Méthodes Combinatoires, Problèmes de Dénombrement

Clément Legrand

31 juillet 2020

Introduction

Notre premier lien avec les mathématiques apparaît lorsqu'on apprend à compter. Au début on compte sur ses doigts, des bonbons et des pièces, mais bientôt cela ne suffit plus. Les nombres deviennent trop grands, les objets deviennent abstraits, et nous devons trouver de nouvelles manières (i.e. des outils) pour compter (i.e. dénombrer) ceux qui nous intéressent. Ces outils ne sont rien d'autre que des méthodes combinatoires, que l'on applique ensuite à divers problèmes de dénombrement.

Les problèmes de dénombrement se retrouvent par ailleurs dans toutes les branches des mathématiques, que ce soit en probabilité, en arithmétique ou en algèbre. Par exemple, à partir de méthodes combinatoires, on peut s'intéresser à la probabilité que deux nombres choisis aléatoirement, soient premiers entre eux. On peut également s'intéresser au nombre de manières de colorer les faces d'un cube avec k couleurs. Pour réaliser un tel dénombrement, il est fondamental de savoir utiliser des techniques d'algèbre faisant intervenir des actions de groupe.

Ce mémoire ne fournit pas une liste exhaustive des méthodes combinatoires, tant il y en a, et elles ne permettront pas non plus de traiter l'intégralité des problèmes de dénombrement auxquels le lecteur pourrait être confronté. En effet, la créativité joue souvent un rôle non négligeable dans la résolution de ce genre de problèmes, puisqu'il y a souvent plusieurs manières pour arriver au résultat. Par ailleurs, l'un des intérêts de savoir dénombrer de différentes manières est de pouvoir relier entre elles différentes quantités. Néanmoins ce mémoire fournit un aperçu des méthodes classiques et couramment utilisées en pratique pour résoudre des problèmes de dénombrement, et fournit au lecteur un bagage pour lui permettre de trouver par lui-même les réponses qu'il cherche. Des références sont également présentées si le lecteur souhaite en apprendre davantage sur une méthode en particulier. D'ailleurs, si le lecteur se trouve être passionné de problèmes combinatoires, il peut sans hésitations se lancer dans la lecture du livre [2], qui regorge de tels problèmes, et qui essaye d'adopter une manière pédagogique pour présenter la résolution des problèmes de dénombrement.

On commence par présenter la méthode combinatoire la plus naturelle pour dénombrer, qui consiste à établir une bijection entre deux ensembles, quand on connaît le cardinal de l'un des deux ensembles. Certains nombres souvent utilisés en dénombrement sont également introduits. Dans une deuxième partie, on présente le paradigme "diviser pour régner" dans le cadre des problèmes combinatoires. Toutefois, dans certains problèmes il est nécessaire d'utiliser des formules d'inversion pour revenir à la quantité recherchée. Une troisième partie introduit les séries génératrices, et présente quelques cas d'application typique. Enfin la dernière partie présente surtout des techniques d'algèbre pour résoudre certains problèmes de dénombrement, dont les coloriages.

Table des matières

1 Le cardinal pour dénombrer

Une première manière de dénombrer un ensemble peut être de rechercher un isomorphisme entre l'ensemble à dénombrer et un ensemble dont on connaît le cardinal. Les notions introduites sont présentes dans le livre [4].

1.1 Un peu de théorie des ensembles finis

Pour définir la notion d'ensembles finis, on se réfère à l'ensemble $\mathbb{N}^* = \mathbb{N} \setminus \{0\} = \{0, 1, \ldots\}$ des entiers naturels. Les sous-ensembles de $\mathbb{N}^*$ qui interviennent constamment dans la suite sont les $\{1, 2, \ldots, n\}$ et $\{m+1, m+2, \ldots, n\}$, qui seront notés respectivement $[n]$ et $[m+1, n]$ dans la suite. Par convention, $[n] = \emptyset$ si $n = 0$. Rappelons les propriétés suivantes, concernant l'ensemble des entiers naturels.

Proposition 1. Soient n et p deux entiers strictement positifs.

1. Il existe une bijection de l'intervalle $[n]$ sur l'intervalle $[p]$, si et seulement si $n = p$;
2. Pour tout sous-ensemble non vide E de $[n]$, il existe une bijection de E sur un intervalle $[p]$ tel que $p \leq n$;
3. Il existe une bijection de $[p]$ sur l'intervalle $[n+1, n+p]$.

On en vient alors à la définition d'un ensemble fini.

Définition 2. On dit qu'un ensemble E, est *fini*, s'il existe une bijection de l'intervalle $[n]$ de $\mathbb{N}^*$ sur E. Une telle bijection est alors appelée *numérotation* de E.

Si E est un ensemble fini, il ne peut être mis en bijection, d'après la proposition 1, qu'avec un seul intervalle de la forme $[n]$. Cet entier est donc déterminé de manière unique.

Définition 3. On appelle *cardinal* de E, l'unique entier n tel que E soit en bijection avec $[n]$. On le note $\text{card}(E)$ ou encore $|E|$ s'il n'y a pas ambiguïté. On dit encore que E contient n éléments.

Dans la suite, on convient que l'ensemble vide est fini et on pose $|\emptyset| = 0$.

Exemple 4. $\{2, 4, 8, 16\}$ est un ensemble fini de cardinal 4, mais $\mathbb{N}$, $\mathbb{Q}$ et $\mathbb{R}$ ne le sont pas.

La proposition suivante est une conséquence immédiate de la définition du cardinal et de la proposition 1.

Proposition 5.

1. Toute partie d'un ensemble fini est finie ;
2. Deux ensembles finis E et F ont le même cardinal, si et seulement s'il existe une bijection de E sur F.

On définit ensuite les trois opérations ensemblistes usuelles, que sont l'union, l'intersection et le produit cartésien.

Définition 6. Soient E et F deux sous-ensembles. L'union de E et F, noté $E \cup F$ est l'ensemble des éléments qui sont soit dans E, soit dans F (non exclusif). On a

$$E \cup F = \{x | x \in E \vee x \in F\}.$$

On peut étendre cette définition à une famille finie d'ensembles. Soit I une partie de $\mathbb{N}$, $(E_i)_{i \in I}$ une famille d'ensembles. On a

$$\bigcup_{i \in I} E_i = \{x | \exists i \in I, x \in E_i\}.$$

Définition 7. Soient E et F deux sous-ensembles. L'intersection de E et F, noté $E \cap F$ est l'ensemble des éléments qui sont à la fois dans E et dans F (non exclusif). On a

$$E \cap F = \{x | x \in E \wedge x \in F\}.$$

Soit I une partie de $\mathbb{N}$, $(E_i)_{i \in I}$ une famille d'ensembles. On a

$$\bigcap_{i \in I} E_i = \{x | \forall i \in I, x \in E_i\}.$$

Définition 8. Soient E et F deux sous-ensembles. Le produit cartésien de E et F, noté $E \times F$ est l'ensemble des paires d'éléments dont le premier élément est dans E, et dont le deuxième est dans F. On a

$$E \times F = \{(x, y) | x \in E \wedge y \in F\}.$$

Soient $E_1, \ldots, E_n$ une famille d'ensembles. On a

$$E_1 \times E_2 \times \ldots \times E_p = \{x = (x_1, x_2, \ldots, x_p) | \forall i \in [p], x_i \in E_i\}.$$

1.2 Calcul de cardinaux

On s'intéresse dans la suite à des formules donnant le cardinal des ensembles définis précédemment. De cette manière, si dans le cadre d'un problème de dénombrement on parvient à se ramener au dénombrement de l'un de ces ensembles, on pourra s'en sortir.

On rappelle que deux ensembles E et F sont dits disjoints, si leur intersection est vide, i.e. $E \cap F = \emptyset$. Dans ce cas on note $E + F$ leur réunion. On a alors la propriété suivante concernant le cardinal d'une union de deux ensembles disjoints.

Proposition 9 (Formule de la somme). Si E et F sont deux ensembles finis disjoints, leur réunion $E + F$ est finie et l'on a :

$$|E + F| = |E| + |F|.$$

On peut alors étendre la formule précédente par récurrence sur $k \in \mathbb{N}^*$, si $E_1, \ldots, E_k$ sont des ensembles finis et disjoints deux à deux, alors

$$|E_1 + \ldots + E_k| = |E_1| + \ldots + |E_k|.$$

Proposition 10. Si E et F sont finis mais non nécessairement disjoints, on a la formule dite des "quatre cardinaux"

$$|E \cup F| + |E \cap F| = |E| + |F|$$

.

On dispose également d'une formule plus générale pour l'union de n ensembles, appelée formule du crible de Poincaré, ou encore principe d'inclusion-exclusion.

Proposition 11 (Principe d'inclusion-exclusion). Soient $n \geq 2$ et $E_1, \ldots, E_n$ des ensembles quelconques, éventuellement vides, mais finis. Alors

$$|E_1 \cup E_2 \cup \ldots \cup E_n| = \sum_{k=1}^{n} (-1)^{k-1} \sum_{1 \leq i_1 < \ldots < i_k \leq n} |E_{i_1} \cap \ldots \cap E_{i_k}|.$$

Exemple 12. Grâce à cette formule, on peut déterminer le nombre $S_{p,n}$ de surjections de $[p]$ dans $[n]$. Montrons le résultat suivant.

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

Pour $y \in [n]$, soit E_y l'ensemble des applications de $[p]$ dans $[n]$ qui ne prennent jamais la valeur y. Une surjection de $[p]$ dans $[n]$, est alors une application qui ne se retrouve dans aucun des E_y. Autrement dit, $S_{p,q} = |[p]^{[n]}| - |\bigcup_{y\in[p]} E_y|$. D'après le principe d'inclusion-exclusion, on a :

$$\left|\bigcup_{y\in[p]} E_y\right| = \sum_{k=1}^{n} (-1)^{k-1} \sum_{\substack{Y\subset[n]\\|Y|=k}} |E_Y|.$$

où $E_Y = \bigcap_{y\in Y} E_y$ est l'ensemble des applications de $[p]$ dans $[n]$ telles qu'aucun élément de Y n'a d'antécédent. On remarque qu'il y en a autant que d'applications de $[p]$ dans $[n] \setminus Y$, et donc $|E_Y| = (n - |Y|)^p$. En remplaçant dans la formule, il vient :

$$\begin{aligned}
\left|\bigcup_{y\in[p]} E_y\right| &= \sum_{k=1}^{n} (-1)^{k-1} \sum_{\substack{|Y|=k\\Y\subset[n]}} (n-k)^p \\
&= \sum_{k=1}^{n} (-1)^{k-1} (n-k)^p |\{Y \subset [n] || Y| = k\}| \\
&= \sum_{k=1}^{n} (-1)^{k-1} (n-k)^p \binom{n}{k}
\end{aligned}$$

On peut alors revenir à l'expression de $S_{p,n}$ et en utilisant la symétrie des coefficients binomiaux : $\binom{n}{k} = \binom{n}{n-k}$, on obtient bien le résultat voulu.

Exemple 13. On peut aussi calculer la probabilité que deux nombres entiers soient premiers entre eux. On reviendra sur ce résultat après avoir introduit la formule d'inversion de Möbius dans la section 2.

La formule de la somme peut être reformulée de façon intuitive en une règle de la somme : "si un objet a peut être choisi de n façons et un objet b de p autres façons, il y $n + p$ façons de choisir soit a, soit b". Toutefois cet énoncé conserve une légère ambiguïté et c'est justement le langage de la théorie des ensembles qui permet de lever celle-ci, avec le produit cartésien.

Proposition 14 (Formule du produit). Si E et F sont deux ensembles finis (non nécessairement disjoints), alors le produit cartésien $E \times F$ est fini et on a

$$|E \times F| = |E| \cdot |F|.$$

La formule précédente se prolonge également au cas de $n \geq 2$ ensembles finis. Ainsi, on obtient pour toute suite $E_1, \ldots, E_n$ d'ensembles finis, la formule

$$|E_1 \times \ldots \times E_n| = |E_1| \times \ldots \times |E_n|.$$

De même la règle du produit s'énonce comme suit : "si un objet a peut être choisi de n façons **et qu'ensuite** un objet b peut être choisi de p façons, la paire (a, b), prise dans cet ordre, peut être choisie de np façons".

Dans le langage fonctionnel, on peut dire que l'ensemble B^A de toutes les applications d'un ensemble A, de cardinal p, dans un ensemble B, de cardinal n, a pour cardinal n^p.

Exemple 15. Le nombre de parties d'un ensemble à n éléments, est 2^n. En effet si $b_1, \ldots, b_n$ sont les éléments de B numérotés, toute partie A de B est entièrement caractérisée par la donnée d'une suite $(x_1, \ldots, x_n)$, où pour $1 \leq i \leq n$ chaque x_i vaut 0 ou 1. On a donc une bijection entre les parties de B et $\{0, 1\}^n$.

Exemple 16. L'alphabet Braille, est un alphabet adapté pour les malvoyants, dont chaque caractère peut être codé avec au plus 6 points. On peut donc coder $2^6 = 64$ caractères différents, ce qui permet de coder l'intégralité de notre alphabet, ainsi que les chiffres et les symboles de ponctuation.

On dispose également d'un résultat fort utile en pratique, connu sous le nom de lemme des bergers, qui s'énonce comme suit.

Proposition 17 (Lemme des bergers). Soient A et B deux ensembles finis, de cardinaux respectifs a et b. Soit $f : A \to B$ une surjection telle que pour tout y $\in B$, $|f^{-1}(y)| = c$, où $c \in \mathbf{N}$, alors on a $a = b \times c$.

Exemple 18. L'application la plus simple de ce lemme, et qui lui donne son nom également, est la suivante. Un berger souhaite compter ses moutons, mais il ne voit que leurs pattes. Chaque mouton ayant 4 pattes, s'il voit 36 pattes, c'est qu'il y a en fait $\frac{36}{4} = 9$ moutons, d'après le lemme des bergers.

Exemple 19. On peut utiliser ce résultat pour dénombrer les sous-espaces vectoriels de dimension finie sur les corps finis. Soit $\mathbf{K}$ un corps fini de cardinal q. Soit $n \in \mathbf{N}^*$, notons $E = \mathbf{K}^n$ un $\mathbf{K}$-espace vectoriel. Cherchons ses sous-espaces vectoriels de dimension p, notons $S_q(n, p)$ leur nombre. Une base de E est la donnée d'un n-uplet de vecteurs de E linéairement indépendants. Pour construire une telle base, on dispose de $q^n - 1$ possibilités pour le premier vecteur (en effet il y a q possibilités pour chaque composante du vecteur, et le vecteur nul ne convient pas). Notons e_1 ce premier vecteur. Pour le deuxième vecteur, on peut prendre tous les vecteurs sauf ceux qui sont dans $vect(e_1)$, ce qui interdit tous les vecteurs de la forme $\mathbf{K}e_1$, c'est à dire q vecteurs. Il reste alors $q^n - q$ possibilités pour le deuxième vecteur, notons le e_2. En remarquant que $vect(e_1, e_2, \ldots, e_i)$ interdit q^i vecteurs, on déduit de proche en proche que le nombre de bases possibles pour E est $(q^n - 1)(q^n - q) \ldots (q^n - q^{n-1})$. Considérons alors l'application :

$$\begin{array}{rccc} f & : & \{\text{bases de } E\} & \to & \{\text{bases de } F\} \\ & & (e_1, e_2, \ldots, e_n) & \mapsto & (e_{i_1}, \ldots, e_{i_p}) \end{array}$$

où $(e_1, e_2, \ldots, e_n)$ est une base de E, F un sous-espace vectoriel de dimension p, et $(e_{i_1}, \ldots, e_{i_p})$ une base de cet espace. Cette application est clairement surjective. Pour appliquer le lemme des bergers, il reste à savoir combien de familles libres de taille p on peut former dans E. On peut raisonner exactement de la même manière que précédemment, en s'arrêtant dès qu'on a p vecteurs. Ceci donne un total de $(k^n - 1) \ldots (k^n - k^{p-1})$ familles. En appliquant le lemme des bergers on obtient alors :

$$S_k(n, p) = \frac{(k^n - 1)(k^n - k) \ldots (k^n - k^{n-1})}{(k^n - 1) \ldots (k^n - k^{p-1})} = \frac{(k^n - 1)(k^{n-1} - 1) \ldots (k^{n-p+1} - 1)}{(k^p - 1)(k^{p-1} - 1) \ldots (k - 1)}.$$

Si $p = 0$, par convention, on prendra $S_k(n, 0) = 1$. Ces entiers sont également appelés coefficients binomiaux de Gauss. En particulier avec $k = 3, n = 3$, on en déduit qu'il y a $S_3(3, 0) + S_3(3, 1) + S_3(3, 2) + S_3(3, 3) = 28$ sous-espaces vectoriels dans $(\mathbf{F}_3)^3$.

1.3 Arrangements

Définition 20. Supposons B de cardinal n. Une suite $(c_1, \ldots, c_p)$ est dite (p, n)-injective, si elle est de longueur n, si tous ses termes c_i sont pris dans B et si tous les c_i sont distincts. On appelle une telle suite, un **arrangement**. L'ensemble de tous les arrangements de p éléments dans un ensemble à n éléments est noté $\mathcal{A}(p, n)$, et son cardinal $A(p, n)$.

Proposition 21. Si $0 \leq p \leq n$, le nombre d'arrangements $A(p, n)$ est donné par :

$$A(p, n) = \frac{n!}{(n-p)!} = n(n-1)\ldots(n-p+1).$$

Exemple 22. En particulier, le nombre de permutations d'un ensemble de cardinal n est égal à $A(n, n) = n!$.

Dans le langage fonctionnel $A(p, n)$ est le cardinal de l'ensemble des injections d'un ensemble de cardinal p dans un ensemble de cardinal n.

Un résultat fort utile en probabilités et souvent utilisé en pratique est celui du paradoxe des anniversaires.

Proposition 23 (Les anniversaires). Parmi n personnes, la probabilité pour qu'au moins deux d'entre elles aient leur anniversaire le même jour est $P_n = 1 - \frac{A(n,365)}{365^n}$.

En particulier on a les valeurs approchées suivantes : $P_{15} = 0,25$, $P_{23} = 0,51$, $P_{32} = 0,75$ et $P_{55} = 0,99$.

Ce paradoxe est notamment utilisé en cryptographie pour prouver certaines propriétés sur des tests de primalité tels que celui de Miller-Rabin.

1.4 Combinaisons

1.4.1 Coefficients binomiaux

Lorsqu'on s'intéresse aux parties de taille $p \geq 0$ d'un ensemble à $n \geq 0$ éléments, on voit apparaître d'autres nombres remarquables : les coefficients binomiaux.

Définition 24. Soient $p \geq 0$ et $n \geq 0$ deux entiers. Le nombre de parties à p éléments d'un ensemble à n éléments est noté $\binom{n}{p}$, et se lit "p parmi n". Ces nombres sont appelés coefficients binomiaux et sont définis par la relation de récurrence :

$$\binom{n}{p} = \binom{n-1}{p-1} + \binom{n-1}{p}.$$

avec les conditions initiales : $\binom{n}{0} = 1$ pour tout $n \geq 0$ et $\binom{0}{p} = 0$ pour tout $p \geq 1$.

Cette relation peut s'obtenir de manière intuitive en remarquant que pour construire une partie à p éléments dans un ensemble à n éléments, soit on part d'une partie à $p-1$ éléments dans un ensemble à $n-1$ éléments, puis on ajoute le n-ième élément pour avoir p éléments, soit on n'utilise pas le n-ième élément, et on prend une partie à p éléments dans un ensemble à $n-1$ éléments. Les petites valeurs de ces coefficients sont visibles dans le tableau 1, et forment une figure appelée triangle de Pascal.

Exemple 25. Les coefficients binomiaux apparaissent naturellement, lorsqu'on élève une somme de deux termes à la puissance n. En effet, si on cherche à développer $(a+b)^n$, dans la somme

	$p=0$	1	2	3
$n=0$	1			
1	1	1		
2	1	2	1	
3	1	3	3	1

TABLE 1 – Triangle de Pascal

on aura uniquement des termes de la forme $a^p b^{n-p}$, et pour obtenir un tel terme il a fallu choisir p fois le terme a dans le produit des n termes, il y a donc exactement $\binom{n}{p}$ manières d'obtenir ce terme. D'où la formule du binôme de Newton :

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

Proposition 26. On peut expliciter la valeur de $\binom{n}{p}$ pour $0 \leq p \leq n$:

$$\binom{n}{p} = \frac{n!}{p!(n-p)!} = \frac{1}{p!} A(n,p).$$

Exemple 27. Il y a exactement 144 mains de cinq cartes d'un jeu de bridge contenant exactement deux as, deux rois et une dame.

Exemple 28. Le nombre de suites strictement croissantes de longueur p, où les termes sont extraits d'un ensemble de cardinal n est $\binom{n}{p}$. De plus le nombre de telles suites croissantes est égal à $\binom{n+p-1}{p}$. En effet soit $c = (c_1 \leq c_2 \leq \ldots \leq c_n)$ une suite croissante. On lui fait correspondre la suite $d = (d_1 < d_2 < \ldots < d_n)$, définie par :

$$d_1 = c_1 \, ; d_2 = c_2 + 1 \, ; \ldots ; d_n = c_n + p - 1.$$

La suite d ainsi formée est bien strictement croissante. De plus,

$$1 \leq d_1 < d_2 < \ldots < d_n \leq n + p - 1.$$

L'application $c \mapsto d$ envoie bijectivement l'ensemble des suites croissantes dans l'ensemble des suites strictement croissantes de longueur p dont les termes sont pris dans $[n+p-1]$. Comme le cardinal de l'ensemble de ces dernières suites est égal $\binom{n+p-1}{p}$, c'est aussi le nombre de suites croissantes voulu.

Proposition 29. Le nombre de suites $(x_1, \ldots, x_p)$ qui sont solutions en nombres entiers positifs de l'équation (à n et p fixés) :

$$x_1 + x_2 + \ldots + x_p = n.$$

est égal au coefficient binomial $\binom{n+p-1}{n}$.

Démonstration. Soit $x = (x_1, \ldots, x_p)$ une telle solution. On lui associe, la suite croissante $y = (y_1, \ldots, y_p)$ définie par $y_i = 1 + x_1 + \ldots + x_i$, pour $i \in [p]$. On a : $1 \leq y_1 \leq \ldots \leq y_{n-1} \leq y_n = 1 + n$. Réciproquement, si y est une telle suite, on définit $x = (x_1, \ldots, x_n)$ par : $x_i = y_i - y_{n-i}$, pour $i \in [2, n]$ et $x_1 = y_1 - 1$. Il y a donc une bijection entre les solutions x de l'équation et les suites croissantes, au sens large, de longueur $(p-1)$, dont les termes sont pris dans $[1+n]$. D'après le résultat précédent, le cardinal de l'ensemble des solutions est :

$$\binom{(1+n)+(p-1)-1}{p-1} = \binom{n+p-1}{p-1} = \binom{n+p-1}{n}.$$

□

1.4.2 Coefficients multinomiaux

On peut généraliser la notion de coefficients binomiaux avec les coefficients multinomiaux.

Définition 30. Soient n et k deux entiers tels que $1 \leq k \leq n$, ainsi qu'une suite d'entiers $(n_1, \ldots, n_k)$ satisfaisant à :

$$n_1 \geq 0, n_2 \geq 0, \ldots, n_k \geq 0 \text{ et } n_1 + n_2 + \ldots + n_k = n.$$

Un coefficient multinomial est un nombre de la forme : $\frac{p!}{n_1!n_2!\ldots n_k!}$. On le note $\binom{n}{n_1,n_2,\ldots,n_k}$. Dans le cas où $k = 2$, on a $n_1 + n_2 = n$ et on retrouve le coefficient binomial : $\binom{n}{n_1,n_2} = \binom{n}{n_1}$.

Exemple 31. Le nombre de suites de longueur p, contenant n_1 fois 1, n_2 fois 2, ..., n_k fois k, où les n_i satisfont les relations ci-dessus, est égal au coefficient multinomial $\binom{n}{n_1,\ldots,n_k}$.

Exemple 32. On peut ainsi compter le nombre d'anagrammes du mot *BONBON*, qui contient 2 lettres B, 2 lettres O et 2 lettres N : $\binom{6}{2,2,2} = \frac{6!}{2!2!2!} = 90$.

La formule binomiale admet également une extension multinomiale, exprimée avec la proposition suivante.

Proposition 33. Soient $z_1, \ldots, z_k$ des éléments pris dans un anneau commutatif. On a l'identité multinomiale :

$$(z_1 + z_2 + \ldots + z_k)^n = \sum \binom{n}{n_1, \ldots, n_k} z_1^{n_1} z_2^{n_2} \ldots z_k^{n_k}$$

où la sommation est étendue à l'ensemble des suites $(n_1, \ldots, n_k)$ d'entiers satisfaisant à : $n_1 \geq 0, \ldots, n_k \geq 0$ et $n_1 + \ldots + n_k = n$.

2 Formules d'inversion et applications

En pratique, pour résoudre un problème de dénombrement, on essaie souvent d'appliquer le paradigme "diviser pour régner" : si on essaye de résoudre un problème de taille n, on va essayer de décomposer le problème en sous-problèmes de taille inférieure, souvent disjoints, puis appliquer la règle de la somme pour revenir au problème de départ. Par exemple si on cherche à compter $u(n)$, on va essayer de trouver un ensemble d'entiers E, et pour chaque $i \in E$, trouver un nombre $v(i)$ tel que $u(n) = \sum_{i \in E} v(i)$. Toutefois, en pratique c'est souvent la quantité v qui est au final recherchée. Dans certains cas on peut échanger le rôle de u et v via une formule dite d'inversion. Nous présentons dans cette section deux telles formules. Les notations et notions introduites s'inspirent de [6], certains exemples viennent de [2]

2.1 Formule d'inversion de Pascal

Supposons que l'on soit parvenu à établir une formule de la forme suivante.

$$f_n = \sum_{k=0}^{n} \binom{n}{k} g_k$$

. Si la quantité qui nous intéresse est g_k alors on dispose d'une formule, dite formule d'inversion de Pascal pour échanger les rôles de f et g.

Proposition 34 (Inversion de Pascal). Si $(f_n)_{n\in\mathbf{N}}$ et $(g_n)_{n\in\mathbf{N}}$ sont deux suites de réels telles que :

$$\forall n \in \mathbf{N}, f_n = \sum_{k=0}^{n} \binom{n}{k} g_k$$

on a alors :

$$\forall n \in \mathbf{N}, g_n = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} f_k.$$

Exemple 35. En remarquant que l'ensemble des applications de $[p]$ dans $[n]$ peut s'écrire comme la réunion disjointe des ensembles d'applications où $k \in \{0, \dots, n\}$ éléments de l'ensemble d'arrivée ont des antécédents, on obtient une nouvelle manière de compter le nombre de surjections de $[p]$ dans $[n]$. En effet, pour obtenir le nombre d'applications où exactement k éléments ont des antécédents, il suffit de choisir les k éléments (il y en a $\binom{n}{k}$), puis de multiplier par le nombre de surjections vers les k éléments choisis : $S_{p,k}$. On a alors : $n^p = \sum_{k=0}^{n} \binom{n}{k} S_{p,k}$. En appliquant la formule d'inversion de Pascal, on a $S_{p,n} = \sum_{k=0}^{n} \binom{n}{k} (-1)^{n-k} k^p$. Et on retrouve bien le résultat de la section 1.

Exemple 36. Intéressons-nous à présent au nombre de dérangements D_n d'un ensemble fini $[n]$. On rappelle qu'un dérangement est simplement une permutation sans points fixes (i.e. il n'y a pas d'entiers i tels que $\sigma(i) = i$). On peut remarquer que l'ensemble des permutations (de cardinal $n!$) est la réunion disjointe des sous-ensembles composés des permutations dans lesquelles il y a exactement $n - k$ points fixes. Or pour obtenir le nombre de permutations ayant exactement $n - k$ points fixes, il suffit de choisir les $n - k$ points fixes, puis de déranger les k éléments restants, ce qui nous donne au total $\binom{n}{n-k} D_k = \binom{n}{k} D_k$. On a alors : $n! = \sum_{k=0}^{n} \binom{n}{k} D_k$, et en appliquant la formule d'inversion de Pascal, cela nous donne : $D_n = \sum_{k=0}^{n} \binom{n}{k} (-1)^{n-k} k! = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}$.

2.2 Formule d'inversion de Möbius

2.2.1 Fonction de Möbius et produit de convolution

Dans la suite, pour $n \geq 2$ on notera $\mathcal{D}_n$ l'ensemble de tous les diviseurs strictement positifs de n. Nous introduisons ici une nouvelle fonction arithmétique, qui est la fonction de Möbius.

Définition 37. Soit $n \in \mathbf{N}$. On note $n = \prod_{i=1}^{r} p_i^{\alpha_i}$, sa décomposition en facteurs premiers, où $r \geq 1$, les p_i sont premiers deux à deux distincts, et les α_i des entiers naturels non nuls. On définit la fonction de Möbius par :

$$\forall n \in \mathbf{N}^* \mu(n) = \begin{cases} 1 & \text{si } n = 1, \\ (-1)^r & \text{si } n = \prod_{i=1}^{r} p_i \quad \text{(i.e. } n \text{ est sans facteurs carrés)}, \\ 0 & \text{sinon .} \end{cases}$$

Proposition 38. Si m et n sont deux entiers premiers entre eux, on a alors $\mu(mn) = \mu(m)\mu(n)$. On dit alors que μ est une fonction multiplicative

On introduit également le produit de convolution (ou de Dirichlet) de deux suites réelles.

Définition 39. Soient u et v deux suites réelles de $\mathbf{R}^{\mathbf{N}^*}$, on appelle produit de Dirichlet de u et v et on note $u * v$, la suite définie par :

$$\forall n \in \mathbf{N}^*, (u * v)(n) = \sum_{d \in \mathcal{D}_n} u(d) v\left(\frac{n}{d}\right).$$

On dispose également du résultat suivant, concernant le produit de deux sommes.

Proposition 40. Soient $(u_n)_{n\in\mathbf{N}^*}$ et $(v_n)_{n\in\mathbf{N}^*}$ deux suites à valeurs réelles, et $(w_n)_{n\in\mathbf{N}^*}$ leur produit de convolution. Si les séries $\sum u_n$ et $\sum v_n$ sont absolument convergentes, il en est de même de la série $\sum w_n$ et on a :

$$\sum_{n=1}^{+\infty} w_n = \left(\sum_{n=1}^{+\infty} u_n\right)\left(\sum_{n=1}^{+\infty} v_n\right).$$

Pour le produit de Dirichlet, la fonction de Möbius est inversible. Plus précisément, on a le résultat suivant.

Proposition 41. En notant e le neutre de $\mathbf{R}^{\mathbf{N}^*}$ pour la loi $*$, et ω la suite constante égale à 1 (i.e. $\omega(n) = 1$ pour tout $n \in \mathbf{N}^*$), on a $\mu * \omega = e$, c'est-à-dire que :

$$\forall n \geq 1, \sum_{d \in \mathcal{D}_n} \mu(d) = \begin{cases} 1 & \text{si } n = 1, \\ 0 & \text{si } n \geq 2. \end{cases}$$

Démonstration. Le résultat pour $n = 1$ est évident car $\mu(1) = 1$. Si $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ est la décomposition en facteurs premiers de l'entier $n \geq 2$, tous les diviseurs de n sont alors de la forme $d = \prod_{i=1}^{r} p_i^{\beta_i}$ avec $0 \leq \beta_i \leq \alpha_i$, pour $1 \leq i \leq r$, et $\mu(d) = 0$ si l'un des β_i est supérieur ou égal à 2. Or pour $i \in [r]$, il y a exactement $\binom{r}{i}$ manières de choisir un r-uplet $(\beta_1, \ldots, \beta_r)$ formé de i termes égaux à 1 (et $r - i$ termes égaux à 0), et pour chacun de ces choix, on a $\mu(d) = (-1)^i$, donc :

$$\sum_{d \in \mathcal{D}_n} \mu(d) = \sum_{i=0}^{r} \binom{r}{i} (-1)^i = (1-1)^r = 0.$$

D'où le résultat pour $n \geq 2$. □

Enfin, pour clore cette partie, on présente un joli résultat concernant la probabilité que deux nombres soient premiers entre eux. Il fait intervenir des résultats décrits en section 1, ainsi que les propriétés de la fonction de Möbius.

Théoreme 42 (Probabilité que deux nombres soient premiers entre eux). Pour tout entier $n \geq 2$, on se place sur l'espace probabilisé $([n]^2, \mathcal{P}([n]^2), \mathbf{P})$, avec la mesure de probabilité $\mathbf{P}$ définie par :

$$\forall (a, b) \in [n]^2, \mathbf{P}(\{(a, b)\}) = \frac{1}{n^2}.$$

On s'intéresse à l'évènement $R_n = \{(a, b) \in [n]^2, a \wedge b = 1\}$ et on note $r_n = \mathbf{P}(R_n)$ sa probabilité. Alors on a :

$$\lim_{n \to +\infty} r_n = \frac{6}{\pi^2}.$$

Démonstration. La démonstration va se faire en trois étapes :
Etape 1 : Montrons dans un premier temps l'expression suivante de r_n :

$$\forall n \in \mathbf{N}^*, r_n = \frac{1}{n^2} \sum_{d=1}^{n} \mu(d) \left\lfloor \frac{n}{d} \right\rfloor^2.$$

Soit $n \in \mathbf{N}^*$. Notons $A_n = \{(a,b) \in [n]^2, a \wedge b = 1\}$, de sorte à avoir $r_n = \frac{|A_n|}{n^2}$. Notons également, $\{p_1, \dots, p_k\}$ les nombres premiers distincts de $[n]$. On cherche donc à déterminer $|A_n|$. Pour cela, on va chercher à appliquer la formule du crible. En notant :

$$\forall i \in [k], U_i = \{(a,b) \in [n]^2, p_i | a \text{ et } p_i | b\},$$

on remarque que :

$$A_n = \left(\bigcup_{i=1}^{k} U_i \right)^c.$$

En effet deux nombres a et b sont premiers entre eux si et seulement s'ils n'ont aucun diviseur premier en commun, si et seulement si pour tout $i \in [k]$, $(a,b) \notin U_i$.

On en déduit alors que $|A_n| = n^2 - \left| \bigcup_{i=1}^{k} U_i \right|$. La formule du crible donne alors :

$$\left| \bigcup_{i=1}^{k} U_i \right| = \sum_{\emptyset \neq I \subset [k]} (-1)^{1+|I|} \left| \bigcap_{i \in I} U_i \right|.$$

Or, pour $I = \{i_1, \dots, i_l\} \subset [k]$, on a : $\bigcap_{i \in I} U_i = \{(a,b) \in [n]^2, p_{i_1} \dots p_{i_l} | a \text{ et } p_{i_1} \dots p_{i_l} | b\}$, car si $p_{i_k} | a$ pour tout $k \in [l]$, comme les p_{i_k} sont des nombres premiers, ils sont deux à deux premiers entre eux, et donc leur produit divise a. De cela, on déduit $\left| \bigcap_{i \in I} U_i \right| = \left\lfloor \frac{n}{p_{i_1} \dots p_{i_l}} \right\rfloor^2$. En effet, seuls les entiers $(kp_{i_1} \dots p_{i_l}, k' p_{i_1} \dots p_{i_l})$ pour $k, k' \in \left\lfloor \frac{n}{p_{i_1} \dots p_{i_l}} \right\rfloor$, sont dans l'intersection des U_i. En revenant au calcul de A_n, on obtient alors :

$$\begin{aligned}
|A_n| &= n^2 - \sum_{\{i_1, \dots, i_l\} \subset [k]} (-1)^{1+l} \left\lfloor \frac{n}{p_{i_1} \dots p_{i_l}} \right\rfloor^2 \\
&= n^2 + \sum_{\{i_1, \dots, i_l\} \subset [k]} \mu(p_{i_1} \dots p_{i_l}) \left\lfloor \frac{n}{p_{i_1} \dots p_{i_l}} \right\rfloor^2 \\
&= n^2 + \sum_{d=2}^{n} \mu(d) \left\lfloor \frac{n}{d} \right\rfloor^2 \\
&= \sum_{d=1}^{n} \mu(d) \left\lfloor \frac{n}{d} \right\rfloor^2.
\end{aligned}$$

Notez que pour le passage de la deuxième à la troisième ligne, on décompose tous les entiers compris entre 2 et n en produit de facteurs premiers, et on remarque que tous les termes ajoutés sont en fait nuls.

Etape 2 : L'expression de r_n obtenue ne permet pas de conclure directement, quant à la probabilité asymptotique de l'évènement R_n. Toutefois, on sait que $\lfloor n \rfloor \underset{n \to +\infty}{\sim} n$, et cela nous donne l'intuition que :

$$\lim_{n \to +\infty} r_n = \sum_{d=1}^{+\infty} \frac{\mu(d)}{d^2}.$$

Montrons ce résultat. Pour tout entier $n \geq 1$, on a $\mu(n) \in \{-1, 0, 1\}$, donc $|\frac{\mu(n)}{n^2}| \leq \frac{1}{n^2}$, et en conséquence la série $\sum \frac{\mu(n}{n^2}$ est absolument convergente. Pour tout entier $n \geq 1$, on a :

$$\epsilon_n = \sum_{k=1}^{n} \frac{\mu(k)}{k^2} - r_n = \frac{1}{n^2} \sum_{k=1}^{n} \mu(k) \left(\left(\frac{n}{k}\right)^2 - \left\lfloor \frac{n}{k} \right\rfloor^2 \right)$$

avec, pour tout entier k compris entre 1 et n, $0 \leq \frac{n}{k} - 1 < \left\lfloor \frac{n}{k} \right\rfloor \leq \frac{n}{k}$. En élevant au carré, on obtient alors :

$$0 \leq \left(\frac{n}{k}\right)^2 - \left\lfloor \frac{n}{k} \right\rfloor^2 < \left(\frac{n}{k}\right)^2 - \left(\frac{n}{k} - 1\right)^2 = 2\frac{n}{k} - 1.$$

Ceci nous donne :

$$|\epsilon_n| \leq \frac{1}{n^2} \sum_{k=1}^{n} \left(\left(\frac{n}{k}\right)^2 - \left\lfloor \frac{n}{k} \right\rfloor^2 \right) < \frac{2}{n} \sum_{k=1}^{n} \frac{1}{k} - \frac{1}{n}.$$

Avec $\sum_{k=1}^{n} \frac{1}{k} \underset{n \to +\infty}{\sim} \log(n)$ et $\lim_{n \to +\infty} \frac{\log(n)}{n} = 0$, il en résulte que $\lim_{n \to +\infty} \epsilon_n = 0$. Donc la suite $(r_n)_{n \in \mathbf{N}^*}$ est convergente et $\lim_{n \to +\infty} r_n = \sum_{d=1}^{+\infty} \frac{\mu(d)}{d^2}$.

Etape 3 : Il ne reste plus qu'à calculer la somme $\sum_{d=1}^{+\infty} \frac{\mu(d)}{d^2}$. Pour cela on va montrer le résultat suivant :

$$\left(\sum_{d=1}^{+\infty} \frac{\mu(d)}{d^2} \right) \left(\sum_{n=1}^{+\infty} \frac{1}{n^2} \right) = 1.$$

Les séries $\sum \frac{1}{n^2}$ et $\sum \frac{\mu(n)}{n^2}$ sont absolument convergentes et on a :

$$\left(\sum_{d=1}^{+\infty} \frac{\mu(d)}{d^2} \right) \left(\sum_{n=1}^{+\infty} \frac{1}{n^2} \right) = \sum_{n=1}^{+\infty} w_n$$

où $w_1 = \mu(1) = 1$ et :

$$\forall n \geq 2, w_n = \sum_{d \in \mathcal{D}_n} \frac{\mu(d)}{d^2} \left(\frac{d}{n}\right)^2 = \frac{1}{n^2} \sum_{d \in \mathcal{D}_n} \mu(d) = 0.$$

Ceci nous donne le résultat voulu, et donc $\sum_{d=1}^{+\infty} \frac{\mu(d)}{d^2} = \frac{1}{\zeta(2)}$. On peut alors conclure :

$$\lim_{n \to +\infty} r_n = \sum_{d=1}^{+\infty} \frac{\mu(d)}{d^2} = \frac{1}{\zeta(2)} = \frac{6}{\pi^2}.$$

□

De manière analogue, si on note $r_{n,k}$ la probabilité que $k \geq 2$ entiers compris entre 1 et n soient premiers entre eux, on peut montrer que :

$$\lim_{n \to +\infty} r_{n,k} = \sum_{d=1}^{+\infty} \frac{\mu(d)}{d^k} = \frac{1}{\zeta(k)}.$$

2.2.2 La formule d'inversion et applications

On présente maintenant le principal résultat de cette section, qui s'obtient directement à partir de l'inversibilité de la fonction de Möbius.

Théoreme 43 (Formule d'inversion). Pour toutes suites u, v dans $\mathbf{R}^{\mathbf{N}^*}$, les assertions suivantes sont équivalentes :

$$\forall n \in \mathbf{N}^*, u(n) = \sum_{d \in \mathcal{D}_n} v(d),$$
$$\forall n \in \mathbf{N}^*, v(n) = \sum_{d \in \mathcal{D}_n} \mu(d) u\left(\frac{n}{d}\right).$$

Présentons maintenant quelques applications de cette formule.

Exemple 44. Soit Σ un alphabet à k lettres. On dit qu'un mot w sur cet alphabet est primitif s'il n'est pas la puissance d'un autre mot (la puissance n-ième d'un mot w^n est simplement la concaténation de n fois le mot w). Notons $M_k(n)$ le nombre de mots primitifs de longueur n sur un alphabet à k lettres. On remarque que tout mot w de n lettres sur Σ est soit un mot primitif de longueur n, soit n'est pas un mot primitif. Dans ce dernier cas, il existe alors un mot primitif r et un entier d tel que $w = r^d$. On en déduit que nécessairement $d|n$. Comme il y a k^n mots de longueur n sur un alphabet de k lettres, on a la relation : $k^n = \sum_{d \in \mathcal{D}_n} M_k(d)d$. En appliquant la formule d'inversion de Möbius, on obtient : $nM_k(n) = \sum_{d \in \mathcal{D}_n} \mu(d)k^{n/d}$. Par exemple, dans le cas où $n = 2$, un mot est primitif si et seulement s'il a deux lettres distinctes. Il est donc censé y avoir $\binom{k}{2}$ mots primitifs, et c'est bien le résultat que l'on retrouve avec la formule établie.

On rappelle que l'indicatrice d'Euler est définie de la manière suivante.

Définition 45. Soit $n \in \mathbf{N}^*$, on note $\phi(n)$, le nombre d'entiers de $[n]$ qui sont premiers avec n. Autrement dit :

$$\phi(n) = |\{p \in [n], p \wedge n = 1\}|.$$

On peut calculer les valeurs de ϕ à partir des valeurs de μ.

Proposition 46. Soit $n \in \mathbf{N}^*$. On a :

$$n = \sum_{d|n} \phi(d) \text{ et } \phi(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) d.$$

Exemple 47. Notons $\mathbf{F}_q$ un corps à $q = p^r$ éléments, avec p premier et $r \geq 0$. On va dénombrer les polynômes irréductibles sur $\mathbf{F}_q[X]$. Notons $A(n,q)$ l'ensemble des polynômes irréductibles unitaires de degré n de $\mathbf{F}_q[X]$ et $I(n,q) = |A(n,q)|$. On admet le résultat suivant, qui fait intervenir des résultats classiques sur les corps finis et sur les polynômes (le lecteur peut en trouver une preuve dans [6] en p. 423) :

$$X^{q^n} - X = \prod_{d|n} \prod_{P \in A(d,q)} P.$$

En passant aux degrés dans l'égalité précédente, on obtient :

$$q^n = \sum_{d|n} \sum_{P \in A(d,q)} deg(P) = \sum_{d|n} dI(d,q).$$

En appliquant la formule d'inversion de Möbius, on obtient :

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

De ce résultat on peut notamment déduire que sur un corps fini, il y a des polynômes irréductibles de tout degré.

3 Séries génératrices

Cette section n'a pas pour objectif de détailler complètement ce que sont les séries génératrices. Si le lecteur veut en apprendre davantage à leur sujet il trouvera son bonheur dans le livre [3], qui présente une méthode symbolique pour déterminer des séries génératrices. Ces dernières sont un outil puissant pour l'étude d'objets combinatoires, c'est pourquoi nous les introduisons ici, avec une mise en pratique sur quelques exemples.

3.1 Introduction aux séries génératrices

Cette première section motive l'introduction des séries génératrices, présente des séries génératrices usuelles, ainsi que les opérations élémentaires que l'on peut effectuer sur de telles séries.

3.1.1 Motivation

Les séries génératrices sont un outil algébrique qui permet de reformuler des problèmes de combinatoire afin de les transformer en des problèmes de manipulation d'expressions algébriques. En particulier, en combinatoire, il s'agit souvent de déterminer le nombre d'objets d'un certain type qui sont de taille n, ce qui donne lieu à une suite (a_n) dont on cherche à déterminer le n-ième terme. La fonction génératrice associée à la suite (a_n) est la série formelle :

$$a_0 + a_1 x + a_2 x^2 + \ldots = \sum_{k\geq 0} a_k x^k.$$

En particulier la série génératrice d'une suite finie est un polynôme.

Mais cela a-t-il vraiment un sens de parler de "somme infinie" ? C'est une vaste question, et on ne va pas trop l'aborder ici. On peut avoir deux points de vue en ce qui concerne les séries. D'un côté, un point de vue algébrique et formel, et c'est celui que nous adopterons ici, où x est une variable formelle. Avec ce point de vue, une série génératrice n'est rien d'autre qu'une nouvelle notation pour la suite (a_n), de sorte que les opérations que nous définirons plus bas apparaissent naturellement. Tant qu'on ne fera pas prendre à x des valeurs réelles, on pourra rester dans ce cadre. D'un autre côté on peut avoir un point de vue plus analytique et regarder pour quelles valeurs de x la série "converge". Si de plus on trouve un voisinage de 0 pour lequel la série est bien définie, la notion coïncide avec celle des séries entières.

Un premier exemple fondamental, et qui nous servira à de nombreuses reprises dans la suite, est celui de la série génératrice de la suite constante égale à 1. D'une part, elle est égale à :

$$A(x) = \sum_{n\geq 0} x^n.$$

On l'appelle la série géométrique (car elle correspond à la somme des termes d'une suite géométrique). On remarque que : $A(x) - 1 = xA(x)$, donc $(1-x)A(x) = 1$. Cela signifie que la

série formelle $A(x)$ a un inverse : la série formelle $(1-x)$, ce que l'on notera de manière un peu plus suggestive :

$$\sum_{n\geq 0} x^n = \frac{1}{1-x}.$$

En revenant un instant au point de vue analytique, on retrouve bien le résultat naturel, si on choisit $|x| < 1$.

On cherchera souvent à trouver ce genre de "formes closes" pour des séries génératrices, c'est-à-dire les écrire comme un quotient $\frac{P}{Q}$ de deux polynômes avec $Q(0) \neq 0$. Ce n'est pas toujours possible, mais ça le sera dans les problèmes combinatoires abordés ici. En particulier, si une suite vérifie une récurrence linéaire, sa série génératrice vérifiera une équation du premier degré, et on obtiendra une forme close. De plus si on cherche une forme close pour les coefficients a_n de la série génératrice, on peut utiliser le développement en série entière de la forme $\frac{P}{Q}$, après avoir effectué une décomposition en éléments simples, pour obtenir le résultat voulu. Évidemment pour pouvoir identifier les coefficients des deux séries il faut veiller à ce que le rayon de convergence soit strictement positif, ce qui sera le plus souvent le cas, en combinatoire.

3.1.2 Opérations sur les séries génératrices

Somme : La somme de deux séries génératrices A et B se définit de manière naturelle en sommant les suites correspondantes : $A + B = \sum_{n\geq 0} (a_n + b_n)x^n$.

Produit : Le produit de deux séries génératrices s'obtient en effectuant le produit de Cauchy des suites associées : $A \times B = \sum_{n\geq 0} \left(\sum_{k=0}^{n} a_k b_{n-k} \right) x^n$.

Inverse : La série formelle $\sum_{i\geq 0} a_i x^i$ a un inverse si et seulement si $a_0 \neq 0$, et cet inverse est également une série formelle. En effet, on veut trouver une série formelle $\sum_{j\geq 0} b_j x^j$ telle que :

$$\left(\sum_{i\geq 0} a_i x^i \right) \left(\sum_{j\geq 0} b_j x^j \right) = \sum_{k\geq 0} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) x^k = 1.$$

Il suffit alors d'identifier les coefficients, ce qui donne une infinité d'équations pour les a_i et les b_j. La première est $a_0 b_0 = 1$, qui nous dit que la condition $a_0 \neq 0$ est effectivement nécessaire. On choisit alors $b_0 = \frac{1}{a_0}$. La deuxième équation est $a_0 b_1 + a_1 b_0 = 0$, et comme $a_0 \neq 0$, on obtient $b_1 = -\frac{a_1 b_0}{a_0}$. On peut effectuer une récurrence sur n pour obtenir le coefficient b_n, connaissant les coefficients $b_0, \ldots, b_{n-1}$. L'équation $\sum_{i=0}^{n} a_i b_{n-i} = 0$ avec la condition $a_0 \neq 0$, nous donne alors b_n. En particulier, les fraction rationnelles de la forme $\frac{P}{Q}$ avec P et Q des polynômes et $Q(0) \neq 0$ peuvent s'écrire comme des séries formelles.

Dérivée : La dérivée au sens formel d'une série génératrice se définit, par analogie avec les polynômes, avec :

$$\left(\sum_{n\geq 0} a_n x^n \right)' = \sum_{n\geq 1} n a_n x^{n-1}.$$

Exemple 48. Soit G la série géométrique définie ci-dessus. Par définition, sa dérivée est $\sum_{n\geq 1} n x^{n-1}$, et en dérivant $\frac{1}{1-x}$, on obtient :

$$\sum_{n\geq 1} n x^{n-1} = \frac{1}{(1-x)^2}.$$

Si on continue de cette manière, on va pouvoir obtenir des formules pour $(1-x)^{-k}$ pour tout entier naturel k. En généralisant la formule du coefficient binomial, on va pouvoir étendre la formule du binôme aux exposants quelconques.

Définition 49. Soient r un réel et k un entier naturel. Alors on définit le coefficient binomial généralisé $\binom{r}{k}$, par :

$$\binom{r}{k} = \frac{r(r-1)\dots(r-k+1)}{k!}.$$

Évidemment, cette formule coïncide avec la formule connue des coefficients binomiaux.

Proposition 50 (Formule du binôme généralisée). Pour tout entier relatif k, on a :

$$(1+x)^k = \sum_{i\geq 0} \binom{k}{i} x^i.$$

En particulier, sachant que par définition, on a pour tout i :

$$\binom{-1}{i} = \frac{(-1)(-2)\dots(-i)}{i!} = (-1)^i \text{ et } \binom{-2}{i} = \frac{(-2)(-3)\dots(-2-i+1)}{i!} = (-1)^i(i+1)$$

on retrouve les expressions obtenues pour $(1-x)^{-1}$ et $(1-x)^{-2}$. Puisque les coefficients de la forme $\binom{-n}{i}$ avec i et n deux entiers naturels jouent un rôle particulièrement important quand on travaille avec des séries formelles, il peut être utile d'avoir la formule suivante, qui les relie aux coefficients binomiaux usuels.

Proposition 51. Soient n et i deux entiers naturels. Alors :

$$\binom{-n}{k} = (-1)^k \binom{n+k-1}{k}.$$

3.2 Applications

On présente dans cette section des exemples qui font intervenir les séries formelles, que ce soit pour simplement simplifier les calculs ou bien obtenir une formule close pour les coefficients d'une série donnée.

3.2.1 Un exemple typique : les partitions

Une partition d'un entier strictement positif n est une représentation de n comme somme d'autres entiers strictement positifs, regardée à permutation des termes près. Par exemple 4 peut être partitionné en $1+1+1+1$, en $1+1+2$, en $2+2$, et en 4. Les séries génératrices constituent un outil très puissant et particulièrement adapté pour traiter les problèmes sur les partitions.

Intéressons-nous au problème suivant : combien y a-t-il de manières de payer n euros avec des pièces de 1 et 2 euros (sans tenir compte de l'ordre) ?

Soit n un entier. Notons a_n le nombre recherché. Chaque manière de payer n euros avec r pièces de 1 et s pièces de 2 peut être encodée sous la forme $x^{1r}x^{2s} = x^n$, où r et s peuvent être des entiers naturels quelconques. La série génératrice de la suite (a_n) s'écrit donc :

$$\sum_{n\geq 0} a_n x^n = \left(\sum_{r\geq 0} x^r\right)\left(\sum_{s\geq 0} x^{2s}\right) = \frac{1}{1-x}\frac{1}{1-x^2} = \frac{1}{(1-x)^2(1+x)}$$

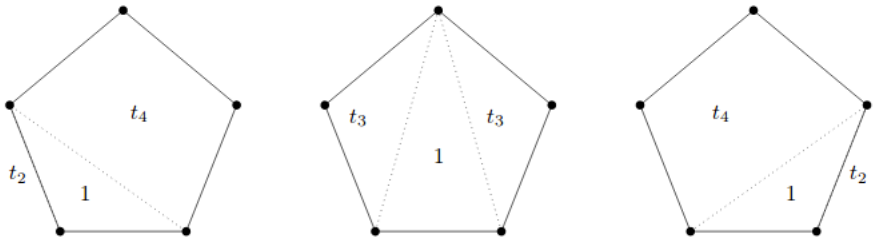

FIGURE 1 – Illustration des triangulations possibles du pentagone.

Une décomposition en éléments simples nous donne alors :

$$\frac{1}{(1-x)^2(1+x)} = \frac{\frac{1}{4}}{1-x} + \frac{\frac{1}{2}}{(1-x)^2} + \frac{\frac{1}{4}}{1+x}.$$

Ceci nous donne :

$$\begin{aligned}\sum_{n\geq 0} a_n x^n &= \frac{1}{2}\left(\frac{1}{(1-x)^2} + \frac{1}{1-x^2}\right) = \frac{1}{2}\left(\sum_{i\geq 0}(i+1)x^i + \sum_{j\geq 0} x^{2j}\right) \\ &= \frac{1}{2}\sum_{k\geq 0}(2k+2)(x^{2k}+x^{2k+1}) = \sum_{k\geq 0}(k+1)(x^{2k}+x^{2k+1}) \\ &= \sum_{n\geq 0}\left(\left\lfloor\frac{n}{2}\right\rfloor + 1\right)x^n.\end{aligned}$$

On a donc finalement $a_n = \left\lfloor\frac{n}{2}\right\rfloor + 1$. Bien entendu, on aurait très bien pu répondre à la question en calculant les premiers termes de la suite, puis conjecturer l'expression de a_n et la démontrer par récurrence. Cependant, la méthode des séries génératrices a l'avantage de se généraliser à tous les problèmes de ce type, même quand la formule est beaucoup moins devinable.

3.2.2 Triangulations d'un n-gone

Soit $n \geq 3$, un entier. Soit $\mathcal{P}_n$ un polygone convexe à n sommets $s_1, \ldots, s_n$. Dans le cas de la recherche du nombre de triangulations de $\mathcal{P}_n$, on peut supposer sans perte de généralité que le polygone est régulier. On appelle triangulation de $\mathcal{P}_n$, une partition de $\mathcal{P}_n$ en triangles. Notons t_n le nombre de triangulations possibles du polygone $\mathcal{P}_n$. On voit immédiatement que $t_3 = 1$ et que $t_4 = 2$. Par convention, on choisit $t_2 = 1$ pour la suite. Établissons une formule de récurrence pour le $(n+1)$-gone convexe. Choisissons une arête de $\mathcal{P}_{n+1}$ comme base du premier triangle. En fonction du troisième sommet on peut construire plusieurs triangles. Le choix d'un triangle coupe le polygone en deux polygones plus petits de tailles k et $n+2-k$.

La figure 1 illustre la méthode utilisée. Le nombre total de triangulations possibles est alors :

$$t_{n+1} = \sum_{k=2}^{n} t_k t_{n+2-k}.$$

Il est plus commode de commencer à numéroter la suite à partir de 0 plutôt qu'à partir de 2. Donc en posant $c_n = t_{n+2}$, on a :

$$c_0 = 1 \text{ et } c_{n+1} = \sum_{k=0}^{n} c_k c_{n-k}.$$

Les nombres c_n sont appelés nombres de Catalan. Considérons la série génératrice associée aux c_n :

$$C(x) = \sum_{n=0}^{+\infty} c_n x^n.$$

Déterminons à présent une équation vérifiée par C. D'après la formule du produit de Cauchy de deux séries, on a :

$$\begin{aligned} C(x)^2 &= \sum_{n=0}^{+\infty} \sum_{k=0}^{n} c_k c_{n-k} x^n \\ &= \sum_{n=0}^{+\infty} c_{n+1} x^n. \end{aligned}$$

Ceci nous donne $1 + xC(x)^2 = 1 + \sum_{n=0}^{+\infty} c_{n+1} x^{n+1} = C(x)$. L'idée est alors de résoudre l'équation polynomiale de degré $2 : 1 - C(x) + xC(x)^2 = 0$, pour deviner le résultat à montrer. On trouve : $C(x) \stackrel{?}{=} \frac{1 \pm \sqrt{1-4x}}{2x}$. Ici, comme $f(0) = c_0 = 1$, on va montrer le résultat suivant :

$$C(x) = \frac{1 - \sqrt{1-4x}}{2x} = \phi(x).$$

Déterminons dans un premier la série formelle associée à $\sqrt{1-4x}$:

$$\begin{aligned} \sqrt{1-4x} &= \sum_{n=0}^{+\infty} \frac{(1/2-1)\dots(1/2-n+1)}{n!} (-1)^n 4^n x^n \\ &= \sum_{n=0}^{+\infty} \frac{(-1)^{n+1}}{2^n n!(2n-1)} (1 \times \dots \times (2n-1))(-1)^n 4^n x^n \\ &= -\sum_{n=0}^{+\infty} \frac{1}{2^n n!(2n-1)} \frac{(2n)!}{2^n n!} 4^n x^n \\ &= 1 - \sum_{n=1}^{+\infty} \binom{2n}{n} \frac{x^n}{(2n-1)}. \end{aligned}$$

De cela, on déduit la série formelle associée à ϕ :

$$\phi(x) = \frac{1}{2x} \sum_{n=1}^{+\infty} \binom{2n}{n} \frac{x^n}{(2n-1)} = \sum_{n=1}^{+\infty} \binom{2n}{n} \frac{x^{n-1}}{(4n-2)} = \sum_{n=0}^{+\infty} \binom{2n+2}{n+1} \frac{x^n}{(4n+2)}.$$

Les séries C et ϕ vérifient la même équation fonctionnelle, en identifiant les coefficients des séries formelles associées, on obtient :

$$\forall n \in \mathbf{N}^*,\ c_n = \frac{1}{4n+2} \binom{2n+2}{n+1} = \frac{1}{n+1} \binom{2n}{n}.$$

4 Méthodes algébriques

Lorsqu'il est question de géométrie, l'algèbre n'est en général jamais très loin. Les problèmes de coloriage n'échappent pas à la règle. En effet, la difficulté majeure dans un problème de coloriage est qu'il ne faut pas compter deux fois le même coloriage. Pour résoudre ce problème, la manière classique est de raisonner sur les isométries de la figure (qui forment un groupe), puis de faire agir ce groupe sur la partie de la figure que l'on veut colorier. On dispose alors de résultats sur les actions de groupe, qui nous permettent de nous en sortir. Cette partie est inspirée de trois livres [1], [5] et [6].

4.1 Actions de groupe

Cette section sert principalement de rappels en ce qui concerne les actions de groupe. Les notations sont introduites, et plusieurs résultats utilisés dans la suite sont présentés. Dans la suite, on notera E un ensemble non vide et $\mathcal{S}(E)$ le groupe des permutations de E.

Définition 52. Une action à gauche du groupe G sur l'ensemble E est une application :

$$\begin{array}{rccc} f & : & G \times E & \to & E \\ & & (g,x) & \mapsto & g \cdot x \end{array}$$

telle que : pour tout $x \in E, 1 \cdot x = x$ et pour tout $(g, g', x) \in G^2 \times E, g \cdot (g' \cdot x) = (gg') \cdot x$.

Une telle application est également appelée action à gauche de G sur E.

Exemple 53. Le groupe G agit sur lui-même par translation à gauche :

$$(g,h) \in G \times G \mapsto g \cdot h = gh.$$

Définition 54. Soit G un groupe opérant sur un ensemble E. Pour tout $x \in E$, le sous-ensemble :

$$G \cdot x = \{g \cdot x | g \in G\}$$

de E est appelé orbite de x sous l'action de G.

On vérifie facilement que la relation $x \sim y$ si, et seulement si, il existe $g \in G$ tel que $y = g \cdot x$ est une relation d'équivalence sur E. La classe de x pour cette relation est l'orbite de x. Il en résulte que les orbites forment une partition de E.

Exemple 55. Pour l'action de $\mathcal{S}(E)$ sur E, il y a une seule orbite. En effet, pour tout $x \in E$, on a $\mathcal{S}(E) \cdot x = \{\sigma(x) | \sigma \in \mathcal{S}(E)\} = E$, car tout $y \in E$ s'écrit $y = \tau(x)$, où τ est la transposition $\tau = (x,y)$ si $y \neq x$, $\tau = id$ si $y = x$.

Définition 56. L'action de G sur E est dite transitive s'il existe une seule orbite (égale à E). Cela signifie que pour tout couple (x,y) d'éléments de E il existe $g \in G$ tel que $g \cdot x = y$. Elle est simplement transitive lorsque le g précédent est unique.

Définition 57. L'action est libre si pour tout couple (x,y) d'éléments de E il existe au plus un élément g de G tel que $g \cdot x = y$ (il en existe exactement un si x et y sont dans la même orbite et aucun sinon).

Définition 58. On dit que l'action de G sur E est fidèle si le morphisme de groupes :

$$\phi : g \in G \mapsto (\phi(g) : x \mapsto g \cdot x) \in \mathcal{S}(E).$$

est injectif, ce qui signifie que :

$$(g \in G) \text{ et } \forall x \in E, g \cdot x = x) \iff (g = 1)$$

Une action fidèle permet d'identifier G à un sous-groupe de $\mathcal{S}(E)$.

Théoreme 59 (Cayley). L'action de G sur lui-même par translation à gauche est fidèle et G est isomorphe à un sous-groupe de $\mathcal{S}(G)$.

Définition 60. Soit G un groupe opérant sur un ensemble non vide E. Pour tout $x \in E$, le sous-ensemble :

$$G_x = \{g \in G | g \cdot x = x\}$$

de G est le stabilisateur de x sous l'action de G.

On vérifie facilement que ces stabilisateurs G_x sont des sous-groupes de G (en général non distingués).

On présente maintenant un résultat liant les cardinaux de l'orbite et du stabilisateur d'un élément.

Théoreme 61. Soit $(G, \cdot)$ un groupe opérant sur un ensemble E. Pour tout $x \in E$ l'application :

$$\begin{array}{rccc} \phi_x & : & G/G_x & \to & G \cdot x \\ & & \bar{g} = gG_x & \mapsto & g \cdot x \end{array}$$

est bien définie et bijective. Dans le cas où G est fini, on a :

$$Card(G \cdot x) = [G : G_x] = \frac{Card(G)}{Card(G_x)}.$$

Du résultat précédent, et du fait que E soit partitionné en orbites, on déduit le résultat suivant.

Théoreme 62 (Equation aux classes). Soit $(G, \cdot)$ un groupe fini opérant sur un ensemble fini E. En notant $G_{x_1}, \ldots, G_{x_r}$ toutes les orbites deux à deux distinctes, on a :

$$Card(E) = \sum_{i=1}^{r} Card(G \cdot x_i) = \sum_{i=1}^{r} \frac{Card(G)}{Card(G_{x_i})}.$$

Exemple 63. Employons les résultats obtenus jusqu'à présent pour dénombrer les matrices diagonalisables sur un corps fini. On note $\mathbf{F}_q = \{\alpha_1, \ldots, \alpha_q\}$ un corps à $q = p^r$ éléments, p premier, $r \geq 0$. Notons $D_n(q)$ l'ensemble des matrices diagonalisables de $\mathcal{M}_n(q) = \mathcal{M}_n(\mathbf{F}_q)$. Alors, avec la convention $|GL_0(q)| = 1$, on a le résultat suivant :

$$|D_n(q)| = \sum_{\substack{m_1, \ldots, m_q \in \mathbf{N} \\ m_1 + \ldots + m_q = n}} \frac{|GL_n(q)|}{\left(\prod_{i=1}^{q} |GL_{m_i}(q)| \right)}$$

Démonstration. Le groupe $GL_n(q)$ agit par conjugaison sur $D_n(q)$. Commençons par décrire les orbites de cette action. Pour $M \in D_n(q)$, on a :

$$GL_n(q) \cdot M = \{PMP^{-1} | P \in GL_n(q)\}.$$

M est diagonalisable donc il existe $m = (m_1, \ldots, m_q) \in \mathbf{N}^q$ tel que $D_m \in GL_n(q) \cdot M$, avec :

$$D_m = \begin{pmatrix} \alpha_1 I_{m_1} & & 0 \\ & \ddots & \\ 0 & & \alpha_q I_{m_q} \end{pmatrix}.$$

De plus si $D_{m'} \in GL_n(q) \cdot D_m$, alors les polynômes caractéristiques de $D_{m'}$ et D_m sont égaux et : $\chi_{D_{m'}} = \chi_{D_m} = \prod_{i=1}^{q} (X - \alpha_i)^{m_i}$, et donc $m = m'$. Finalement, comme les orbites forment une partition de l'ensemble $D_n(q)$, on obtient :

$$D_n(q) = \bigsqcup_{m_1+\ldots+m_q=n} GL_n(q) \cdot D_m.$$

Il reste à trouver le cardinal des orbites. Pour cela on va utiliser la relation entre l'orbite et le stabilisateur d'un élément :

$$|GL_n(q) \cdot D_m| = \frac{|GL_n(q)}{|GL_n(q)_{D_m}|}.$$

Si $P \in GL_n(q)_{D_m}$ alors $PD_m = D_m P$, i.e. P est dans le commutant de D_m. Notons $E_\lambda(D_m)$ le sous-espace propre de D_m associé à la valeur propre λ. Soit $X \in E_\lambda(D_m)$. On a : $D_m PX = PD_m X = \lambda PX$ et donc $PX \in E_\lambda(D_m)$. Donc P laisse stable tous les sous espaces propre de D_m. Or $\mathbf{K}^n = \bigoplus_\lambda E_\lambda(D_m)$, donc :

$$P = \begin{pmatrix} P_1 & & 0 \\ & \ddots & \\ 0 & & P_q \end{pmatrix}$$

avec $P_i \in GL_{m_i}(q)$.

Réciproquement, si P est de cette forme alors on a bien $PD_m = D_m P$.

Finalement, pour chaque choix de P_i il y a $|GL_{m_i}(q)|$ possibilités, d'où $|GL_n(q)_{D_m}| = \prod_{i=1}^{q} |GL_{m_i}(q)|$. On en déduit le résultat voulu en passant aux cardinaux dans l'expression de $D_n(q)$

4.2 Problèmes de coloration

Dans cette partie nous allons dans un premier temps établir la formule de Burnside, que nous appliquerons ensuite au problème du nombre de coloriages du cube.

4.2.1 La formule de Burnside

La formule de Burnside permet de compter le nombre d'orbites distinctes en fonction des ensembles $fix(g) = \{x \in E | g \cdot x = x\}$ des éléments de E fixes par $g \in G$.

Théoreme 64 (Formule de Burnside). Soit G un groupe fini qui agit sur un ensemble fini E. Le nombre d'orbites de cette action est donnée par :

$$k = \frac{1}{|G|} \sum_{g \in G} |fix(g)|.$$

Démonstration. Notons $O_1, \ldots, O_k$ les k orbites de cette action. Pour obtenir la formule voulue il suffit de calculer le cardinal de $F = \{(g, x) \in G \times E | g \cdot x = x\}$ de deux façons :

$$card(F) = \sum_{g \in G} \sum_{x \in E} card(\{(g, x) | g \cdot x = x\}) = \sum_{g \in G} card(fix(g))$$

$$card(F) = \sum_{x \in E} |G_x| = \sum_{x \in E} \frac{|G|}{|G \cdot x|} = \sum_{i=1}^{k} \sum_{x \in O_i} \frac{|G|}{|G \cdot x|}$$

$$= |G| \sum_{i=1}^{k} \sum_{x \in O_i} \frac{1}{card(O_i} = |G| \sum_{i=1}^{k} 1 = k|G|$$

D'où le résultat en divisant par $|G|$.

Cette formule est particulièrement utile pour des dénombrements en géométrie puisqu'en faisant agir le groupe des isométries directes (i.e. des déplacements) d'une figure sur la figure elle-même, on peut facilement déterminer le cardinal de $fix(g)$, du moins en dimensions 2 et 3 car cela reste assez visuel. Une application typique de cette formule correspond au dénombrement de colliers de perles, qui ne sera pas présenté ici, mais dont un exemple est présent dans le livre [1]. Mais l'idée reste la même que celle présentée dans l'application qui suit.

4.2.2 Coloriages du cube

On dispose d'un cube C, représenté par un ensemble de huit sommets, et l'on souhaite colorer ses 6 faces en sachant que l'on dispose de k couleurs. On veut déterminer le nombre de façons différentes qu'il y a de colorier le cube. En remarquant que si deux colorations s'obtiennent via un déplacement du cube, alors elles vont correspondre à la même coloration, cela revient à déterminer le nombre d'orbites de l'action des déplacements du cube sur le cube lui-même. En notant $Is^+(C)$ les déplacements du cube, on admet le résultat suivant :

Proposition 65. $Is^+(C)$ est isomorphe à $\mathcal{S}_4$.

Pour chaque type de déplacement, on va préciser leur nombre, ainsi que le nombre de coloriages laissés fixes. Comme $\mathcal{S}_4 = 24$, il y a 24 déplacements du cube.

- L'identité Id laisse fixe tous les coloriages du cube, comme il y a k couleurs possibles pour chacune des 6 faces cela fait k^6 coloriages ;
- Il y a 6 rotations d'angle $\pm\frac{\pi}{2}$ autour des trois axes passant par les milieux de deux faces opposées. Chacune de ces rotations laisse fixe deux faces et ont chacune un 4-cycle. Un coloriage fixé par ce déplacement, doit garder la même couleur sur chacune des 4 faces du 4-cycle. On doit donc choisir 3 couleurs, cela fait donc k^3 coloriages possibles pour chaque rotation ;
- Il y a 3 rotations d'angle π autour des trois axes passant par les milieux de deux faces opposés. Chacune de ces rotations laisse fixe deux faces, et ont chacune deux 2-cycles. Un coloriage fixé par un tel déplacement doit avoir la même couleur sur les deux faces du 2-cycle. On doit donc choisir 4 couleurs, cela fait k^4 coloriages possibles ;
- Il y a 6 rotations d'angle π autour des six axes joignant les milieux de deux arêtes diagonalement opposées. Elles ont chacune trois 2-cycles. Un coloriage fixé par cette rotation est constitué de 3 couleurs (une pour chaque 2-cycle). Cela fait donc k^3 coloriages possibles ;
- Enfin, il y a les 8 rotations d'angle $\pm\frac{2\pi}{3}$ autour des quatre axes joignant deux sommets diagonelement opposés. Ces rotations ont chacune deux 3-cycles. Un coloriage fixé par cette rotation est constitué de 2 couleurs, ce qui nous fait un total de k^2 coloriages possibles.

En appliquant la formule de Burnside on obtient alors, en notant $C(k)$ le nombre de coloriages possibles avec k couleurs :

$$C(k) = \frac{1}{|\mathcal{S}_4|}(k^6 + 6k^3 + 3k^4 + 6k^3 + 8k^2) = \frac{k^2(k^4 + 3k^2 + 12k + 8)}{24}.$$

En particulier, si on veut colorier le cube avec $k = 3$ couleurs, on a $C(3) = 57$ manières de le colorier.

5 Questions posées lors de l'oral

5.1 Sur le développement

Le développement présenté était celui de la probabilité que deux nombres soient premiers entre eux.

— Comment peut-on interpréter le résultat obtenu en utilisant la fonction ζ de Riemann ? → En utilisant l'expression de ζ comme produit eulérien on a : $\zeta(s) = \prod_{i=1}^{\infty} \frac{1}{1-p_i^{-s}}$. D'où : $\frac{1}{\zeta(2)} = \frac{6}{\pi^2} = \prod_{i=1}^{\infty}(1 - p_i^{-2})$. On peut interpréter la quantité $(1 - p_i^{-2})$, comme la probabilité que le pgcd de deux nombres ne soit pas divisible par p_i. De ce fait, le produit infini exprime que le pgcd des deux nombres n'est divisible par aucun nombre premier, et donc qu'ils sont premiers entre eux.

— A-t-on tendance à tirer des nombres premiers entre eux ? → Oui, car $\frac{6}{\pi^2} > 0.5$.

— Questions sur les étapes de calcul dans l'étape 1. → Des détails ont été apportés dans la démonstration en section 2.2.1.

— Démontrer que la fonction de Möbius est inversible. → La démonstration est rédigée en section 2.2.1.

5.2 Sur le plan

— Déterminer une formule pour le nombre de surjections d'un ensemble à p éléments dans un ensemble à n éléments. → La démonstration a été faite en section 1 en exemple 12.

— Déterminer le nombre de mots primitifs sur un alphabet à 8 lettres. → C'est un cas particulier de l'application 44 sur les mots primitifs, réalisée en section 2.2.1.

— Combien y a-t-il de manières de colorier un collier de 5 perles avec 3 couleurs différentes ? → On fait agir le groupe diédral sur les sommets d'un pentagone régulier, puis on applique la formule de Burnside. Le groupe diédral est engendré par la rotation d'angle $\frac{2\pi}{5}$ et la symétrie d'axe (OS) où O est le centre de la figure, et S un sommet du pentagone. Le groupe diédral contient 10 éléments : l'identité (qui laisse fixe 3^5 coloriages), 4 rotations (qui laissent fixe 3 coloriages), et 5 réflexions (qui laissent fixe une perle, et deux 2-cycles, donc 3^3 coloriages). La formule de Burnside nous dit alors qu'il y a : $\frac{1}{10}(3^5 + 4 \cdot 3 + 5 \cdot 3^3) = 39$ colliers de perles possibles.

Références

[1] François Combes. *Algèbre et géométrie*, volume 51. Bréal, 1998.

[2] Arthur Engel and Jean-Christophe Trad Novelli. *Solutions d'expert. V. 1.* Cassini, Pole Paris, 2007 Collection : Enseignement des mathématiques Format .

[3] Philippe Flajolet and Robert Sedgewick. *Analytic combinatorics*. cambridge University press, 2009.

[4] Dominique Foata, Aimé Fuchs, and Jacques Franchi. *Calcul des probabilités-3e édition : Cours, exercices et problèmes corrigés*. Dunod, 2012.

[5] Daniel Guin and Thomas Hausberger. *Algebre*, volume 1. EDP sciences, 2012.

[6] Jean-Etienne Rombaldi. *Mathématiques pour l'Agrégation : Algèbre & géométrie*. De Boeck Superieur, 2017.