_{n+1,k}| = \sum_{m=1}^{n+1} |\mathfrak{S}_{n+1,k}(m)| = C(n,k-1) + \sum_{m=1}^{n} C(n,k) = C(n,k-1) + nC(n,k).$$

On montre alors par récurrence sur $n \in \mathbb{N}^*$ que pour tout $k \in [\![0,n]\!]$, $C(n,k) = |s(n,k)|$.

Étape 4 : Conclusion

Si Σ est une variable aléatoire suivant la loi $\mathscr{U}(\mathfrak{S}_n)$, et si C désigne son nombre de cycles à supports disjoints apparaissant dans sa décomposition, on a :

$$\mathbb{P}(C = k) = \frac{C(n,k)}{n!} = \frac{|s(n,k)|}{n!}.$$

On peut alors en déduire sa série génératrice :

$$\forall t \in \mathbb{R}, \quad G_C(t) = \sum_{k=0}^{+\infty} \mathbb{P}(C=k)t^k = \sum_{k=0}^{n} \frac{|s(n,k)|}{n!} t^k = \frac{t^{\overline{n}}}{n!}.$$

On en déduit donc :

$$\mathbb{E}(C) = G_C'(1) = \underbrace{G_C(1)}_{=1} \times \frac{\mathrm{d}}{\mathrm{d}t} \left(\ln \left(t^{\overline{n}} \right) \right)_{|t=1}$$

Or, pour tout $t > 0$, on a :

$$\ln \left(t^{\overline{n}} \right) = \sum_{i=0}^{n-1} \ln(t+i).$$

D'où :

$$\frac{\mathrm{d}}{\mathrm{d}t} \left(\ln \left(t^{\overline{n}} \right) \right) = \sum_{i=0}^{n-1} \frac{1}{t+i}.$$

On conclut donc que :

$$\mathbb{E}(C) = \sum_{i=0}^{n-1} \frac{1}{i+1}$$

ce qui termine la preuve du premier point !

2. Pour tout $k \in \mathbb{N}$, on a, par définition de F :

$$\mathbb{E}\left(F^k\right) = \frac{1}{n!} \sum_{\sigma \in \mathfrak{S}_n} |\mathrm{Fix}(\sigma)|^k$$

où $\mathrm{Fix}(\sigma)$ désigne l'ensemble des points fixes d'une permutation σ. Si $k = 0$, on a $\mathbb{E}\left(F^k\right) = 1$ et $B_0 = 1$ par convention. Si $k = 1$, on reconnaît un des deux membres de l'égalité dans la formule de Burnside lorsqu'un groupe G agit sur un ensemble X :

$$\left| \frac{X}{G} \right| = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)|.$$

Ici, $G = \mathfrak{S}_n$ et $X = [\![1, n]\!]$. L'action de $\mathfrak{S}_n$ sur $[\![1, n]\!]$ étant transitive, le nombre d'orbites est 1. Ainsi :

$$\mathbb{E}\left(F\right) = \frac{1}{n!} \sum_{\sigma \in \mathfrak{S}_n} |\mathrm{Fix}(\sigma)| = 1.$$

On a également $B_1 = 1$. La clef de ce résultat est donc la formule de Burnside. On va donc considérer l'action de $\mathfrak{S}_n$ sur $[\![1, n]\!]^k$:

$$\forall \sigma \in \mathfrak{S}_n, \ \forall (i_1, \ldots, i_k) \in [\![1, n]\!]^k, \quad \sigma \cdot (i_1, \ldots, i_k) = (\sigma(i_1), \ldots, \sigma(i_k)).$$

On l'appelle *action diagonale*. Si $\mathrm{Fix}^k(\sigma)$ désigne l'ensemble des points fixes de la permutation σ pour cette action, alors, on a :

$$\mathrm{Fix}^k(\sigma) = \mathrm{Fix}(\sigma)^k.$$

Ainsi :

$$\mathbb{E}\left(F^k\right) = \frac{1}{n!} \sum_{\sigma \in \mathbb{S}_n} \left| \mathrm{Fix}^k(\sigma) \right| = \left| \frac{[\![1, n]\!]^k}{\mathfrak{S}_n} \right|.$$

En notant $\mathscr{P}_{k,j}$ l'ensemble des partitions de $[\![1, k]\!]$ en exactement j sous-ensembles non vides, considérons l'application :

$$\begin{array}{rccc} f & : & \dfrac{[\![1, n]\!]^k}{\mathfrak{S}_n} & \longrightarrow & \displaystyle\bigsqcup_{j=1}^{n} \mathscr{P}_{k,j} \\ & & \mathfrak{S}_n \cdot (i_1, \ldots, i_k) & \longmapsto & P_{(i_1, \ldots, i_k)} \end{array}$$

où $P_{(i_1,\dots,i_k)}$ désigne la partition de $[\![1,k]\!]$ donnée par la relation d'équivalence $\mathscr{R}_{(i_1,\dots,i_k)}$:

$$\forall m,l \in [\![1,k]\!], \quad m\mathscr{R}_{(i_1,\dots,i_k)}l \Longleftrightarrow i_m = i_l.$$

c'est-à-dire que $P_{(i_1,\dots,i_k)}$ est la partition $\{I_1,\dots,I_r\}$ de $[\![1,k]\!]$ regroupant les indices de sorte que les valeurs de la liste en ces indices soient identiques. Plus concrètement :

$$\begin{aligned} \forall s \in [\![1,r]\!],\ \forall m,l \in I_s, \quad & i_l = i_m, \\ \forall s,t \in [\![1,r]\!], s \neq t,\ \forall (l,m) \in I_s \times I_t \quad & i_l \neq i_m. \end{aligned}$$

Par exemple, si $k=7$ et $n=5$, alors $P_{(1,3,2,3,1,5,1)} = \{\{1,5,7\},\{2,4\},\{3\},\{6\}\} \in \mathscr{P}_{7,4}$.
f est bien définie à la source car si $(i_1,\dots,i_k) \in [\![1,n]\!]^k$ et $\sigma \in \mathfrak{S}_n$, alors $\mathscr{R}_{(i_1,\dots,i_k)} = \mathscr{R}_{(\sigma(i_1),\dots,\sigma(i_k))}$ et f est bien définie au but car, si $k \leqslant n$, alors il y a forcément moins de n éléments dans une partition $P_{(i_1,\dots,i_k)}$ et si $k > n$, alors dans toute liste $(i_1,\dots,i_k) \in [\![1,n]\!]^k$, il y a au plus n éléments distincts, et donc au plus n éléments dans la partition $P_{(i_1,\dots,i_k)}$. De plus, f est bijective par définition de la relation $\mathscr{R}_{(i_1,\dots,i_k)}$ et par le fait que $\mathfrak{S}_n$ agit transitivement sur $[\![1,n]\!]$. En effet, on a la caractérisation suivante de $\mathfrak{S}_n \cdot (i_1,\dots,i_k)$:

$$\mathfrak{S}_n \cdot (i_1,\dots,i_k) := \{(\sigma(i_1),\dots,\sigma(i_k)) \mid \sigma \in \mathfrak{S}_n\} = \left\{(m_1,\dots,m_k) \in [\![1,n]\!]^k \;\middle|\; P_{(m_1,\dots,m_k)} = P_{(i_1,\dots,i_k)}\right\}.$$

Si on reprend l'exemple précédent,

$$\begin{aligned} \mathfrak{S}_5 \cdot (1,3,2,3,1,5,1) &= \{(\sigma(1),\sigma(3),\sigma(2),\sigma(3),\sigma(1),\sigma(5),\sigma(1)) \mid \sigma \in \mathfrak{S}_5\} \\ &= \{(a,b,c,b,a,d,a) \mid a,b,c,d \in [\![1,5]\!] \text{ distincts 2 à 2}\}, \end{aligned}$$

et on a bien que $P_{(a,b,c,b,a,d,a)} = P_{(1,2,3,2,1,5,1)}$.
Ainsi, on a :

$$\left|\frac{[\![1,n]\!]^k}{\mathfrak{S}_n}\right| = \sum_{j=1}^{n} |\mathscr{P}_{k,j}| = \sum_{j=1}^{n} S(k,j).$$

Vérifions pour finir que les moments de la loi de Poisson $\mathscr{P}(1)$ sont égaux aux nombres de Bell. Il s'agit en fait exactement de la formule de Dobinski (cf. application 2.1.1) que l'on redémontre via les nombres de Stirling de deuxième espèce :

$$\forall k \in \mathbb{N}, \quad e^{-1}\sum_{i=0}^{+\infty}\frac{i^k}{i!} = e^{-1}\sum_{i=0}^{+\infty}\sum_{j=0}^{k} S(k,j) i^{\underline{j}}\frac{1}{i!}.$$

Or, pour $i \leqslant j$, $i^{\underline{j}} = 0$. Donc :

$$e^{-1}\sum_{i=0}^{+\infty}\frac{i^k}{i!} = e^{-1}\sum_{j=0}^{k}\sum_{i=j}^{+\infty} S(k,j)\frac{i^{\underline{j}}}{i!} = e^{-1}\sum_{j=0}^{k} S(k,j)\sum_{i=j}^{+\infty}\frac{1}{(i-j)!} = \sum_{j=0}^{k} S(k,j) = B_k.$$

Cela termine la preuve !

□

C Questions possibles

1. **Pour une application entre deux ensembles finis de même cardinal, il y a équivalence entre injectivité, surjectivité et bijectivité. Dans quel(s) autre(s) cas ce phénomène se retrouve-t-il ?**

Réponse : Si on considère une application linéaire entre deux espaces vectoriels de dimension finie égales, alors on a également équivalence entre injectivité, surjectivité et bijectivité.

Références

[3Bl] 3Blue1Brown. Olympiad level counting (Generating functions) - https ://www.youtube.com/watch ?v=bOXCLR3Wric.

[Ber20] Grégory Berhuy. *Algèbre : le grand combat*. Calvage & Mounet, 2020.

[CG13] Philippe Caldero and Jérôme Germoni. *Histoires hédonistes de groupes et de géométrie*, volume 1. Calvage & Mounet, 2013.

[CG15] Philippe Caldero and Jérôme Germoni. *Histoires hédonistes de groupes et de géométrie*, volume 2. Calvage & Mounet, 2015.

[Exc] Math Stack Exchange. Sum of k-th powers of numbers of fixed points of permutations of $\{1, 2, ..., n\}$ - https ://math.stackexchange.com/questions/3805970/sum-of-k-th-powers-of-numbers-of-fixed-points-of-permutations-of-1-2-cdots.

[FGN07] Serge Francinou, Hervé Gianella, and Serge Nicolas. *Oraux X-ENS, Algèbre*, volume 1. Cassini, 2007.

[Gou21] Xavier Gourdon. *Les maths en tête - Algèbre et probabilités*. Ellipses, 2021.

[Goz97] Ivan Gozard. *Théorie de Galois*. Ellipses, 1997.

[Per96] Daniel Perrin. *Cours d'algèbre*. Ellipses, 1996.

[Ten22] Gérald Tenenbaum. *Introduction à la théorie analytique et probabiliste des nombres*. Dunod, 2022.