

République Française.
Ministère de l'Enseignement supérieur, de la Recherche et de l'Innovation.
Université Gustave Eiffel.



Institut Gaspard Monge

Mémoire de master 1 en informatique

Thème

Lemme de Burnside et théorie de Pólya
--

Réalisé par : Hadjer Djerroumi, Elise Ruan & Alexis Le Gal

Soutenu le 1 septembre 2020, devant le jury composé de :

Table des matières

1	Groupes, groupe symétrique et groupe de symétrie	2
1.1	Généralités dans la théorie des groupes	2
1.2	Groupe symétrique	6
2	Actions de groupe	10
2.1	Définition de l'action de groupe	10
2.2	Orbites	10
2.2.1	Relations d'équivalence	10
2.2.2	Classes d'équivalence	11
2.2.3	Orbites	11
2.3	Exemples : Coloration de colliers	12
2.3.1	Application 1 : 3 perles et 2 couleurs	12
2.3.2	Application 2 : 5 perles et 2 couleurs	14
2.3.3	Application 3 : 5 perles et 3 couleurs	15
2.4	Stabilisateur et fixateur	17
2.5	Action de groupe sur un ensemble de fonctions	19
2.5.1	Groupe produit	20
2.5.2	Action du groupe produit	20
3	Lemme de Burnside et théorie de Pólya	22
3.1	Fonctions de poids	22
3.2	Lemme de Burnside	23
3.3	Exemples : Coloration de collier	24
3.3.1	Application 1 : 3 perles et 2 couleurs	24
3.3.2	Application 2 : 5 perles et 2 couleurs	25
3.3.3	Application 3 : 5 perles et 3 couleurs	25
3.4	Généralisation du lemme de Burnside : Formule de De Bruijn . . .	26
3.5	Polynômes indicateur de cycles	27
3.5.1	Indicateur de cycles d'une permutation	27
3.5.2	Indicateur de cycles d'un groupe de permutations	27
3.5.3	Calcul de l'indicateur de cycle de \mathfrak{S}_3	27
3.5.4	Calcul de l'indicateur de cycle de C_n	28
3.6	Théorème de dénombrement de Pólya	32
3.6.1	Poids d'une application	32
3.6.2	Théorème de Pólya	33

3.7	Exemples : Coloration de colliers	37
3.7.1	Application 1 : 3 perles et 2 couleurs	38
3.7.2	Application 2 : 5 perles et 2 couleurs	38
3.7.3	Application 3 : 5 perles et 3 couleurs	38
3.8	Théorème de Pólya appliqué aux problèmes de coloration : Version pondérée	39
3.8.1	Coloration de collier	40
4	Classes de conjugaison et produit semi-direct	42
4.1	Classes de conjugaison	42
4.2	Sous-groupe normal	43
4.2.1	Normalité dans le groupe diedral	44
4.3	Produit semi-direct	45
5	Applications	47
5.1	Jetons transparents hexagonaux	47
5.2	Coloration des solides de Platon	50
5.2.1	Dualité entre solides de Platon	50
5.2.2	Le tétraèdre	50
5.2.3	Le cube et l'octaèdre	53
5.2.4	Le dodécaèdre et l'icosaèdre	56
5.3	Sudoku	62
5.3.1	Sudoku classique	62
5.3.2	Mini-Sudoku	62
5.3.3	Définition formelle du Sudoku $n^2 \times n^2$	63
5.3.4	Groupe de symétrie du Sudoku	64
6	Programmation	66
6.1	Langage et installation	66
6.2	Descriptions des classes	66
6.3	Diagramme de classe	67
6.4	Exécution et utilisation	68
6.4.1	Exécution	68
6.4.2	Utilisation de CyclicGroup, DiedralGroup, CubicGroup et OctahedralGroup	68
6.4.3	Utilisation de SudokuGroup	69
6.5	Complexité dans \mathfrak{S}_n	69
A	Triangle de Pascal	72
B	Suites des solides de Platon	73
B.1	Tétraèdre	73
B.2	Cube et octaèdre	74

B.3	Dodécaèdre et icosaèdre	75
-----	-----------------------------------	----

Table des figures

1.1	Le carré et ses axes de rotations/réflexions.	8
2.1	Toutes les colorations du collier de 3 perles avec 2 couleurs.	12
2.2	Orbite de la coloration brr	13
2.3	Orbite de la coloration bbr	13
2.4	Partition des colorations en orbites.	14
2.5	Les 8 colorations réellement différentes d'un collier de 5 perles avec 2 couleurs	15
4.1	L'opération $r \circ s \circ r^{-1}$ sur une partie d'un polygone à n sommets. .	45
4.2	La réflexion s sur la même partie du polygone précédent.	45
5.1	4 colorations équivalentes d'un hexagone.	48
5.2	4 colorations non-équivalentes d'un hexagone.	48
5.3	Illustration de deux positions d'un tétraèdre.	50
5.4	Les cinq colorations différentes du tétraèdre avec 2 couleurs.	52
5.5	Les 15 colorations différentes du tétraèdre avec 3 couleurs.	53
5.6	Deux types d'axes de rotation du cube.	54
5.7	Les dix colorations non-équivalentes du cube avec deux couleurs. .	56
5.8	Deux positions différentes d'un dodécaèdre régulier.	57
5.9	Le dual du dodécaèdre de la figure 5.8.	57
5.10	Trois cycles de sommets de longueur 3 d'un dodécaèdre.	59
5.11	Axe de rotation passant par les milieux de deux arêtes opposées. .	59
6.1	Diagramme de classe.	67

Liste des tableaux

1.1	Table de multiplication dans $\mathbb{Z}/5\mathbb{Z}$	4
1.2	Table de multiplication dans $\mathbb{Z}/4\mathbb{Z}$	4
1.3	Table de multiplication modulo 5 de éléments 1 et 4.	5
1.4	Table de multiplication modulo 5 de éléments 1 et 2.	5
1.5	Les opérations laissant le carré inchangé.	8
2.1	Nombre de colorations/orbites d'un collier de 5 perles avec au plus 2 couleurs	16
2.2	Cinq orbites des colorations utilisant exactement 3 couleurs.	17
3.1	$c_k(\sigma)$ pour $k \in \{1, 2, \dots, 8\}$ de la permutation $\sigma = 37862451$	27
3.2	Valeurs de $\phi(n)$ pour $n \leq 8$	30
4.1	Les éléments de D_4	46
5.1	Les douze éléments de D_6	48
5.2	Monôme et $ \text{fixateur} $ par classe de conjugaison de T	51
5.3	Parités des éléments du groupe tétraédral.	51
5.4	Monôme et $ \text{fixateur} $ par classe de conjugaison de $Cube$	55
5.5	Monôme et $ \text{fixateur} $ par classe de conjugaison de $Octa$	55
5.6	paires de faces opposées du dodécaèdre de la figure 5.8.	57
5.7	Monôme et $ \text{fixateur} $ par classe de conjugaison de $Dode$ et Ico	60
5.8	Illustration d'une pile, une bande et des neuf blocks sur un Sudoku classique.	62
5.9	Un mini-Sudoku.	63
5.10	Le sudoku trivial.	63
5.11	Les éléments générateurs du groupe de symétrie du Sudoku $n^2 \times n^2$	64
6.1	Les six groupes implémentés.	66
6.2	Temps de construction de \mathfrak{S}_n en Cython.	69
A.1	15 premières lignes du triangle de Pascal.	72
B.1	48 premiers termes de la suite du tétraèdre.	73
B.2	30 premiers termes des suites du cube et de l'octaèdre.	74
B.3	30 premiers termes de la suite du dodécaèdre et de l'icosaèdre.	75

Introduction

L'histoire des problèmes de dénombrements remonte à l'antiquité grecque, quand Hipparque (190 – 120 av J.C) comptait le nombre de propositions composées à partir de dix élémentaires. Les nombres de Schröder-Hipparque font référence à son nom car il avait trouvé le dixième terme qui est 103049.

Aujourd'hui, les problèmes de dénombrements sont tellement nombreux et constituent tout un domaine d'étude appelé : La combinatoire énumérative.

Tout le monde sait qu'il existe des objets identiques et des objets qui se ressemblent. Imaginons qu'au lieu de compter tous les objets d'un ensemble, on compte seulement ceux qui ne se ressemblent pas. L'idée est de généraliser l'égalité à la ressemblance. Dans la théorie des groupes, on utilise le terme *équivalence* pour désigner la ressemblance.

Les objets équivalents sont donc considérés comme étant identiques, et ensemble, forment ce qu'on appelle *classe d'équivalence*.

Notre étude consiste à dénombrer les objets qui ne se ressemblent pas. L'idée est de regrouper tous les objets en classes d'équivalences et de compter le nombre de classes.

Le document est composé de cinq chapitres : le [chapitre 1](#) est un rappel des éléments de la théorie des groupes : groupes, groupes symétriques, groupes de symétrie. Le [chapitre 2](#) introduit l'action de groupe fini sur un ensemble fini : c'est l'opération qui partitionne l'ensemble en classes d'équivalence. Dans le [chapitre 3](#), nous présenterons et prouverons le lemme de Burnside qui représente en lui-même un théorème, nous prouverons également le théorème de Polya : ces deux théorèmes résolvent le problème de comptage de classes d'équivalence. Dans le [chapitre 4](#), nous verrons des outils facilitant l'application des deux théorèmes. Finalement, le [chapitre 5](#) est dédié aux applications des deux théorèmes pour faire des dénombrements d'objets non équivalents.

Tout au long du document, des exemples de calcul et des dessins illustratifs seront donnés.

1 Groupes, groupe symétrique et groupe de symétrie

1.1 Généralités dans la théorie des groupes

Dans cette section, des rappels, des définitions et des notations relatifs aux groupes sont données avec des exemples et des contre exemples facilitant la compréhension.

Définition 1.1 (Loi de composition interne). Une loi de composition interne sur un ensemble E , notée $*$ est une application :

$$\begin{aligned} * : E \times E &\longrightarrow E \\ (x, y) &\longmapsto x * y. \end{aligned}$$

Définition 1.2 (Magma). Un magma est la donnée d'un ensemble E muni d'une loi de composition interne $*$. Il est noté $(E, *)$.

Exemple 1.1. L'ensemble des entiers naturels \mathbb{N} muni de l'addition usuelle est un magma. En effet, l'addition de deux entiers naturels est un entier naturel. De même, $(\mathbb{Z}, +)$ et $(\mathbb{R}, +)$ sont des magmas.

Contre exemple 1.1. Soit $E = \{0, 1\}$. $(E, +)$ n'est pas un magma car l'addition n'est pas interne, en effet $1 + 1 = 2 \notin E$.

Définition 1.3 (Associativité). Étant donné un magma $(E, *)$. La loi de composition interne $*$ est dite associative ou $(E, *)$ est dit associatif si et seulement si :

$$\forall x, y, z \in E, (x * y) * z = x * (y * z). \quad (1.1)$$

Exemple 1.2. Les magmas $(\mathbb{N}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$ sont associatifs.

La multiplication dans $\mathbb{Z}/4\mathbb{Z}$ est associative, nous avons par exemple :

$$\begin{aligned} 1 * (2 * 3) &= 1 * 2 = 2 \\ (1 * 2) * 3 &= 2 * 3 = 2 \end{aligned} \quad (1.2)$$

Ceci est vrai quels que soient $x, y, z \in \mathbb{Z}/4\mathbb{Z}$.

Contre exemple 1.2. La soustraction dans \mathbb{Z} n'est pas associative. En effet :

$$\begin{aligned} (1 - 2) - 3 &= -1 - 3 = -4 \\ 1 - (2 - 3) &= 1 - (-1) = 2 \end{aligned} \quad (1.3)$$

Définition 1.4 (Élément neutre). Soit un magma $(E, *)$. Un élément e dans E vérifiant pour tout x dans E : $x * e = e * x = x$ est appelé élément neutre de $*$.

Exemple 1.3. Le magma $(\mathbb{N}, +)$ possède l'élément neutre 0. En effet : pour tout n dans \mathbb{N} , $n + 0 = 0 + n = n$. De même pour $(\mathbb{Z}, +)$.

Le magma $(\mathbb{R}^*, *)$ possède l'élément neutre 1. En effet : pour tout x dans \mathbb{R}^* , $x * 1 = 1 * x = x$.

Contre exemple 1.3. Le magma $(\mathbb{N}^*, +)$ n'a pas d'élément neutre.

Définition 1.5 (Élément symétrique). Étant donné un magma $(E, *)$ dont l'élément neutre est e .

On dit que $x \in E$ possède un élément symétrique, ou que x est inversible dans $(E, *)$ si et seulement s'il existe $y \in E$ tel que $x * y = y * x = e$. y est appelé l'inverse de x et est noté x^{-1} .

Exemple 1.4. Chaque élément x du magma $(\mathbb{R}^*, *)$ possède un élément symétrique égal à $\frac{1}{x}$. En effet : $x * \frac{1}{x} = \frac{1}{x} * x = 1$.

Chaque élément du magma $(\mathbb{Z}, +)$ possède un élément symétrique égal à $-n$. En effet : $n + (-n) = (-n) + n = 0$.

Contre exemple 1.4. Les éléments dans $(\mathbb{N}, +)$ et dans $(\mathbb{Z}, *)$ ne sont pas inversibles.

Dans $(\mathbb{R}, *)$, le seul élément non inversible est 0. En effet, il n'existe aucun élément $x \in \mathbb{R}$ pour lequel $x * 0 = 0 * x = 1$.

Définition 1.6 (Commutativité). Soit un magma $(E, *)$. Le magma est dit commutatif si et seulement si $\forall x, y \in E, x * y = y * x$.

Exemple 1.5. Les magmas $(\mathbb{N}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Z}, *)$, $(\mathbb{R}, *)$ sont commutatifs.

Contre exemple 1.5. Les magmas $(\mathbb{Z}, -)$ et $(\mathbb{R}, /)$ ne sont pas commutatifs. En effet $3 - 2 \neq 2 - 3$ et $2/3 \neq 3/2$.

Définition 1.7 (Groupe). Un magma associatif, possédant un élément neutre et dont chaque élément est inversible est appelé un groupe.

Exemple 1.6. Les magmas $(\mathbb{Z}, +)$, $(\mathbb{Z}/n\mathbb{Z}, +)$ pour $n \in \mathbb{N}^*$, $(\mathbb{R}, +)$ et $(\mathbb{R}^*, *)$ sont des groupes.

Exemple 1.7. L'ensemble $\{1, 2, 3, 4\}$ muni de la multiplication modulo 5 est un groupe noté $(\mathbb{Z}/5\mathbb{Z}, *)$. En effet, la table de multiplication modulo 5 de $\{1, 2, 3, 4\}$ est la suivante :

*	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

TABLE 1.1 – Table de multiplication dans $\mathbb{Z}/5\mathbb{Z}$.

Nous pouvons voir que :

- Tous les éléments sont dans $\{1, 2, 3, 4\}$, donc la loi est interne.
- La multiplication par 1 ne change pas l'élément donc 1 est l'élément neutre.
- L'élément neutre se trouve sur toutes les lignes donc tous les éléments sont inversibles.

De plus la multiplication est associative.

Contre exemple 1.6. La table de multiplication modulo 4 est :

*	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

TABLE 1.2 – Table de multiplication dans $\mathbb{Z}/4\mathbb{Z}$.

L'ensemble $\{0, 1, 2, 3\}$ muni de la multiplication modulo 4 n'est pas un groupe. En effet, d'après la table 1.2, on remarque que l'élément neutre 1 ne figure pas sur les lignes 0 et 2, donc les éléments 0 et 2 ne sont pas inversibles.

Remarque 1.1. L'ensemble $\{0, 1, 2, \dots, n-1\}$ muni de la multiplication modulo n n'est jamais un groupe car 0 n'est pas inversible.

Remarque 1.2. L'ensemble $\{1, 2, \dots, n-1\}$ muni de la multiplication modulo n noté $(\mathbb{Z}/n\mathbb{Z}, *)$ ne peut être un groupe que si n est premier. Car sinon, il existerait deux éléments $a, b \in \{1, 2, \dots, n-1\}$ vérifiant $a * b = 0$ or, 0 n'est pas dans $\{1, 2, \dots, n-1\}$.

Définition 1.8 ((Ordre d'un groupe)). L'ordre d'un groupe G est le cardinal de son ensemble. Il est noté $|G|$.

Exemple 1.8. Soit p un nombre premier et $n \in \mathbb{N}^*$.

L'ordre du groupe $(\mathbb{Z}/p\mathbb{Z}, *)$ est $p-1$.

L'ordre du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ est n .

Définition 1.9 (Sous-groupe). Soit $G = (E, *)$ un groupe. $H \subseteq E$ est un sous-groupe de G si et seulement si :

- H est stable par la loi $*$: pour tout $x, y \in H, x * y \in H$.
- L'élément neutre de G appartient à H .
- L'inverse de tout élément de H est dans H .

On note $H \leq G$.

Exemple 1.9. Les ensembles $\{1\}$, $\{1, 4\}$ et $\{1, 2, 3, 4\}$ sont les sous-groupes de $(\mathbb{Z}/5\mathbb{Z}, *)$. $\{1\}$ et $\{1, 2, 3, 4\}$ sont des sous-groupes triviaux. La table de multiplication de l'ensemble $\{1, 4\}$ est :

*	1	4
1	1	4
4	4	1

TABLE 1.3 – Table de multiplication de modulo 5 de éléments 1 et 4.

On peut voir facilement qu'il s'agit d'un groupe.

Contre exemple 1.7. L'ensemble $\{1, 2\}$ n'est pas un sous-groupe de $(\mathbb{Z}/5\mathbb{Z}, *)$. En effet, la table nous montre qu'il n'est pas stable par la multiplication.

*	1	2
1	1	2
2	2	4

TABLE 1.4 – Table de multiplication de modulo 5 de éléments 1 et 2.

Remarque 1.3. Tout groupe possède deux sous-groupes triviaux : le groupe réduit à l'élément neutre et lui même.

Définition 1.10 (Groupe abélien). Un groupe abélien est un groupe commutatif.

Exemple 1.10. Tous les groupes vus précédemment sont des groupes commutatifs, à savoir $(\mathbb{Z}, +)$, $(\mathbb{Z}/n\mathbb{Z}, +)$ pour $n \in \mathbb{N}^*$, $(\mathbb{R}, +)$, $(\mathbb{R}^*, *)$ et $(\mathbb{Z}/p\mathbb{Z}, *)$ pour p premier.

Contre exemple 1.8. L'ensemble des matrices carrées d'ordre n ayant un déterminant non nul, muni de la multiplication des matrices est un groupe non-commutatif. En effet :

- La loi est interne car la multiplication de deux matrices carrées d'ordre n est une matrice carrée d'ordre n .
- La multiplication des matrices est associative.
- L'élément neutre est la matrice identité d'ordre n .
- Chaque matrice est inversible car son déterminant est non nul.
- La multiplication des matrices n'est pas commutative.

Définition 1.11 (Anneau). Un anneau noté $(A, +, \cdot)$ est la donnée d'un ensemble A muni de deux lois de composition internes $+$ et \cdot telles que :

- $(A, +)$ est un groupe abélien dont l'élément neutre est souvent noté 0 ,
- \cdot possède un élément neutre souvent noté 1 ,
- \cdot est associative,
- \cdot est distributive par rapport à $+$, c'est à dire pour tous a, b, c dans A on a :

$$\begin{aligned} a * (b + c) &= a * b + a * c \\ (b + c) * a &= b * a + c * a \end{aligned} \tag{1.4}$$

Si la multiplication est commutative, on dit que A est un anneau commutatif.

Exemple 1.11. $(\mathbb{Z}, +, \cdot)$ et $(\mathbb{R}, +, \cdot)$ sont des anneaux commutatifs.

Exemple 1.12. Si A est un anneau commutatif, alors l'ensemble des polynômes en $n \geq 1$ indéterminées x_1, \dots, x_n à coefficients dans A noté $A[x_1, \dots, x_n]$ est un anneau commutatif.

1.2 Groupe symétrique

Soit $n \geq 1$ et soit $\mathcal{N} = \{1, \dots, n\}$.

Définition 1.12 (Permutation). Une permutation σ de l'ensemble \mathcal{N} est une bijection de \mathcal{N} dans lui-même. Elle est le plus souvent notée $\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ x_1 & x_2 & \dots & x_n \end{pmatrix}$ ou tout simplement $\sigma = x_1 x_2 \dots x_n$. On lit $\sigma(k) = x_k$ pour tout $k \in \{1, \dots, n\}$. Dans ce document, nous utiliserons la seconde notation¹, et nous confondrons $\sigma(k)$, $\sigma \cdot k$ et σk .

Exemple 1.13. Si $\mathcal{N} = \{1, 2, 3, 4\}$ alors $\sigma = 2341$ est une permutation de \mathcal{N} . Celle-ci est définie par $\sigma(1) = 2$, $\sigma(2) = 3$, $\sigma(3) = 4$ et $\sigma(4) = 1$.

Définition 1.13 (Cycle). Un cycle de longueur k ou un k -cycle noté $(x_{i_1}, x_{i_2}, \dots, x_{i_k})$ est une permutation γ de l'ensemble $\{x_{i_1}, x_{i_2}, \dots, x_{i_k}\}$ telle que $\gamma(x_{i_j}) = x_{i_{j+1}}$ pour tout $j = 1, \dots, k-1$ et $\gamma(x_{i_k}) = x_{i_1}$.

Un 1-cycle est dit point fixe. Un 2-cycle est dit transposition.

Théorème 1.1. [4] Toute permutation σ se décompose de façon unique en un produit de cycles à supports disjoints, à l'ordre près des facteurs.

Exemple 1.14. Soit la permutation $\sigma = 37862451$

$$\left\{ \begin{array}{l} \sigma(1) = 3 \\ \sigma(3) = 8 \\ \sigma(8) = 1 \end{array} \right\} \implies \gamma_1 = (1, 3, 8) \quad \left\{ \begin{array}{l} \sigma(2) = 7 \\ \sigma(7) = 5 \\ \sigma(5) = 2 \end{array} \right\} \implies \gamma_2 = (2, 7, 5) \quad \left\{ \begin{array}{l} \sigma(4) = 6 \\ \sigma(6) = 4 \end{array} \right\} \implies \gamma_3 = (4, 6)$$

1. Une permutation pourrait aussi être notée $\sigma = (x_1, x_2, \dots, x_n)$. Mais dans ce document, on représentera les cycles (voir définition du cycle 1.13), par des tuples, pour ne pas confondre cycle et permutation, la permutation (x_1, x_2, \dots, x_n) sera notée $x_1 x_2 \dots x_n$.

Donc $\sigma = (1, 3, 8) \cdot (2, 7, 5) \cdot (4, 6)$. On dit que σ possède deux 3-cycles, une transposition, et aucun point fixe.

Définition 1.14 (Parité). [4] La parité d'une permutation σ est la parité du nombre de cycles de longueur paire dans sa décomposition en produit de cycles.

Exemple 1.15. D'après l'exemple 1.14, la décomposition de la permutation $\sigma = 37862451$ est $\sigma = (1, 3, 8) \cdot (2, 7, 5) \cdot (4, 6)$. Il existe un seul cycle de longueur paire donc σ est impaire.

Définition 1.15 (Type). Le type d'une permutation $\sigma \in \mathfrak{S}_n$ se décomposant en k_1 points fixes, k_2 transpositions, ..., k_n cycles de longueur n est la partition de n ($1^{k_1} 2^{k_2} 3^{k_3} \dots n^{k_n}$).

Exemple 1.16. Dans l'exemple précédent, comme $\sigma = (1, 3, 8) \cdot (2, 7, 5) \cdot (4, 6)$, alors son type est $(1^0 2^1 3^2)$. Il se note plus légèrement par $(2^1 3^2)$. Nous avons bien $8 = 2 + 3 + 3$.

Théorème 1.2 (Groupe symétrique). [4] L'ensemble de toutes les permutations de \mathcal{N} , noté \mathfrak{S}_n , muni de la loi de composition des applications de \mathcal{N} dans \mathcal{N} est un groupe, appelé groupe symétrique de \mathcal{N} . Il est d'ordre $n!$.

Démonstration. **Loi interne :** Appliquer les permutations $\sigma \in \mathfrak{S}_n$ puis $\gamma \in \mathfrak{S}_n$ aux éléments de \mathcal{N} initialement dans l'ordre, revient à changer leur ordre deux fois. Le résultat est un nouvel ordre qui peut être obtenu par une permutation $\delta \in \mathfrak{S}_n$, celle-ci est la composition $\sigma \circ \gamma$ donc la composition est interne.

Élément neutre : L'élément neutre est la permutation identité $12 \dots n$ qui n'a aucun effet sur l'ordre des éléments.

Élément symétrique : L'inverse d'une permutation de \mathcal{N} est une permutation de \mathcal{N} car l'inverse d'une bijection $\mathcal{N} \longrightarrow \mathcal{N}$ est une bijection $\mathcal{N} \longrightarrow \mathcal{N}$.

Associativité : La loi de composition des applications est associative par définition. En effet, si σ, γ, δ sont trois permutations de \mathcal{N} et si $x \in \mathcal{N}$ alors,

$$[\sigma \circ (\gamma \circ \delta)](x) = \sigma((\gamma \circ \delta)(x)) = \sigma[\gamma(\delta(x))] = (\sigma \circ \gamma)(\delta(x)) = [(\sigma \circ \gamma) \circ \delta](x).$$

L'ordre de \mathfrak{S}_n : Nous rappelons que le nombre d'injections d'un ensemble \mathcal{E} dans un ensemble \mathcal{F} avec $|\mathcal{E}| = p, |\mathcal{F}| = n \geq p$ est le nombre $A_n^p = \frac{n!}{(n-p)!}$.

Le nombre de bijections de \mathcal{N} dans lui même est exactement le nombre d'injections de \mathcal{N} dans lui même. Donc $|\mathfrak{S}_n| = A_n^n = n!$. \square

Définition 1.16 (Groupe de permutations). Un sous-groupe du groupe symétrique \mathfrak{S}_n est appelé groupe de permutations. Son degré est n qui est la taille de ses permutations.

Définition 1.17 (Groupe alterné). Le groupe alterné noté A_n est le sous-groupe de \mathfrak{S}_n formé des permutations paires.

Théorème 1.3. *L'ensemble des isométries d'un objet géométrique régulier laissant l'objet invariant, muni de la loi de composition des applications est un groupe, appelé groupe de symétrie de l'objet.*

Propriété 1.1. *Le groupe de symétrie d'un objet ayant n éléments identiques (un élément peut être un sommet, une arête, une diagonale, une facette ...) peut être compris comme un sous-groupe du groupe symétrique \mathfrak{S}_n .*

Exemple : Groupe des isométries du carré

Soit Δ l'axe normal au plan du carré et passant par le centre du carré, et soient D_1, D_2, D_3 et D_4 les axes de réflexions du carré montrés sur la figure suivante (Figure 1.1) :

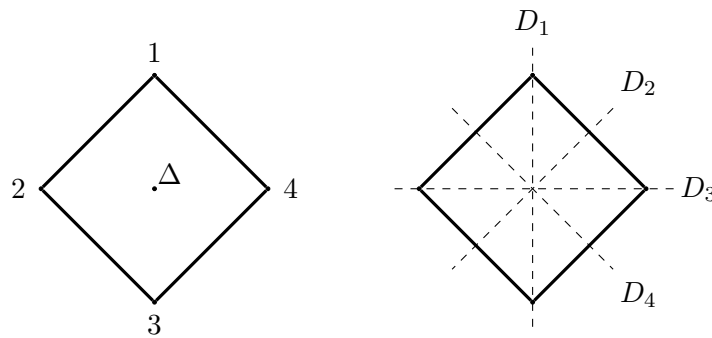


FIGURE 1.1 – Le carré et ses axes de rotations/réflexions.

Le groupe des isométries du carré, ou le groupe de symétrie du carré contient 8 éléments : l'identité, les 3 rotations d'axe Δ et d'angles $\pi/2$, π , $3\pi/2$, et les 4 réflexions d'axes D_1, D_2, D_3 et D_4 .

Soient r la rotation d'angle $\pi/2$, et s est la réflexion d'axe D_1 . Comme les axes D_2, D_3 et D_4 sont obtenus à partir de D_1 par les trois rotations, alors les réflexions d'axes D_2, D_3 et D_4 sont les composées de s et d'une rotation, soient $s \circ r$, $s \circ r^2$ et $s \circ r^3$.

On peut exprimer ces opérations par des permutations de sommets 1, 2, 3, et 4. La table suivante (Table 4.1) donne toutes les permutations laissant le carré globalement inchangé ainsi que les opérations correspondantes :

Transformation	id	r	r^2	r^3	s	$s \circ r$	$s \circ r^2$	$s \circ r^3$
Permutation	1234	2341	3412	4123	1432	4321	3214	2143

TABLE 1.5 – Les opérations laissant le carré inchangé.

Comme les éléments du groupe sont les composés de r et s . On dit que le groupe est engendré par ces deux éléments.

Ce groupe est appelé le groupe diedral d'ordre 8 noté D_4 . Plus généralement, le

groupe diedral d'ordre $2n$ noté D_n est le groupe de symétrie du polygone régulier à n sommets.

2 Actions de groupe

L'action de groupe est une notion fondamentale dans la théorie des groupes. Nous la présenterons dans ce chapitre et nous l'utiliserons dans les prochains. Nous commencerons par présenter la notion d'action de groupe en toute généralité, puis nous particulariserons au cas d'un ensemble de fonctions.

Tout au long de ce chapitre, (G, \cdot) désignera un groupe fini dont l'élément neutre sera noté e et \mathcal{X} désignera un ensemble fini.

2.1 Définition de l'action de groupe

L'action du groupe G sur \mathcal{X} est une loi de composition externe :

$$\begin{aligned} G \times \mathcal{X} &\longrightarrow \mathcal{X} \\ (g, x) &\longmapsto g \cdot x \end{aligned}$$

vérifiant :

- pour tout $x \in \mathcal{X} : e \cdot x = x$
- pour tout $x \in \mathcal{X}$, et pour tout $g_1, g_2 \in G, g_1 \cdot (g_2 \cdot x) = (g_1 \cdot g_2) \cdot x$

On dit que le groupe G agit ou opère sur l'ensemble \mathcal{X} .

Parmi les exemples classiques on cite :

- Chaque groupe opère sur lui même par translation à gauche $(g_1, g_2) \longmapsto g_1 \cdot g_2$.
- Chaque groupe opère sur lui même par conjugaison $(g_1, g_2) \longmapsto g_1 \cdot g_2 \cdot g_1^{-1}$.
- Le groupe symétrique \mathfrak{S}_n des permutations de $\mathcal{N} = \{1, 2, \dots, n\}$ opère naturellement sur \mathcal{N} par $(\sigma, n) \longmapsto \sigma(n)$.

2.2 Orbites

Commençons par faire un bref rappel de ce qui est une classe d'équivalence avant de parler de la notion d'orbites.

2.2.1 Relations d'équivalence

Une relation d'équivalence sur \mathcal{X} notée \sim est une relation binaire vérifiant pour tous x, y, z dans \mathcal{X} :

- *Reflexivité* : $x \sim x$.

- Symétrie : si $x \sim y$ alors $y \sim x$.
- Transitivité : si $x \sim y$ et $y \sim z$ alors $x \sim z$.

2.2.2 Classes d'équivalence

Définition 2.1 (Classe d'équivalence). Soit \sim une relation d'équivalence sur \mathcal{X} . La classe d'équivalence de $x \in \mathcal{X}$ notée \dot{x} est l'ensemble $\dot{x} = \{y \in \mathcal{X} : x \sim y\}$. On dit que x est le représentant de la classe \dot{x} .

Propriété 2.1. L'ensemble des classes d'équivalence est une partition de \mathcal{X} .

Démonstration. Par réflexivité, un élément $z \in \mathcal{X}$ appartient à \dot{z} donc il appartient à au moins une classe. Il reste à prouver que z appartient à au plus une classe. Soient $x, y \in \mathcal{X}$ tels que $\dot{x} \neq \dot{y}$ et supposons par absurde que $z \in \dot{x}$ et $z \in \dot{y}$. Alors :

$$\begin{aligned}
 z \in \dot{x} \text{ et } z \in \dot{y} &\implies z \sim x \text{ et } z \sim y \\
 &\implies x \sim z \text{ et } z \sim y \quad (\text{par symétrie}) \\
 &\implies x \sim y \quad (\text{par transitivité}) \\
 &\implies \dot{x} = \dot{y} \quad (\text{absurde})
 \end{aligned}$$

□

Notation 2.1. L'ensemble des classes d'équivalence se note \mathcal{X}/\sim .

2.2.3 Orbites

Définition 2.2 (Orbite). L'orbite d'un élément $x \in \mathcal{X}$ notée \mathcal{O}_x est l'ensemble

$$\mathcal{O}_x = \{g \cdot x, g \in G\}.$$

Par définition de l'orbite, deux éléments $x, y \in \mathcal{X}$ sont dans la même orbite c'est à dire $\mathcal{O}_x = \mathcal{O}_y$, si et seulement s'il existe $g \in G$ tel que $y = g \cdot x$.

Propriété 2.2. Soit la relation \mathcal{R} définie par :

$$x\mathcal{R}y \iff x, y \in \mathcal{O}_x \iff \exists g \in G, y = g \cdot x. \quad (2.1)$$

Alors l'orbite \mathcal{O}_x est une classe d'équivalence.

Démonstration. Il suffit de prouver que \mathcal{R} est une relation d'équivalence.

- \mathcal{R} est réflexive car $e \cdot x = x$.
- \mathcal{R} est symétrique. En effet, supposons $x\mathcal{R}y$ c'est à dire il existe $g \in G : y = g \cdot x$. En multipliant à gauche par g^{-1} on a $x = g^{-1} \cdot y$ et comme $g^{-1} \in G$ alors $y\mathcal{R}x$.
- \mathcal{R} est transitive. En effet, supposons $x\mathcal{R}y, y\mathcal{R}z$ c'est à dire il existe $g_1, g_2 \in G$:

$$\begin{cases} y = g_1 \cdot x & (1) \\ z = g_2 \cdot y & (2) \end{cases}$$

En remplaçant (1) dans (2) on trouve : $z = g_2 \cdot (g_1 \cdot x)$
et comme il s'agit d'une action de groupe alors $z = (g_2 \cdot g_1) \cdot x$
posons $g = g_2 \cdot g_1$, alors $z = g \cdot x, g \in G$ donc \mathcal{R} est transitive.

□

Notation 2.2. L'ensemble des orbites se note \mathcal{X}/G .

2.3 Exemples : Coloration de colliers

Nous calculerons dans ce paragraphe les orbites engendrées par l'action du groupe de symétrie d'un collier sur l'ensemble de ses colorations dans les trois situations suivantes : 3 perles et 2 couleurs, 5 perles et 2 couleurs et 5 perles et 3 couleurs.

2.3.1 Application 1 : 3 perles et 2 couleurs

Les isométries laissant le collier inchangé sont l'identité et les rotations de $2\pi/3$ et $4\pi/3$, notées r_0, r_1 et r_2 respectivement.

Une rotation du collier à 3 perles est une permutation de ses sommets.

Soit $\{1, 2, 3\}$ l'ensemble des perles, notons alors

$$r_0 = 123 \quad r_1 = 231 \quad r_2 = 312$$

D'où, le groupe des isométries d'un collier à 3 perles contient les trois rotations r_0, r_1 et r_2 . Il s'appelle le *groupe cyclique d'ordre 3* et se note G_3 . $G_3 = \{123, 231, 312\}$. Soit $\{r, b\}$ l'ensemble des couleurs rouge et bleu. L'ensemble \mathcal{C} de toutes les colorations possibles contient $2^3 = 8$ éléments montrées par la figure 2.1 suivante :

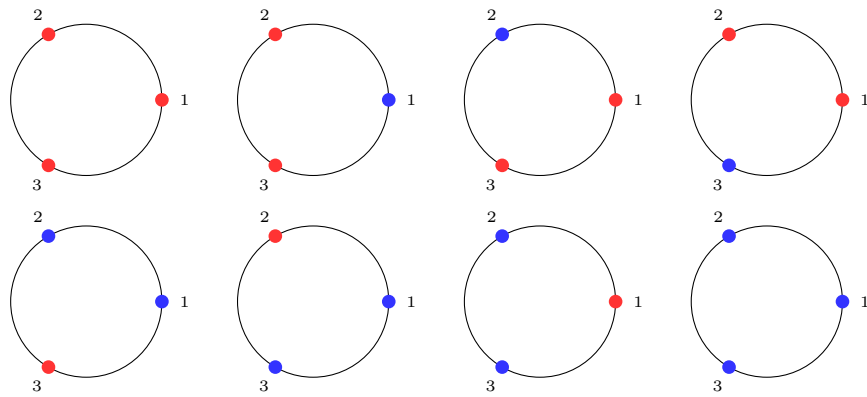


FIGURE 2.1 – Toutes les colorations du collier de 3 perles avec 2 couleurs.

Une coloration $c \in \mathcal{C}$ est une application :

$$\begin{aligned} c : \{1, 2, 3\} &\longrightarrow \{r, b\} \\ x &\longmapsto c(x), \end{aligned}$$

notée plus simplement sous la forme du mot $c = c(1)c(2)c(3)$ sur l'alphabet $\{r, b\}$. Ainsi, $\mathcal{C} = \{rrr, brr, rbr, rrb, bbr, brb, rbb, bbb\}$. La coloration rrb veut dire que les perles 1 et 2 sont rouges tandis que la perle 3 est bleue.

G_3 agit sur \mathcal{C} par :

$$\begin{aligned} G_3 \times \mathcal{C} &\longrightarrow \mathcal{C} \\ (g, c) &\longmapsto g \cdot c = c \circ g^{-1} \end{aligned}$$

Il est clair que l'orbite $\mathcal{O}_{rrr} = \{rrr\}$ et $\mathcal{O}_{bbb} = \{bbb\}$.

Calculons l'orbite $\mathcal{O}_{brr} = \{g \cdot brr, g \in G_3\}$

$$\begin{cases} 123 \cdot brr = brr \circ 123 = brr \\ 231 \cdot brr = brr \circ 312 = rbr \\ 312 \cdot brr = brr \circ 231 = rrb \end{cases} \implies \mathcal{O}_{brr} = \{brr, rbr, rrb\}$$

L'orbite \mathcal{O}_{brr} correspond à toutes les colorations avec une perle bleue et 2 perles rouges.

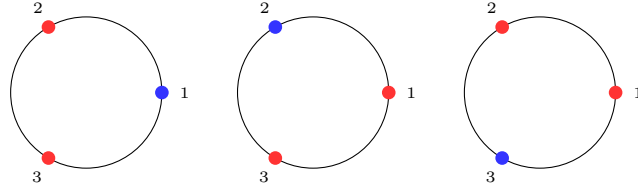


FIGURE 2.2 – Orbite de la coloration brr .

Calculons l'orbite $\mathcal{O}_{bbr} = \{g \cdot bbr, g \in G_3\}$

$$\begin{cases} 123 \cdot bbr = bbr \circ 123 = bbr \\ 231 \cdot bbr = bbr \circ 312 = rbb \\ 312 \cdot bbr = bbr \circ 231 = brb \end{cases} \implies \mathcal{O}_{bbr} = \{bbr, rbb, brb\}$$

Elle correspond à toutes les colorations avec 2 perles bleues et une perle rouge.

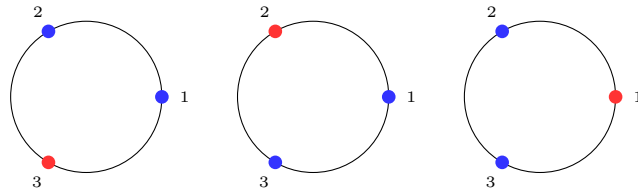


FIGURE 2.3 – Orbite de la coloration bbr .

La figure 2.4 suivante montre l'ensemble \mathcal{C} partitionné en orbites.

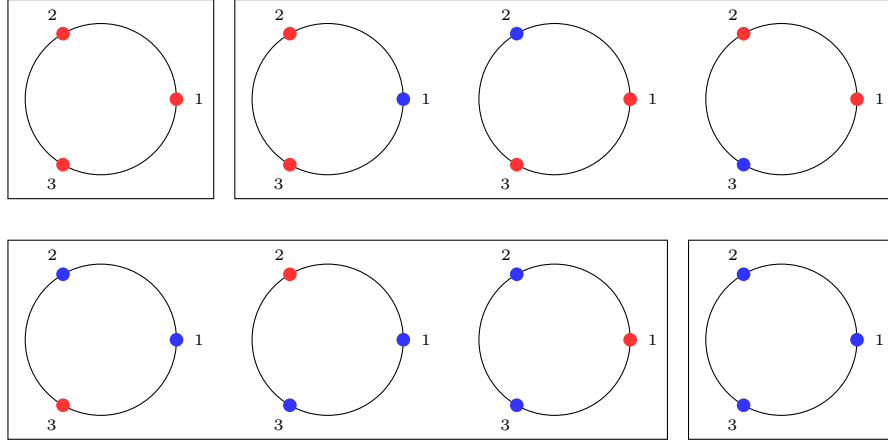


FIGURE 2.4 – Partition des colorations en orbites.

2.3.2 Application 2 : 5 perles et 2 couleurs

Le groupe sous-jacent est le groupe cyclique d'ordre 5 noté C_5 , il contient les rotations $i \times 2\pi/5$ pour $i \in \llbracket 0, 4 \rrbracket$. Chaque rotation est une permutation de sommets. Si $\mathcal{X} = \{1, 2, 3, 4, 5\}$ est l'ensemble des perles, alors le groupe de symétrie du collier à 5 perles est :

$$C_5 = \{12345, 23451, 34512, 45123, 51234\}.$$

L'ensemble \mathcal{C} de toutes les colorations possible contient $2^5 = 32$ éléments.

Action de C_5 sur \mathcal{C}

$$\begin{aligned} C_5 \text{ agit sur } \mathcal{C} \text{ par : } C_5 \times \mathcal{C} &\longrightarrow \mathcal{C} \\ (g, c) &\longmapsto g \cdot c = c \circ g^{-1} \end{aligned}$$

Il est clair que $\mathcal{O}_{rrrrr} = \{rrrrr\}$ et $\mathcal{O}_{bbbbb} = \{bbbbb\}$

Calcul des orbites \mathcal{O}_{rrrrb} et \mathcal{O}_{bbbbb}

Par définition, $\mathcal{O}_{rrrrb} = \{g \cdot rrrrb, g \in C_5\}$

$$\left\{ \begin{array}{l} 12345 \cdot rrrrb = rrrrb \circ 12345 = rrrrb \\ 23451 \cdot rrrrb = rrrrb \circ 51234 = brrrr \\ 34512 \cdot rrrrb = rrrrb \circ 45123 = rbrrr \\ 45123 \cdot rrrrb = rrrrb \circ 34512 = rrbrr \\ 51234 \cdot rrrrb = rrrrb \circ 23451 = rrrbr \end{array} \right.$$

D'où $\mathcal{O}_{rrrrb} = \{rrrrb, brrrr, rbrrr, rrbrr, rrrbr\}$.

De même on trouve que $\mathcal{O}_{bbbbb} = \{bbbbb, rbbbr, brbbb, bbrbb, bbbbr\}$.

Calcul des orbites \mathcal{O}_{rrrbb} et \mathcal{O}_{bbbrb}

$$\mathcal{O}_{rrrbb} = \{g \cdot rrrbb, g \in C_5\}$$

$$\left\{ \begin{array}{l} 12345 \cdot rrrbb = rrrbb \circ 12345 = rrrbb \\ 23451 \cdot rrrbb = rrrbb \circ 51234 = brrrb \\ 34512 \cdot rrrbb = rrrbb \circ 45123 = brrrr \\ 45123 \cdot rrrbb = rrrbb \circ 34512 = rbrrr \\ 51234 \cdot rrrbb = rrrbb \circ 23451 = rbbrb \end{array} \right.$$

D'où $\mathcal{O}_{rrrbb} = \{rrrbb, brrrb, brrrr, rbrrr, rbbrb\}$.

De même on trouve que $\mathcal{O}_{bbrrr} = \{bbrrr, rbbrb, rrbbb, brrbb, brrrb\}$.

Calcul des orbites \mathcal{O}_{rbrbr} et \mathcal{O}_{brbrb}

Par définition, $\mathcal{O}_{rbrbr} = \{g \cdot rbrbr, g \in C_5\}$

$$\left\{ \begin{array}{l} 12345 \cdot rbrbr = rbrbr \circ 12345 = rbrbr \\ 23451 \cdot rbrbr = rbrbr \circ 51234 = rrbrb \\ 34512 \cdot rbrbr = rbrbr \circ 45123 = brrbr \\ 45123 \cdot rbrbr = rbrbr \circ 34512 = rbrrb \\ 51234 \cdot rbrbr = rbrbr \circ 23451 = brbbbr \end{array} \right.$$

D'où $\mathcal{O}_{rbrbr} = \{rbrbr, rrbrb, brrbr, rbrrb, brbbbr\}$.

De même on trouve que $\mathcal{O}_{brbrb} = \{brbrb, bbrbr, rbbrb, brbbbr, rbrrb\}$.

Les colorations réellement différentes de 5 perles et 2 couleurs

Les 8 orbites trouvées contiennent les 32 colorations. D'après la propriété 2.1, il n'existe pas d'autres orbites. Les colorations réellement différentes sont les représentants des orbites présentées à la Figure 2.5 suivante :

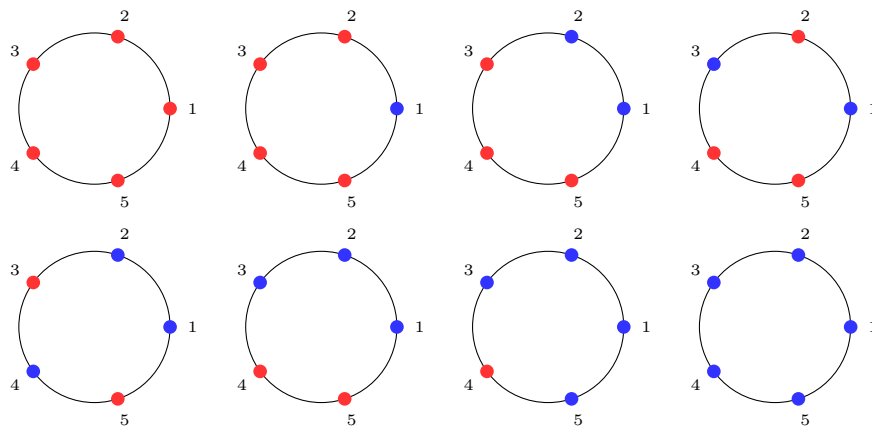


FIGURE 2.5 – Les 8 colorations réellement différentes d'un collier de 5 perles avec 2 couleurs

2.3.3 Application 3 : 5 perles et 3 couleurs

Le groupe sous-jacent est C_5 , $\{r, b, j\}$ est l'ensemble de couleurs rouge, bleu et jaune. Les colorations possibles sont en nombre de $3^5 = 243$. Le calcul fait dans

l'application précédente (paragraphe 2.3.2) nous donne le résultat pour une et deux couleurs soit le résultat avec les ensembles de couleurs $\{r\}$, $\{b\}$, $\{j\}$, $\{r, b\}$, $\{r, j\}$, $\{b, j\}$ comme le montre la table 2.1 suivante :

couleurs	nombre de colorations utilisant exactement l'ensemble de couleurs spécifiés	nombre d'orbites
$\{r\}$	1	1
$\{b\}$	1	1
$\{j\}$	1	1
$\{r, b\}$	30	6
$\{r, j\}$	30	6
$\{b, j\}$	30	6

TABLE 2.1 – Nombre de colorations/orbites d'un collier de 5 perles avec au plus 2 couleurs

Nous avons déjà 21 orbites. Calculons maintenant les orbites des colorations avec exactement 3 couleurs.

Calcul des orbites avec exactement trois couleurs

Par définition, $\mathcal{O}_{rrrbj} = \{g \cdot rrrbj, g \in C_5\}$.

$$\left\{ \begin{array}{l} 12345 \cdot rrrbj = rrrbj \circ 12345 = rrrbj \\ 23451 \cdot rrrbj = rrrbj \circ 51234 = jrrrb \\ 34512 \cdot rrrbj = rrrbj \circ 45123 = bjrrr \\ 45123 \cdot rrrbj = rrrbj \circ 34512 = rbjrr \\ 51234 \cdot rrrbj = rrrbj \circ 23451 = rrbjr \end{array} \right.$$

D'où $\mathcal{O}_{rrrbj} = \{rrrbj, jrrrb, bjrrr, rbjrr, rrbjr\}$.

En permutant les noms de couleurs (ex. r par b) dans les colorations, on trouve les orbites de $rrrbjb$, $bbbrj$, $bbbjr$, $jjjrb$ et $jjjbr$. Ce qui fait 6 nouvelles orbites différentes.

Les quatre colorations $rrbbj$, $rbrjj$, $rbjrr$ et $rbrbj$ ne peuvent pas être obtenues les unes des autres par des rotations et donc elles appartiennent à des orbites différentes. Pour chacune, il existe $3! = 6$ autres colorations obtenues en permutant les noms de couleurs, et ces colorations sont elles aussi différentes. Nous avons $4 \times 6 = 24$ nouvelles orbites.

La table 2.2 suivante montre les éléments des orbites calculées à la main :

Orbite	Éléments	$ Orbite $	# orbites en permutant les couleurs
\mathcal{O}_{rrrbj}	$rrrbj, jrrrb, bjr rr, rbj rr, rrbjr$	5	6
\mathcal{O}_{rrbbj}	$rrbbj, jrbb, bjrrb, bjrrb, bbjrr$	5	6
\mathcal{O}_{rbrjj}	$rbrjj, jrbrj, jjrbr, rjjrb, brjjr$	5	6
\mathcal{O}_{rbjrr}	$rbjrr, jrbjr, rjrbj, jrjrb, bjrjr$	5	6
\mathcal{O}_{rbrbj}	$rbrbj, jrbrb, bjrbr, rbjrb, brbjr$	5	6

TABLE 2.2 – Cinq orbites des colorations utilisant exactement 3 couleurs.

La table 2.2 montre qu'il existe $6 \times 5 = 30$ orbites avec exactement trois couleurs. Et que le nombre de colorations avec exactement trois couleurs est $30 \times 5 = 150$ colorations.

Chacune des orbites avec au moins 2 couleurs contient 5 éléments (chaque rotation donne une nouvelle coloration). Les orbites avec exactement une couleur sont des singletons et elles sont trois : \mathcal{O}_{rrrrr} , \mathcal{O}_{bbbbb} et \mathcal{O}_{jjjjj} . La somme des cardinalités des orbites d'après les tables 2.1 et 2.2 est :

$$(6 \times 8) \times 5 + 3 = 243 = 3^5$$

Comme l'ensemble d'orbites est une partition de \mathcal{C} (propriété 2.1) nous avons trouvé toutes les orbites.

Les colorations réellement différentes de 5 perles et 3 couleurs

Les colorations réellement différentes sont les représentants d'orbites. Donc le nombre recherché est le nombre d'orbites. Or, d'après les tables 2.1 et 2.2 ce nombre est $1 + 1 + 1 + 6 + 6 + 6 + 30 = 51$.

Après ces trois applications, nous remarquons que l'augmentation du nombre de perles ou de couleurs, rend le calcul plus long et plus complexe. Dans la suite du document, nous verrons des méthodes plus efficaces.

2.4 Stabilisateur et fixateur

Définition 2.3 (Stabilisateur). *Le stabilisateur d'un élément $x \in \mathcal{X}$ noté $Stab(x)$ est l'ensemble*

$$Stab(x) = \{g \in G, g \cdot x = x\}. \quad (2.2)$$

Théorème 2.1. *Le stabilisateur de $x \in \mathcal{X}$ est un sous groupe de G .*

Démonstration. Soit $x \in G$. Prouvons que $Stab(x)$ est un sous-groupe de G .

- $Stab(x) \subseteq G$.
- $e \cdot x = x$ donc $e \in Stab(x)$.

— Soient $g_1, g_2 \in \text{Stab}(x)$:

$$g_1 \cdot (g_2 \cdot x) = g_1 \cdot x = x \quad (1)$$

Comme il s'agit d'une action de groupe on a :

$$(g_1 \cdot g_2) \cdot x = g_1 \cdot (g_2 \cdot x) \quad (2)$$

(1) et (2) impliquent que $(g_1 \cdot g_2) \cdot x = x$, donc $g_1 \cdot g_2 \in \text{Stab}(x)$.

— Soit $g \in \text{Stab}(x)$, on a $g \cdot x = x$,

$$g^{-1} \cdot x = g^{-1} \cdot (g \cdot x) = (g^{-1} \cdot g) \cdot x = e \cdot x = x$$

donc $g^{-1} \in \text{Stab}(x)$.

□

Reprenons l'exemple de coloration du collier de 3 perles avec les couleurs rouge et bleu. Calculons quelques stabilisateurs. Ici, $G = \{123, 231, 312\}$.

Par définition, le stabilisateur d'une coloration $c \in \mathcal{C}$ est $\text{Stab}(c) = \{g \in G : g \cdot c = c\}$.

$$\left\{ \begin{array}{l} 123 \cdot rrr = rrr \circ 123 = rrr \\ 231 \cdot rrr = rrr \circ 312 = rrr \\ 312 \cdot rrr = rrr \circ 231 = rrr \end{array} \right. \implies \text{Stab}(rrr) = \{123, 231, 312\} = G.$$

Même chose pour la coloration bbb , on trouve $\text{Stab}(bbb) = G$.

$$\left\{ \begin{array}{l} 123 \cdot brr = brr \circ 123 = brr \\ 231 \cdot brr = brr \circ 312 = rbr \\ 312 \cdot brr = brr \circ 231 = rrb \end{array} \right. \implies \text{Stab}(brr) = \{123\} = \{e\}.$$

$$\left\{ \begin{array}{l} 123 \cdot rbr = rbr \circ 123 = rbr \\ 231 \cdot rbr = rbr \circ 312 = rrb \\ 312 \cdot rbr = rbr \circ 231 = brr \end{array} \right. \implies \text{Stab}(rbr) = \{123\} = \{e\}.$$

Lemme 2.1. (théorème du stabilisateur [4]) Soit $x \in \mathcal{X}$. Alors : $|\text{Stab}(x)| \times |\mathcal{O}_x| = |G|$.

Démonstration. Tout d'abord nous avons,

$$|G| = |\{(g, g \cdot x), g \in G\}| \quad (2.3)$$

$$= |\{(g, y) \in G \times \mathcal{O}_x, g \cdot x = y\}| \quad (2.4)$$

$$= \sum_{y \in \mathcal{O}_x} \sum_{\substack{g \in G \\ g \cdot x = y}} 1 \quad (2.5)$$

$$= \sum_{y \in \mathcal{O}_x} |\{g \in G, g \cdot x = y\}| \quad (2.6)$$

Soit $y \in \mathcal{O}_x$ tel que $g_0 \cdot x = y$ pour un élément $g_0 \in G$. Pour prouver que $|\{g \in G, g \cdot x = y\}| = |\{g \in G, g \cdot x = x\}|$, prouvons qu'il existe une bijection entre les deux ensembles. Soit l'application :

$$\begin{aligned} \phi : \{g \in G, g \cdot x = y\} &\longrightarrow \text{Stab}(x) \\ g &\longmapsto g_0^{-1} \cdot g \end{aligned}$$

Pour montrer que ϕ est correctement définie, montrons que si $g \in \{g \in G, g \cdot x = y\}$, alors $\phi(g) \in \text{Stab}(x)$.

$$\begin{aligned} g \in \{g \in G, g \cdot x = y\} &\implies (g_0^{-1} \cdot g) \cdot x = g_0^{-1} \cdot (g \cdot x) = g_0^{-1} \cdot y = x \\ &\implies (g_0^{-1} \cdot g) \in \text{Stab}(x) \end{aligned}$$

Pour montrer que ϕ est une bijection, il faut trouver son "inverse". Soit l'application :

$$\begin{aligned} \psi : \text{Stab}(x) &\longrightarrow \{g \in G, g \cdot x = y\} \\ g &\longmapsto g_0 \cdot g \end{aligned}$$

ψ est correctement définie :

$$\begin{aligned} g \in \text{Stab}(x) &\implies (g_0 \cdot g) \cdot x = g_0 \cdot (g \cdot x) = g_0 \cdot x = y \\ &\implies g_0 \cdot g \in \{g \in G, g \cdot x = y\} \end{aligned}$$

Nous avons bien $\phi \circ \psi(g) = g$ et $\psi \circ \phi(g) = g$. Donc ϕ est une bijection et $\psi = \phi^{-1}$. Donc pour tout $x \in \mathcal{X}$ et pour tout $y \in \mathcal{O}_x$:

$$|\{g \in G, g \cdot x = y\}| = |\{g \in G, g \cdot x = x\}| = |\text{Stab}(x)|. \quad (2.7)$$

D'après le calcul (2.3), nous avons :

$$\begin{aligned} |G| &= \sum_{y \in \mathcal{O}_x} |\{g \in G, g \cdot x = y\}| \\ &= \sum_{y \in \mathcal{O}_x} |\text{Stab}(x)| \\ &= |\text{Stab}(x)| \sum_{y \in \mathcal{O}_x} 1 \\ &= |\text{Stab}(x)| \times |\mathcal{O}_x| \end{aligned}$$

□

Définition 2.4. (*Fixateur*) Le fixateur d'un élément $g \in G$, noté $\text{Fix}(g)$, est le sous-ensemble de \mathcal{X} défini par :

$$\text{Fix}(g) = \{x \in \mathcal{X}, g \cdot x = x\}. \quad (2.8)$$

2.5 Action de groupe sur un ensemble de fonctions

Dans cette section, nous considérerons le groupe produit $G \times H$, où H est un autre groupe fini. e_G , e_H et $e_{G \times H}$ sont les éléments neutres de G , H et $G \times H$ respectivement.

La notation $\text{Map}(\mathcal{X}, \mathcal{Y})$ désignera l'ensemble de toutes les applications de \mathcal{X} vers \mathcal{Y} , où \mathcal{Y} est un ensemble fini.

2.5.1 Groupe produit

Rappelons que le groupe produit $G \times H$ est la structure algébrique mise sur le produit cartésien $G \times H = \{(g, h), g \in G, h \in H\}$, muni de la loi de composition interne :

$$\begin{aligned} (G \times H)^2 &\longrightarrow G \times H \\ ((g_1, h_1), (g_2, h_2)) &\longmapsto (g_1 \cdot g_2, h_1 \cdot h_2) \end{aligned} \quad (2.9)$$

avec $e_{G \times H} = (e_G, e_H)$ et $(g, h)^{-1} = (g^{-1}, h^{-1})$.

2.5.2 Action du groupe produit

Propriété 2.3. Si G agit sur \mathcal{X} et H agit sur \mathcal{Y} , alors le groupe produit $G \times H$ agit sur $\text{Map}(\mathcal{X}, \mathcal{Y})$ par :

$$\begin{aligned} G \times H \times \text{Map}(\mathcal{X}, \mathcal{Y}) &\longrightarrow \text{Map}(\mathcal{X}, \mathcal{Y}) \\ (g, h, \phi) &\longmapsto (g, h) \cdot \phi : \quad \mathcal{X} \longrightarrow \mathcal{Y} \\ x &\longmapsto h \cdot \phi(g^{-1} \cdot x) \end{aligned} \quad (2.10)$$

Démonstration. Vérifions que l'application est une action de groupe.

e_G, e_H sont les éléments neutres de G et de H respectivement.

Soient $g_1, g_2 \in G, h_1, h_2 \in H$, et $\phi \in \text{Map}(\mathcal{X}, \mathcal{Y})$. Nous avons alors :

$$\begin{aligned} i) \quad ((e_G, e_H) \cdot \phi)(x) &= e_H \cdot \phi(e_G^{-1} \cdot x) \\ &= e_H \cdot \phi(x) && (\text{car } G \text{ agit sur } \mathcal{X}) \\ &= \phi(x) && (\text{car } \phi \cdot x \in \mathcal{Y} \text{ et } H \text{ agit sur } \mathcal{Y}) \end{aligned}$$

Notation 2.3. Pour simplifier l'écriture, notons $(g, h) \cdot \phi(x)$ sous la forme $h \cdot \phi \cdot g^{-1} \cdot x$.

Le point le plus à droite est l'action de G sur \mathcal{X} , celui du milieu désigne l'action de ϕ sur $g^{-1} \cdot x$, enfin, le point le plus à gauche désigne l'action de H sur $\phi \cdot g^{-1} \cdot x = \phi(g^{-1} \cdot x)$.

$$\begin{aligned} ii) \quad (g_1, h_1) \cdot ((g_2, h_2) \cdot \phi)(x) &= h_1 \cdot ((g_2, h_2) \cdot \phi) \cdot g_1^{-1} \cdot x \\ &= h_1 \cdot (h_2 \cdot \phi \cdot g_2^{-1}) \cdot g_1^{-1} \cdot x \\ &= h_1 \cdot h_2 \cdot \phi \cdot g_2^{-1} \cdot g_1^{-1} \cdot x \\ &= (h_1 \cdot h_2) \cdot \phi \cdot (g_2^{-1} \cdot g_1^{-1}) \cdot x \\ &= (h_1 \cdot h_2) \cdot \phi \cdot (g_2 \cdot g_1)^{-1} \cdot x \\ &= ((g_1 \cdot g_2, h_1 \cdot h_2) \cdot \phi)(x) && (\text{par définition de l'application 2.10}). \\ &= ((g_1, h_1) \cdot (g_2, h_2)) \cdot \phi(x). \end{aligned}$$

□

Relation d'équivalence induite par l'action du groupe produit

Si ϕ, ψ sont deux fonctions de $Map(\mathcal{X}, \mathcal{Y})$, alors la relation d'équivalence \sim sous-jacente à l'action du groupe $G \times H$ sur $Map(\mathcal{X}, \mathcal{Y})$ est définie par :

$$\begin{aligned}\phi \sim \psi &\iff \exists (g, h) \in G \times H, \phi = (g, h) \cdot \psi \\ &\iff \exists (g, h) \in G \times H, \phi = h \cdot \psi \cdot g^{-1} \\ &\iff \exists (g, h) \in G \times H, \phi \cdot g = h \cdot \psi \\ &\iff \exists (g, h) \in G \times H, \forall x \in \mathcal{X}, \phi(g \cdot x) = h \cdot \psi(x).\end{aligned}$$

3 Lemme de Burnside et théorie de Pólya

Introduction

Nous avons vu dans le paragraphe 2.3 (Application aux coloration de colliers) que la construction manuelle d'orbites devient fastidieuse à partir de 5 perles seulement, et surtout nous ne sommes pas à l'abri d'un oubli ou d'une erreurs de calcul.

Nous présenterons dans ce chapitre un cadre théorique pour compter les orbites, sans les construire, grâce à des outils de la théorie des groupes.

Dans tout ce chapitre, on se donne deux ensembles finis \mathcal{X} et \mathcal{Y} , deux groupes finis G et H tels que G agit sur \mathcal{X} et H agit sur \mathcal{Y} . D'après le paragraphe 2.5.2 (action du groupe produit), nous savons que le groupe produit $G \times H$ agit sur l'ensemble de fonctions de \mathcal{X} à valeurs dans \mathcal{Y} , noté $\text{Map}(\mathcal{X}, \mathcal{Y})$.

Enfin, A désignera un anneau que nous particulariserons dans les exemples.

3.1 Fonctions de poids

Une fonction de poids est une application $w : \mathcal{X} \rightarrow A$ définie sur l'ensemble \mathcal{X} à valeurs dans un anneau A .

La fonction de poids triviale est : $w : \mathcal{X} \rightarrow \mathbb{Z}$

$$x \mapsto 1$$

Plus généralement, si $\mathcal{P}(\mathcal{X})$ désigne l'ensemble des parties de \mathcal{X} , alors la fonction de poids d'une partie $S \subseteq \mathcal{X}$ est :

$$\begin{aligned} w : \mathcal{P}(\mathcal{X}) &\longrightarrow A \\ S &\longmapsto \sum_{\delta \in S} w(\delta) \end{aligned}$$

La fonction de poids moyen, notée W , associée à la fonction de poids $w : \mathcal{P}(\mathcal{X}) \rightarrow A$ est une application :

$$\begin{aligned} W : \mathcal{P}(\mathcal{X}) &\longrightarrow A \\ S &\longmapsto \begin{cases} 0 & \text{si } S = \emptyset \\ \frac{1}{|S|} w(S) & \text{sinon.} \end{cases} \end{aligned}$$

3.2 Lemme de Burnside

Ce lemme portant le nom de Burnside en référence au mathématicien anglais William Burnside (1852 – 1927) connu pour ses travaux dans la théorie des groupes, est aussi nommé **théorème de Burnside–Frobenius**, **lemme de Cauchy–Frobenius**, ou le **lemme qui n’est pas de Burnside**. Déjà connu par Augustin-Louis Cauchy (1789 – 1857) et Ferdinand Frobenius (1849 – 1917), mais il a été popularisé par Burnside [3] en 1897 qui l’a lui même attribué à Frobenius-1887 [5].

Lemme 3.1. [3] Soit W la fonction de poids moyen associée à une fonction de poids $w : \mathcal{P}(\mathcal{X}) \longrightarrow A$.

$$\sum_{\mathcal{O} \in \mathcal{X}/G} W(\mathcal{O}) = \frac{1}{|G|} \sum_{g \in G} w(\text{Fix}(g)). \quad (3.1)$$

Un cas particulier important est de considérer la fonction de poids triviale. La fonction du poids moyen devient :

$$\begin{aligned} W : \mathcal{P}(\mathcal{X}) &\longrightarrow \mathbb{Z} \\ S &\longmapsto \begin{cases} 0 & \text{si } S = \emptyset. \\ 1 & \text{sinon.} \end{cases} \end{aligned}$$

car la moyenne des poids égaux à 1 est 1. Le lemme devient :

$$|\mathcal{X}/G| = \frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g)|. \quad (3.2)$$

Ceci donne une formule pour calculer le nombre d’orbites de \mathcal{X} sous l’action de G .

Démonstration. Prouvons le cas général.

Nous avons par définition de la fonction poids moyen :

$$\sum_{\mathcal{O} \in \mathcal{X}/G} W(\mathcal{O}) = \sum_{\mathcal{O} \in \mathcal{X}/G} \frac{1}{|\mathcal{O}|} \sum_{x \in \mathcal{O}} w(x) = \sum_{\mathcal{O} \in \mathcal{X}/G} \sum_{x \in \mathcal{O}} \frac{w(x)}{|\mathcal{O}_x|} = \sum_{x \in \mathcal{X}} \frac{w(x)}{|\mathcal{O}_x|},$$

car \mathcal{X}/G est une partition de \mathcal{X} d’après les propriétés 2.1 et 2.2. Or, d’après le lemme 2.1, $|G| = |\mathcal{O}_x| \times |\text{Stab}(x)|$ pour tout $x \in \mathcal{X}$.

En remplaçant donc $|\mathcal{O}_x|$ par $\frac{|G|}{|\text{Stab}(x)|}$, on trouve :

$$\begin{aligned}
\sum_{\mathcal{O} \in \mathcal{X}/G} W(\mathcal{O}) &= \frac{1}{|G|} \sum_{x \in \mathcal{X}} (w(x) |Stab(x)|) = \frac{1}{|G|} \sum_{x \in \mathcal{X}} \left(w(x) \sum_{g \in Stab(x)} 1 \right) \\
&= \frac{1}{|G|} \sum_{x \in \mathcal{X}} \left(w(x) \sum_{\substack{g \in G \\ g \cdot x = x}} 1 \right) = \frac{1}{|G|} \sum_{x \in \mathcal{X}} \sum_{\substack{g \in G \\ g \cdot x = x}} w(x) \\
&= \frac{1}{|G|} \sum_{g \in G} \sum_{\substack{x \in \mathcal{X} \\ g \cdot x = x}} w(x) \quad (\text{car les deux sommes sont finies}) \\
&= \frac{1}{|G|} \sum_{g \in G} \sum_{x \in Fix(g)} w(x) = \frac{1}{|G|} \sum_{g \in G} w(Fix(g)).
\end{aligned}$$

□

3.3 Exemples : Coloration de collier

Nous allons reprendre les exemples calculés à la main dans le paragraphe 2.3 du chapitre précédent, et nous verrons que le lemme de Burnside est une amélioration substantielle : une page et demi de calcul contre cinq et demi.

3.3.1 Application 1 : 3 perles et 2 couleurs

Rappelons que le groupe sous-jacent est le groupe cyclique d'ordre 3 : $C_3 = \{123, 231, 312\}$.

Soit aussi $\{r, b\}$ l'ensemble des couleurs rouge et bleu. L'ensemble de colorations possibles est $\mathcal{C} = \{rrr, brr, rbr, rrb, bbr, brb, rbb, bbb\}$.

D'après le lemme de Burnside (Équation 3.2) le nombre de coloration réellement différentes est donné par le nombre d'orbites de l'action de C_3 sur \mathcal{C} .

Ainsi, ce nombre est donné par :

$$|\mathcal{C}/C_3| = \frac{1}{|C_3|} \sum_{\sigma \in C_3} |Fix(\sigma)|. \quad (3.3)$$

Il est facile de calculer à la main les fixateurs et trouver que :

$$|Fix(123)| = |\mathcal{C}| = 8, \quad |Fix(231)| = |\{rrr, bbb\}| = 2, \quad |Fix(312)| = |\{rrr, bbb\}| = 2$$

Donc,

$$|\mathcal{C}/C_3| = \frac{|Fix(123)| + |Fix(231)| + |Fix(312)|}{3} = \frac{8 + 2 + 2}{3} = 4.$$

Ceci correspond au nombre d'orbites calculées à la main dans le chapitre précédent, qui sont les suivants :

$$\begin{aligned}
\mathcal{O}_{rrr} &= \{rrr\}, & \mathcal{O}_{bbb} &= \{bbb\}, \\
\mathcal{O}_{rrb} &= \{rrb, brr, rbr\}, & \mathcal{O}_{bbr} &= \{bbr, rbb, brb\}.
\end{aligned}$$

3.3.2 Application 2 : 5 perles et 2 couleurs

Le groupe cyclique d'ordre 5 est $C_5 = \{12345, 23451, 34512, 45123, 51234\}$. Les couleurs sont rouge et bleu $\mathcal{Y} = \{r, b\}$. L'ensemble de colorations possible est \mathcal{C} contient $2^5 = 32$ éléments. On cherche à calculer :

$$|\mathcal{C}/C_5| = \frac{1}{|C_5|} \sum_{\sigma \in C_5} |Fix(\sigma)|. \quad (3.4)$$

Il est clair que l'identité fixe toutes les colorations, donc $Fix(12345) = \mathcal{C}$. Les autres rotations ne fixent que les colorations avec une seule couleur, c'est à dire, $rrrrr$ et $bbbbb$. Nous verrons plus loin dans le document une formule pour compter les colorations fixes (voir le corollaire 3.2). Ainsi :

$$|Fix(12345)| = |\mathcal{C}| = 32, \quad |Fix(\sigma)| = |\{rrrrr, bbbbb\}| = 2 \quad \forall \sigma \neq 12345.$$

Donc,

$$|\mathcal{C}/C_5| = \frac{32 + 2 + 2 + 2 + 2}{5} = \frac{40}{5} = 8.$$

Les huit orbites calculées précédemment sont :

$$\begin{aligned} \mathcal{O}_{rrrrr} &= \{rrrrr\}, & \mathcal{O}_{bbbbb} &= \{bbbbb\}, \\ \mathcal{O}_{rrrrb} &= \{rrrrb, brrrr, rbrrr, rrbr, rrrbr\}, & \mathcal{O}_{bbbbb} &= \{bbbbb, rbbbb, brbbb, bbrbb, bbbbr\}, \\ \mathcal{O}_{rrrrb} &= \{rrrrb, brrrb, brrrr, rbbrr, rrbbr\}, & \mathcal{O}_{bbbbb} &= \{bbbbb, rbbbr, rrbbr, brrbb, bbbrr\}, \\ \mathcal{O}_{rbrbr} &= \{rbrbr, rrbrb, brrbr, rbrrb, brbbr\}, & \mathcal{O}_{brbrb} &= \{brbrb, bbrbr, rbbbr, brbbr, rbrrb\}. \end{aligned}$$

3.3.3 Application 3 : 5 perles et 3 couleurs

Soient les couleurs rouge, bleu, jaune. $\mathcal{X} = \{1, 2, 3, 4, 5\}$ et $\mathcal{Y} = \{r, b, j\}$. L'ensemble de colorations possible est \mathcal{C} contient $3^5 = 243$ éléments. On cherche à calculer :

$$|\mathcal{C}/C_5| = \frac{1}{|C_5|} \sum_{\sigma \in C_5} |Fix(\sigma)|.$$

Pour les mêmes raisons citées dans l'exemple précédent, on trouve que :

$$Fix(12345) = \mathcal{C} \text{ et } Fix(\sigma) = \{rrrrr, bbbbb, jjjjj\} \text{ pour toute permutation } \sigma \neq 12345.$$

Donc,

$$|Fix(12345)| = |\mathcal{C}| = 243 \quad |Fix(\sigma)| = |\{rrrrr, bbbbb, jjjjj\}| = 3, \sigma \neq 12345.$$

Finalement,

$$|\mathcal{C}/C_5| = \frac{243 + 3 + 3 + 3 + 3}{5} = \frac{255}{5} = 51.$$

3.4 Généralisation du lemme de Burnside : Formule de De Bruijn

Nicolaas Govert De Bruijn (1918 - 2012) est un mathématicien néerlandais connu pour ses travaux dans la théorie des graphes, la combinatoire, la géométrie et l'analyse asymptotique.

Parmi ses travaux en combinatoire, on trouve la formule de De Bruijn qui est une généralisation du lemme de Burnside. Elle reprend le résultat pour l'action du groupe produit $G \times H$ sur l'ensemble de fonctions $Map(\mathcal{X}, \mathcal{Y})$.

Le résultat suivant est la formule de De Bruijn [2] :

Lemme 3.2. *Soit A un anneau, et soit $W : Map(\mathcal{X}, \mathcal{Y}) \longrightarrow A$ la fonction de poids moyen associée à la fonction de poids $w : Map(\mathcal{X}, \mathcal{Y}) \longrightarrow A$. Alors,*

$$\sum_{\mathcal{O} \in Map(\mathcal{X}, \mathcal{Y}) /_{G \times H}} W(\mathcal{O}) = \frac{1}{|G \times H|} \sum_{(g, h) \in G \times H} w(Fix(g, h)). \quad (3.5)$$

où,

$$Fix(g, h) = \{\phi \in Map(\mathcal{X}, \mathcal{Y}) : (g, h) \cdot \phi = \phi\} \quad (3.6)$$

$$= \{\phi \in Map(\mathcal{X}, \mathcal{Y}) : \phi \cdot g = h \cdot \phi\} \quad (3.7)$$

Démonstration. Il suffit d'appliquer le lemme de Burnside [Équation 3.1](#) à l'action du groupe produit $G \times H$ sur l'ensemble de fonctions $Map(\mathcal{X}, \mathcal{Y})$. \square

$\{e_H\}$ est le groupe réduit à son élément neutre e_H . D'après la proposition [2.3](#) du paragraphe [2.5.2](#), $G \times \{e_H\}$ agit sur $Map(\mathcal{X}, \mathcal{Y})$ par :

$$\begin{aligned} G \times \{e_H\} \times Map(\mathcal{X}, \mathcal{Y}) &\longrightarrow Map(\mathcal{X}, \mathcal{Y}) \\ (g, e_H, \phi) &\longmapsto (g, e_H) \cdot \phi : \mathcal{X} \longrightarrow \mathcal{Y} \\ x &\longmapsto e_H \cdot \phi(g^{-1} \cdot x) \end{aligned}$$

ou de manière équivalente, G agit sur $Map(\mathcal{X}, \mathcal{Y})$ par :

$$\begin{aligned} G \times Map(\mathcal{X}, \mathcal{Y}) &\longrightarrow Map(\mathcal{X}, \mathcal{Y}) \\ (g, \phi) &\longmapsto g \cdot \phi : \mathcal{X} \longrightarrow \mathcal{Y} \\ x &\longmapsto \phi(g^{-1} \cdot x) \end{aligned}$$

Ainsi, la formule de De Bruijn ([Équation 3.5](#)) devient :

$$\sum_{\mathcal{O} \in Map(\mathcal{X}, \mathcal{Y}) /_G} W(\mathcal{O}) = \frac{1}{|G|} \sum_{g \in G} w(Fix(g)). \quad (3.8)$$

Nous utiliserons cette formule plus loin pour prouver le théorème de Pólya.

3.5 Polynômes indicateur de cycles

Supposons maintenant que G soit un groupe de permutation de degré n , (c'est à dire un sous groupe de \mathfrak{S}_n). Rappelons que toute permutation $\sigma \in \mathfrak{S}_n$ se décompose en un produit de cycles (voir [Théorème 1.1](#)).

Notation 3.1. Notons $c_k(\sigma)$ le nombre de cycles de longueur k de cette décomposition.

Exemple 3.1. D'après l'exemple [1.14](#), la décomposition de la permutation $\sigma = 37862451$ donne $\sigma = (1, 3, 8)(2, 7, 5)(4, 6)$. Les $c_k(\sigma)$ pour $k \in \{1, 2, \dots, 8\}$ sont données dans la table [3.1](#) suivante :

$c_1(\sigma)$	$c_2(\sigma)$	$c_3(\sigma)$	$c_4(\sigma)$	$c_5(\sigma)$	$c_6(\sigma)$	$c_7(\sigma)$	$c_8(\sigma)$
0	1	2	0	0	0	0	0

TABLE 3.1 – $c_k(\sigma)$ pour $k \in \{1, 2, \dots, 8\}$ de la permutation $\sigma = 37862451$.

3.5.1 Indicateur de cycles d'une permutation

Définition 3.1. [\[4\]](#) L'indicateur de cycles d'une permutation $\sigma \in G$, noté $Z_\sigma(x_1, x_2, \dots, x_n)$ est le monôme défini par :

$$Z_\sigma(x_1, x_2, \dots, x_n) = x_1^{c_1(\sigma)} x_2^{c_2(\sigma)} \dots x_n^{c_n(\sigma)}. \quad (3.9)$$

Exemple 3.2. Soit $\sigma = 132$. Nous avons $\sigma = (1)(2, 3)$ donc $c_1(\sigma) = 1$, $c_2(\sigma) = 1$, et $c_3(\sigma) = 0$, d'où le monôme $Z_\sigma(x_1, x_2, x_3) = x_1 x_2$.

Exemple 3.3. Pour $\sigma = 37862451$ de l'exemple [3.1](#), on trouve $Z_\sigma(x_1, x_2, \dots, x_8) = x_2 x_3^2$.

3.5.2 Indicateur de cycles d'un groupe de permutations

Définition 3.2. [\[4\]](#) L'indicateur de cycles de G , noté $Z_G(x_1, x_2, \dots, x_n)$ est le polynôme suivant :

$$Z_G(x_1, x_2, \dots, x_n) = \frac{1}{|G|} \sum_{\sigma \in G} Z_\sigma(x_1, x_2, \dots, x_n). \quad (3.10)$$

3.5.3 Calcul de l'indicateur de cycle de \mathfrak{S}_3

Nous avons par définition $\mathfrak{S}_3 = \{123, 132, 213, 231, 312, 321\}$. Posons $x = (x_1, x_2, x_3)$. Nous voulons calculer :

$$Z_{\mathfrak{S}_3}(x) = \frac{1}{6} \sum_{\sigma \in \mathfrak{S}_3} x_1^{c_1(\sigma)} x_2^{c_2(\sigma)} x_3^{c_3(\sigma)}$$

Pour chaque permutation, calculons la décomposition en produit de cycles, puis calculons le monôme correspondant :

$$\begin{aligned}
\sigma_1 = 123 &= (1)(2)(3) \rightsquigarrow c_1(\sigma_1) = 3 \quad c_2(\sigma_1) = 0 \quad c_3(\sigma_1) = 0 \rightsquigarrow x_1^3 \\
\sigma_2 = 132 &= (1)(2, 3) \rightsquigarrow c_1(\sigma_2) = 1 \quad c_2(\sigma_2) = 1 \quad c_3(\sigma_2) = 0 \rightsquigarrow x_1 x_2 \\
\sigma_3 = 213 &= (1, 2)(3) \rightsquigarrow c_1(\sigma_3) = 1 \quad c_2(\sigma_3) = 1 \quad c_3(\sigma_3) = 0 \rightsquigarrow x_1 x_2 \\
\sigma_4 = 231 &= (1, 2, 3) \rightsquigarrow c_1(\sigma_4) = 0 \quad c_2(\sigma_4) = 0 \quad c_3(\sigma_4) = 1 \rightsquigarrow x_3 \\
\sigma_5 = 312 &= (1, 3, 2) \rightsquigarrow c_1(\sigma_5) = 0 \quad c_2(\sigma_5) = 0 \quad c_3(\sigma_5) = 1 \rightsquigarrow x_3 \\
\sigma_6 = 321 &= (1, 3)(2) \rightsquigarrow c_1(\sigma_6) = 1 \quad c_2(\sigma_6) = 1 \quad c_3(\sigma_6) = 0 \rightsquigarrow x_1 x_2
\end{aligned}$$

Le polynôme indicateur de cycles de \mathfrak{S}_3 est la moyenne des monômes calculés :

$$Z_{\mathfrak{S}_3}(x) = \frac{x_1^3 + 3x_1 x_2 + 2x_3}{6}.$$

3.5.4 Calcul de l'indicateur de cycle de C_n

Calcul de $Z_{C_4}(x)$

Le groupe cyclique d'ordre 4 est $C_4 = \{1234, 2341, 3412, 4123\}$, $x = (x_1, \dots, x_4)$.

$$Z_{C_4}(x) = \frac{1}{4} \sum_{\sigma \in C_4} x_1^{c_1(\sigma)} \dots x_4^{c_4(\sigma)}.$$

Pour chaque $\sigma \in C_4$, calculons la décomposition en produit de cycles, puis calculons Z_σ :

$$\begin{aligned}
\sigma_1 = 1234 &= (1)(2)(3)(4) \rightsquigarrow c_1(\sigma_1) = 4 \quad c_{\neq 1}(\sigma_1) = 0 \rightsquigarrow Z_{\sigma_1} = x_1^4 \\
\sigma_2 = 2341 &= (1, 2, 3, 4) \rightsquigarrow c_{\neq 4}(\sigma_2) = 0 \quad c_4(\sigma_2) = 1 \rightsquigarrow Z_{\sigma_2} = x_4 \\
\sigma_3 = 3412 &= (1, 3)(3, 4) \rightsquigarrow c_2(\sigma_3) = 2 \quad c_{\neq 2}(\sigma_3) = 0 \rightsquigarrow Z_{\sigma_3} = x_2^2 \\
\sigma_4 = 4123 &= (1, 4, 3, 2) \rightsquigarrow c_{\neq 4}(\sigma_4) = 0 \quad c_4(\sigma_4) = 1 \rightsquigarrow Z_{\sigma_4} = x_4
\end{aligned}$$

La moyenne des monômes donne :

$$Z_{C_4}(x) = \frac{x_1^4 + x_2^2 + 2x_4}{4}.$$

Calcul de $Z_{C_5}(x)$

Le groupe cyclique d'ordre 5 est $C_5 = \{12345, 23451, 34512, 45123, 51234\}$.

Nous voulons calculer :

$$Z_{C_5}(x) = \frac{1}{5} \sum_{\sigma \in C_5} x_1^{c_1(\sigma)} \dots x_5^{c_5(\sigma)}.$$

avec $x = (x_1, \dots, x_5)$. Comme dans les exemples précédents, calculons la décomposition puis le monôme pour chaque permutation :

$$\begin{aligned}
\sigma_1 = 12345 &= (1)(2)(3)(4)(5) \rightsquigarrow c_1(\sigma_1) = 5 \quad c_{>1}(\sigma_1) = 0 \rightsquigarrow x_1^5 \\
\sigma_2 = 23451 &= (1, 2, 3, 4, 5) \rightsquigarrow c_{<5}(\sigma_2) = 0 \quad c_5(\sigma_2) = 1 \rightsquigarrow x_5 \\
\sigma_3 = 34512 &= (1, 3, 5, 2, 4) \rightsquigarrow c_{<5}(\sigma_3) = 0 \quad c_5(\sigma_3) = 1 \rightsquigarrow x_5 \\
\sigma_4 = 45123 &= (1, 4, 2, 5, 3) \rightsquigarrow c_{<5}(\sigma_4) = 0 \quad c_5(\sigma_4) = 1 \rightsquigarrow x_5 \\
\sigma_5 = 51234 &= (1, 5, 4, 3, 2) \rightsquigarrow c_{<5}(\sigma_5) = 0 \quad c_5(\sigma_5) = 1 \rightsquigarrow x_5
\end{aligned}$$

La moyenne des monômes donne :

$$Z_{C_5}(x) = \frac{x_1^5 + 4x_5}{5}.$$

Calcul de $Z_{C_6}(x)$

Le groupe cyclique d'ordre 6 est $C_6 = \{123456, 234561, 345612, 456123, 561234, 612345\}$. Pour chaque permutation, calculons la décomposition en produit de cycles, puis calculons le monôme correspondant :

$$\begin{aligned}
\sigma_1 = 123456 &= (1)(2)(3)(4)(5)(6) \rightsquigarrow Z_{\sigma_1} = x_1^6 \\
\sigma_2 = 234561 &= (1, 2, 3, 4, 5, 6) \rightsquigarrow Z_{\sigma_2} = x_6 \\
\sigma_3 = 345612 &= (1, 3, 5)(2, 4, 6) \rightsquigarrow Z_{\sigma_3} = x_3^2 \\
\sigma_4 = 456123 &= (1, 4)(2, 5)(3, 6) \rightsquigarrow Z_{\sigma_4} = x_2^3 \\
\sigma_5 = 561234 &= (1, 5, 3)(2, 6, 4) \rightsquigarrow Z_{\sigma_5} = x_3^2 \\
\sigma_6 = 612345 &= (1, 6, 5, 4, 3, 2) \rightsquigarrow Z_{\sigma_6} = x_6
\end{aligned}$$

La moyenne des monômes donne :

$$Z_{C_6}(x) = \frac{x_1^6 + x_2^3 + 2x_3^2 + 2x_6}{6}.$$

Polynôme indicateur de cycles du groupe cyclique C_n

C_n est le groupe cyclique d'ordre n , donc à n permutations. Il représente le groupe des symétries d'un collier à n perles.

Définition 3.3. La fonction indicatrice d'Euler est définie par :

$$\begin{aligned}
\phi : \mathbb{N}^* &\longrightarrow \mathbb{N}^* \\
n &\longmapsto |\{m \in \llbracket 1, n \rrbracket, \text{pgcd}(n, m) = 1\}|
\end{aligned}$$

La table suivante montre les valeurs de $\phi(n)$ pour $n \leq 8$:

n	$\{m \in \llbracket 1, n \rrbracket, \text{pgcd}(n, m) = 1\}$	$\phi(n)$
1	$\{1\}$	1
2	$\{1\}$	1
3	$\{1, 2\}$	2
4	$\{1, 3\}$	2
5	$\{1, 2, 3, 4\}$	4
6	$\{1, 5\}$	2
7	$\{1, 2, 3, 4, 5, 6\}$	6
8	$\{1, 3, 5, 7\}$	4

TABLE 3.2 – Valeurs de $\phi(n)$ pour $n \leq 8$.

Théorème 3.1. [10] *Le polynôme indicateur de cycles de C_n est :*

$$Z_{C_n}(x) = \frac{1}{n} \sum_{\substack{d \in \mathbb{N}^* \\ d|n}} \phi(d) x_d^{n/d} \quad (3.11)$$

Démonstration. Calculons dans **la partie 1** les monômes des permutations. Et dans **la partie 2**, le polynôme.

Partie 1 :

Soit $\sigma \in C_n$ la permutation représentant la rotation d'angle $(k-1)2\pi/n$ (i.e. celle qui envoie le sommet 1 sur le sommet k) ($3 \leq k \leq n$), elle est de la forme :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n-k+1 & n-k+2 & n-k+3 & \dots & n \\ k & k+1 & k+2 & \dots & n & 1 & 2 & \dots & k-1 \end{pmatrix}$$

Nous avons $\sigma(x) = 1 + (x + k - 2 \pmod{n})$ pour tout $x \in \llbracket 1, n \rrbracket$. Ceci nous permet de construire les cycles de σ , ainsi

$$\text{Le cycle contenant } 1 \quad \gamma_1 = (1, \quad k, \quad 2k-1, \quad 3k-2, \quad \dots, \quad n-k+2).$$

$$\text{Le cycle contenant } 2 \quad \gamma_2 = (2, \quad k+1, \quad 2k, \quad 3k-1, \quad \dots, \quad n-k+3).$$

$$\vdots \quad \quad \quad \vdots \quad \quad \quad \vdots$$

$$\text{Le cycle contenant } k-1 \quad \gamma_{k-1} = (k-1, \quad 2k-2, \quad 3k-3, \quad 4k-4, \quad \dots, \quad n).$$

Les $k-1$ cycles $\gamma_1, \gamma_2, \dots, \gamma_{k-1}$ sont de même longueur. Soit d cette longueur. S'ils sont disjoints, alors σ se décompose en $k-1$ cycles de longueur d donc $Z_\sigma = x_d^{k-1}$. Mais comme $n = d \times (k-1)$ alors $k-1 = n/d$. D'où $Z_\sigma = x_d^{n/d}$.

S'ils ne sont pas disjoints, alors ils sont identiques et σ se décompose en un seul cycle de longueur n ($d = n$), d'où $Z_\sigma = x_n$.

Nous venons de prouver donc que pour tout $\sigma \in C_n$, il existe un diviseur d de n tel que $Z_\sigma = x_d^{n/d}$.

Partie 2 :

Lemme 3.3. *Une permutation σ se décomposant en un produit de d -cycles est d'ordre d .*

Démonstration. Soit $\gamma = (x_1, \dots, x_d)$ un d -cycle de σ avec $d \geq 2$. Pour tout entier $i, 1 \leq i \leq d$ on a :

$$\begin{aligned} \gamma^d(x_i) &= \gamma^d(\gamma^{i-1}(x_1)) && \text{car par définition, } x_i = \gamma^{i-1}(x_1). \\ &= \gamma^{i-1}(\gamma^d(x_1)) \\ &= \gamma^{i-1}(\gamma(\gamma^{d-1}(x_1))) \\ &= \gamma^{i-1}(\gamma(x_d)) && \text{car par définition, } x_d = \gamma^{d-1}(x_1). \\ &= \gamma^{i-1}(x_1) = x_i. \end{aligned}$$

Soit $x \in \mathcal{X}$ et soit γ_x le cycle contenant x . Alors, $\sigma^d(x) = \gamma_x^d(x) = x$ (car γ_x est un d -cycle) donc $\sigma^d = e$. Mais est ce que d est le plus petit entier vérifiant $\sigma^d = e$?

Soit r un entier plus petit que d , nous avons $1 \leq r < d$. Est ce que $\sigma^r = e$?

$$\begin{aligned} \sigma^r(x_1) &= \gamma^r(x_1) = x_{r+1} \quad (\text{par définition}). \\ \Rightarrow \sigma^r(x_1) &\neq x_1 && (\text{car } r \neq 0). \\ \Rightarrow \sigma^r &\neq e \end{aligned}$$

Nous concluons que l'ordre de σ est d . □

Lemme 3.4. *Le nombre d'éléments d'ordre d dans C_n est $\phi(d)$.*

Comme les $\gamma_i, i \in \llbracket 1, n/d \rrbracket$ sont des d -cycles alors d'après le lemme 3.3, σ est d'ordre d . Et d'après le lemme 3.4, il existe $\phi(d)$ permutations d'ordre d . Nous avons par définition :

$$Z_{C_n}(x_1, \dots, x_n) = \frac{1}{n} \sum_{\sigma \in C_n} Z_\sigma(x_1, \dots, x_n). \quad (3.12)$$

Mais comme pour chaque diviseur d de n il existe un ensemble Γ_d des permutations se décomposant en un produit de d -cycles, et pour chaque diviseur d de n il existe un Γ_d . Alors, l'application suivante est une bijection :

$$\begin{aligned} F : \quad \{\Gamma_d \subseteq C_n, d|n\} &\longrightarrow \{d \in \mathbb{N}^* : d|n\} \\ \Gamma_d &\longmapsto d \end{aligned} \quad (3.13)$$

C'est à dire que les $\Gamma_d \subseteq C_n, d|n$ forment une partition de C_n . Nous pouvons donc remplacer la somme sur les $\sigma \in C_n$ dans l'équation 3.12, par une somme sur les

$\Gamma_d :$

$$\begin{aligned}
Z_{C_n}(x_1, \dots, x_n) &= \frac{1}{n} \sum_{\sigma \in C_n} Z_{\sigma}(x_1, \dots, x_n) \\
&= \frac{1}{n} \sum_{\substack{d \in \mathbb{N}^* \\ d|n}} \sum_{\sigma \in \Gamma_d} Z_{\sigma}(x_1, \dots, x_n) \\
&= \frac{1}{n} \sum_{\substack{d \in \mathbb{N}^* \\ d|n}} \phi(d) x_d^{n/d}.
\end{aligned}$$

Conclusion : Le polynôme indicateur de cycles de C_n est :

$$Z_{C_n}(x_1, x_2, \dots, x_n) = \frac{1}{n} \sum_{\substack{d \in \mathbb{N}^* \\ d|n}} \phi(d) x_d^{n/d}.$$

□

Corollaire 3.1. *Si p est un nombre premier alors :*

$$Z_{C_p}(x) = \frac{x_1^p + (p-1)x_p}{p}. \quad (3.14)$$

Démonstration. Si p est un nombre premier alors p est premier avec tous les entiers strictement plus petits que lui, donc $\phi(p) = |\{1, 2, 3, \dots, p-1\}| = p-1$.

En remplaçant dans la formule de [Théorème 3.1](#), on trouve le résultat souhaité. □

3.6 Théorème de dénombrement de Pólya

Le théorème de dénombrement de Pólya porte le nom du mathématicien hongrois George Pólya (1887 – 1985) qui l’a découvert et l’a publié dans son livre [\[7\]](#) en 1937, dans lequel il fait des dénombrements des objets géométriques, des graphes et des composés chimiques.

Cependant, le résultat a été découvert dix ans auparavant par le mathématicien américain John Howard Redfield (1879 – 1944) qui l’a publié pour la première fois dans son article [\[8\]](#).

3.6.1 Poids d’une application

Nous étendons la fonction de poids w pour calculer le poids des applications de $\text{Map}(\mathcal{X}, \mathcal{Y})$.

Définition 3.4. [\[4\]](#) *Le poids d’une fonction noté w est une application :*

$$\begin{aligned}
w : \text{Map}(\mathcal{X}, \mathcal{Y}) &\longrightarrow A \\
\phi &\longmapsto \prod_{x \in X} w(\phi(x))
\end{aligned}$$

Lemme 3.5. [\[4\]](#) *Soient ϕ et ψ deux applications dans $\text{Map}(\mathcal{X}, \mathcal{Y})$ alors :*

$$\phi \sim \psi \implies w(\phi) = w(\psi).$$

Démonstration. Comme ϕ et ψ sont équivalentes, alors il existe $g \in G, \phi = g \cdot \psi$. Calculons $w(\phi)$ en remplaçant ϕ par $g \cdot \psi$:

$$\begin{aligned} w(\phi) &= \prod_{x \in \mathcal{X}} w(\phi(x)) &= \prod_{x \in \mathcal{X}} w((g \cdot \psi)(x)) \\ &= \prod_{x \in \mathcal{X}} w(\psi(g^{-1} \cdot x)) &= \prod_{y \in \mathcal{X}} w(\psi(y)) \\ &= w(\psi) \end{aligned}$$

□

3.6.2 Théorème de Pólya

Dans cette section, nous supposons que $\mathcal{X} = \{1, 2, \dots, n\}$ et que G est un groupe de permutation des éléments de \mathcal{X} (c'est à dire un sous-groupe de \mathfrak{S}_n). G agit donc naturellement sur \mathcal{X} par :

$$\begin{aligned} G \times \mathcal{X} &\longrightarrow \mathcal{X} \\ (\sigma, x) &\longmapsto \sigma \cdot x = \sigma(x) \end{aligned} \tag{3.15}$$

Le résultat donné par le lemme suivant est très important. Commençons par le prouver.

Lemme 3.6. *Soit σ une permutation de G telle que $\sigma = \gamma_1 \gamma_2 \cdots \gamma_k$ soit sa décomposition en produit de cycles.*

$\phi \in \text{Fix}(\sigma)$ si et seulement si ϕ est constante sur chacun des cycles $\gamma_1, \gamma_2, \dots, \gamma_k$.

Démonstration. Condition nécessaire : $\phi \in \text{Fix}(\sigma)$, est-ce-que σ est stable sur $\gamma_1, \dots, \gamma_k$?

Soit $\gamma = (x_1, x_2, \dots, x_d)$ un cycle quelconque de longueur d . Alors, pour un élément $x_i \in \gamma, i \in \llbracket 1, d \rrbracket$:

$$\phi(x_i) = \sigma \cdot \phi(x_i) = \phi \circ \sigma^{-1}(x_i) = \phi(\sigma^{-1}(x_i)) = \phi(\gamma^{-1}(x_i)).$$

Donc :

$$\phi(x_i) = \phi(x_{i-1}) \quad \forall i \in \llbracket 2, d \rrbracket, \quad \phi(x_1) = \phi(x_d).$$

C'est à dire que les $\phi(x_i)$ sont tous identiques donc ϕ est stable sur γ .

Condition suffisante : ϕ est stable sur $\gamma_1, \dots, \gamma_k$, est-ce-que $\phi \in \text{Fix}(\sigma)$?

Soit $x \in \mathcal{X}$ et soit γ le cycle contenant x alors :

$$\sigma \cdot \phi(x) = \phi \circ \sigma^{-1}(x) = \phi \circ \gamma^{-1}(x) = \phi(x).$$

c'est à dire $\phi \in \text{Fix}(\sigma)$.

□

Théorème 3.2. (Pólya, 1937 [7]) Si $w : \mathcal{Y} \rightarrow A$ est une fonction de poids alors le poids de l'ensemble des orbites de $\text{Map}(\mathcal{X}, \mathcal{Y})$ par l'action de G est :

$$\sum_{\mathcal{O} \in \text{Map}(\mathcal{X}, \mathcal{Y})/G} W(\mathcal{O}) = Z_G \left(\sum_{y \in \mathcal{Y}} w(y), \sum_{y \in \mathcal{Y}} w(y)^2, \dots, \sum_{y \in \mathcal{Y}} w(y)^n \right). \quad (3.16)$$

Démonstration. L'idée de la preuve est d'appliquer la formule (3.8) de De Bruijn à l'action du groupe G sur $\text{Map}(\mathcal{X}, \mathcal{Y})$.

Soit $\sigma \in G$, se décomposant en k cycles. $\sigma = \gamma_1 \cdot \gamma_2 \cdots \gamma_k$.

Rappelons que $\text{Fix}(\sigma) = \{\phi \in \text{Map}(\mathcal{X}, \mathcal{Y}) : \sigma \cdot \phi = \phi\}$ et commençons par calculer son poids. Nous avons, par définition du poids d'un ensemble :

$$w(\text{Fix}(\sigma)) = \sum_{\phi \in \text{Fix}(\sigma)} w(\phi) \quad (3.17)$$

Au lieu d'une somme sur $\phi \in \text{Fix}(\sigma)$, nous voulons des sommes sur les $y \in \mathcal{Y}$ pour $i \in \llbracket 1, k \rrbracket$. Si $\text{Fix}(\sigma) \neq \emptyset$, alors d'après le lemme 3.6, les applications appartenant au $\text{Fix}(\sigma)$ sont constantes sur chacun des k cycles, donc on peut définir une application qui associe à chaque application $\phi \in \text{Fix}(\sigma)$ k valeurs dans \mathcal{Y} , soit :

$$\begin{aligned} F : \text{Fix}(\sigma) &\longrightarrow \mathcal{Y}^k \\ \phi &\longmapsto (\phi(\gamma_1), \phi(\gamma_2), \dots, \phi(\gamma_k)). \end{aligned} \quad (3.18)$$

Lemme 3.7. L'application F est une bijection.

Démonstration. Supposons sans perte de généralité que :

$\mathcal{X} = \{1, 2, \dots, n\}$ est l'ensemble des éléments constituant un objet.

\mathcal{Y} est l'ensemble de couleurs disponibles.

G est le groupe de symétrie de l'objet.

$\text{Map}(\mathcal{X}, \mathcal{Y})$ est l'ensemble de colorations de l'objet.

$\text{Fix}(\sigma)$ est l'ensemble de colorations fixes par σ . D'après le lemme 3.6, les éléments appartenant à un même cycle sont de même couleur. Pour chacun des k cycles, il existe $\binom{|\mathcal{Y}|}{1} = |\mathcal{Y}|$ choix de couleur. Donc $|\text{Fix}(\sigma)| = |\mathcal{Y}|^k$. Reste à prouver que F est injective.

Chaque élément de l'ensemble \mathcal{Y}^k est de la forme $(\phi(\gamma_1), \phi(\gamma_2), \dots, \phi(\gamma_k))$ telle que $\phi(\gamma_1)$ est la couleur de γ_1 , $\phi(\gamma_2)$ est la couleur de γ_2 , ... et $\phi(\gamma_k)$ est la couleur de γ_k . Si γ_{i_x} est le cycle contenant x , alors l'application suivante :

$$\begin{aligned} \phi : \mathcal{X} &\longrightarrow \mathcal{Y} \\ x &\longmapsto \phi(\gamma_{i_x}). \end{aligned} \quad (3.19)$$

est une coloration utilisant k couleurs et $F(\phi) = (\phi(\gamma_1), \phi(\gamma_2), \dots, \phi(\gamma_k))$. Donc F est injective (au moins un antécédent pour chaque image). \square

Posons $y_i = \phi(\gamma_i)$ pour $i \in \llbracket 1, k \rrbracket$. Nous avons $F(\phi) = (y_1, y_2, \dots, y_k)$, et comme F est une bijection (lemme 3.7) alors $\phi = F^{-1}(y_1, y_2, \dots, y_k)$. En remplaçant la

valeur de ϕ dans l'équation (3.17) on trouve :

$$w(Fix(\sigma)) = \sum_{y_1, y_2, \dots, y_k \in \mathcal{Y}} w(F^{-1}(y_1, y_2, \dots, y_k)) \quad (3.20)$$

D'autre part, d'après le lemme 3.6, l'application ϕ est constante sur chaque cycle γ_i , $i \in \llbracket 1, k \rrbracket$ donc pour tout $j \in \gamma_i$, $\phi(j)$ est une constante soit $y_i \in \mathcal{Y}$. On peut donc écrire $\phi(\gamma_i) = y_i$.

Notation 3.2. La longueur d'un cycle γ est noté $|\gamma|$.

$$\begin{aligned} w(\phi) &= \prod_{x \in \mathcal{X}} w(\phi(x)) \\ &= \prod_{i=1}^k w(\phi(\gamma_i))^{|\gamma_i|} \quad \text{car les } \gamma_i \text{ forment une partition de } \mathcal{X} \\ &= \prod_{i=1}^k w(y_i)^{|\gamma_i|}. \end{aligned}$$

Et comme $w(\phi) = w(F^{-1}(y_1, y_2, \dots, y_k))$, alors nous avons :

$$w(F^{-1}(y_1, y_2, \dots, y_k)) = \prod_{i=1}^k w(y_i)^{|\gamma_i|} \quad (3.21)$$

Remplaçons cette valeur dans l'équation (3.20), on trouve :

$$w(Fix(\sigma)) = \sum_{y_1, y_2, \dots, y_k \in \mathcal{Y}} \prod_{i=1}^k w(y_i)^{|\gamma_i|}. \quad (3.22)$$

Développons la somme et le produit,

$$w(Fix(\sigma)) = \sum_{y_1 \in \mathcal{Y}} \sum_{y_2 \in \mathcal{Y}} \cdots \sum_{y_k \in \mathcal{Y}} w(y_1)^{|\gamma_1|} \cdot w(y_2)^{|\gamma_2|} \cdots w(y_{k-1})^{|\gamma_{k-1}|} \cdot w(y_k)^{|\gamma_k|}.$$

Lemme 3.8. Étant donnés n ensembles X_i et n fonctions $f_i : X_i \rightarrow f_i(X_i)$, $i \in \llbracket 1, n \rrbracket$, $n \geq 2$. Alors :

$$\sum_{x_1 \in X_1} \cdots \sum_{x_n \in X_n} f_1(x_1) \cdots f_n(x_n) = \left(\sum_{x_1 \in X_1} f_1(x_1) \right) \cdots \left(\sum_{x_n \in X_n} f_n(x_n) \right). \quad (3.23)$$

Démonstration. Pour $n = 2$, le résultat est vérifié. En effet, posons $S = \sum_{x_2 \in X_2} f_2(x_2)$.

Alors :

$$\begin{aligned} \sum_{x_1 \in X_1} \sum_{x_2 \in X_2} f_1(x_1) f_2(x_2) &= \sum_{x_1 \in X_1} \left(f_1(x_1) \sum_{x_2 \in X_2} f_2(x_2) \right) \\ &= \sum_{x_1 \in X_1} \left(f_1(x_1) S \right) \\ &= S \sum_{x_1 \in X_1} f_1(x_1) \\ &= \left(\sum_{x_1 \in X_1} f_1(x_1) \right) \left(\sum_{x_2 \in X_2} f_2(x_2) \right). \end{aligned}$$

Supposons maintenant par récurrence que le résultat de l'équation (3.23) est vrai jusqu'à l'ordre $n - 1$. C'est à dire :

$$\sum_{x_1 \in X_1} \cdots \sum_{x_{n-1} \in X_{n-1}} f_1(x_1) \cdots f_{n-1}(x_{n-1}) = \left(\sum_{x_1 \in X_1} f_1(x_1) \right) \cdots \left(\sum_{x_{n-1} \in X_{n-1}} f_{n-1}(x_{n-1}) \right)$$

et prouvons qu'il est vrai à l'ordre n .

$$\sum_{x_1 \in X_1} \cdots \sum_{x_n \in X_n} f_1(x_1) \cdots f_n(x_n) = \sum_{x_1 \in X_1} \cdots \sum_{x_{n-1} \in X_{n-1}} f_1(x_1) \cdots f_{n-1}(x_{n-1}) \left(\sum_{x_n \in X_n} f_n(x_n) \right)$$

Et par hypothèse de récurrence, ceci est égal à :

$$\left(\sum_{x_1 \in X_1} f_1(x_1) \right) \cdots \left(\sum_{x_{n-1} \in X_{n-1}} f_{n-1}(x_{n-1}) \right) \left(\sum_{x_n \in X_n} f_n(x_n) \right).$$

□

D'après le lemme 3.8, la somme de produits est égale au produit des sommes, donc :

$$\begin{aligned} w(Fix(\sigma)) &= \left(\sum_{y_1 \in \mathcal{Y}} w(y_1)^{|\gamma_1|} \right) \left(\sum_{y_2 \in \mathcal{Y}} w(y_2)^{|\gamma_2|} \right) \cdots \left(\sum_{y_k \in \mathcal{Y}} w(y_k)^{|\gamma_k|} \right) \\ &= \left(\sum_{y \in \mathcal{Y}} w(y)^{|\gamma_1|} \right) \left(\sum_{y \in \mathcal{Y}} w(y)^{|\gamma_2|} \right) \cdots \left(\sum_{y \in \mathcal{Y}} w(y)^{|\gamma_k|} \right). \end{aligned}$$

Les $|\gamma_1|, |\gamma_2|, \dots, |\gamma_k|$ prennent leurs valeurs dans $\llbracket 1, n \rrbracket$ et comme $c_l(\sigma)$, $l \in \llbracket 1, n \rrbracket$ est le nombre de cycles de longueur de l , alors on peut écrire :

$$\begin{aligned} w(Fix(\sigma)) &= \left(\sum_{y \in \mathcal{Y}} w(y) \right)^{c_1(\sigma)} \left(\sum_{y \in \mathcal{Y}} w(y)^2 \right)^{c_2(\sigma)} \cdots \left(\sum_{y \in \mathcal{Y}} w(y)^n \right)^{c_n(\sigma)} \\ &= Z_\sigma \left(\sum_{y \in \mathcal{Y}} w(y), \sum_{y \in \mathcal{Y}} w(y)^2, \dots, \sum_{y \in \mathcal{Y}} w(y)^n \right) \end{aligned}$$

En appliquant la formule de De Bruijn de l'équation (3.8), on trouve :

$$\begin{aligned} \sum_{\mathcal{O} \in Map(\mathcal{X}, \mathcal{Y})/_G} W(\mathcal{O}) &= \frac{1}{|G|} \sum_{\sigma \in G} w(Fix(\sigma)) \\ &= \frac{1}{|G|} \sum_{\sigma \in G} Z_\sigma \left(\sum_{y \in \mathcal{Y}} w(y), \sum_{y \in \mathcal{Y}} w(y)^2, \dots, \sum_{y \in \mathcal{Y}} w(y)^n \right) \\ &= Z_G \left(\sum_{y \in \mathcal{Y}} w(y), \sum_{y \in \mathcal{Y}} w(y)^2, \dots, \sum_{y \in \mathcal{Y}} w(y)^n \right). \end{aligned}$$

□

Le corollaire suivant est une conséquence de la preuve du théorème de Pólya. Il nous aide à calculer $|Fix(g)|$:

Corollaire 3.2. *soit $\sigma \in G$ se décomposant en un produit de k cycles. Alors,*

$$|Fix(\sigma)| = \begin{cases} |\mathcal{Y}|^k & \text{si } Fix(\sigma) \neq \emptyset \\ 0 & \text{sinon.} \end{cases}$$

Démonstration. Si $Fix(\sigma) \neq \emptyset$ alors l'application F donnée par la formule (3.18) est correctement définie. Et d'après le lemme 3.7, elle est bijective, on en déduit que $|Fix(\sigma)| = |\mathcal{Y}|^k$. \square

Corollaire 3.3. *Le nombre d'orbites de $Map(\mathcal{X}, \mathcal{Y})$ par l'action de G est :*

$$|Map(\mathcal{X}, \mathcal{Y})/G| = Z_G(|\mathcal{Y}|, |\mathcal{Y}|, \dots, |\mathcal{Y}|). \quad (3.24)$$

Démonstration. Soit la fonction de poids w suivante :

$$\begin{aligned} w : \mathcal{Y} &\longrightarrow \mathbb{Z} \\ y &\longmapsto 1. \end{aligned}$$

Alors, si \mathcal{O} est une orbite dans $Map(\mathcal{X}, \mathcal{Y})/G$ alors $W(\mathcal{O}) = w(\phi)$ pour une fonction ϕ quelconque dans \mathcal{O} , car le poids moyen d'un ensemble d'éléments de même poids est le poids d'un élément de l'ensemble. Et comme

$$w(\phi) = \prod_{x \in \mathcal{X}} w(\phi(x)) = \prod_{x \in \mathcal{X}} 1 = 1 \quad (\text{car } \phi(x) \in \mathcal{Y}),$$

alors $W(\mathcal{O}) = 1$.

L'équation (3.16) devient :

$$\begin{aligned} \sum_{\mathcal{O} \in Map(\mathcal{X}, \mathcal{Y})/G} 1 &= Z_G\left(\sum_{y \in \mathcal{Y}} 1, \sum_{y \in \mathcal{Y}} 1^2, \dots, \sum_{y \in \mathcal{Y}} 1^n\right) \\ \implies |Map(\mathcal{X}, \mathcal{Y})/G| &= Z_G\left(\sum_{y \in \mathcal{Y}} 1, \sum_{y \in \mathcal{Y}} 1, \dots, \sum_{y \in \mathcal{Y}} 1\right) \\ \implies |Map(\mathcal{X}, \mathcal{Y})/G| &= Z_G(|\mathcal{Y}|, |\mathcal{Y}|, \dots, |\mathcal{Y}|) \end{aligned}$$

\square

3.7 Exemples : Coloration de colliers

Nous allons reprendre les exemples calculés à la main dans le paragraphe 2.3, puis avec le lemme de Burnside dans le paragraphe 3.3 et nous verrons que les calculs sont plus rapides avec le théorème de Pólya.

3.7.1 Application 1 : 3 perles et 2 couleurs

Rappelons que le groupe sous-jacent est le groupe cyclique d'ordre 3 : $C_3 = \{123, 231, 312\}$.

Soit aussi $\{r, b\}$ l'ensemble des couleurs rouge et bleu.

Soient $\mathcal{X} = \{1, 2, 3\}$ l'ensemble de perles, $\mathcal{Y} = \{r, b\}$ l'ensemble de couleurs rouge et bleu, donc $Map(\mathcal{X}, \mathcal{Y})$ est l'ensemble de toutes les colorations possibles.

Comme 3 est un nombre premier, alors le polynôme indicateur de cycles de C_3 est donné par le lemme 3.1, ainsi,

$$Z_{C_3}(x_1, x_2, x_3) = \frac{x_1^3 + 2x_3}{3}.$$

D'après le théorème de Pólya (formule (3.24)) le nombre l'orbites est donné par :

$$\begin{aligned} \left| Map(\mathcal{X}, \mathcal{Y}) / C_3 \right| &= Z_{C_3}(|\mathcal{Y}|, |\mathcal{Y}|, |\mathcal{Y}|) = Z_{C_3}(2, 2, 2) \\ &= \frac{2^3 + 2 \cdot 2}{3} = \frac{12}{3} = 4. \end{aligned}$$

3.7.2 Application 2 : 5 perles et 2 couleurs

Le groupe cyclique d'ordre 5 est $C_5 = \{12345, 23451, 34512, 45123, 51234\}$. Les couleurs sont rouge et bleu $\mathcal{Y} = \{r, b\}$. L'ensemble de perles est $\mathcal{X} = \{1, 2, 3, 4, 5\}$, et l'ensemble des couleurs rouge et bleu est $\mathcal{Y} = \{r, b\}$. L'ensemble de toutes les colorations possible est donné donc par $Map(\mathcal{X}, \mathcal{Y})$.

Comme 5 est un nombre premier, alors le polynôme indicateur de cycles de C_5 est donné par le lemme 3.1, nous avons :

$$Z_{C_5}(x_1, x_2, x_3, x_4, x_5) = \frac{x_1^5 + 4x_5}{5}.$$

D'après le théorème de Pólya (formule (3.24)), le nombre l'orbites est donné par :

$$\begin{aligned} \left| Map(\mathcal{X}, \mathcal{Y}) / C_5 \right| &= Z_{C_5}(|\mathcal{Y}|, |\mathcal{Y}|, |\mathcal{Y}|, |\mathcal{Y}|, |\mathcal{Y}|) = Z_{C_5}(2, 2, 2, 2, 2) \\ &= \frac{2^5 + 4 \cdot 2}{5} = \frac{40}{5} = 8. \end{aligned}$$

3.7.3 Application 3 : 5 perles et 3 couleurs

L'ensemble de perles est $\mathcal{X} = \{1, 2, 3, 4, 5\}$, et l'ensemble des couleurs rouge, bleu, jaune est $\mathcal{Y} = \{r, b, j\}$. L'ensemble de toutes les colorations possible est donné donc par $Map(\mathcal{X}, \mathcal{Y})$.

Comme dans l'exemple précédent, le polynôme indicateur de cycles de C_5 est donné par :

$$Z_{C_5}(x_1, x_2, x_3, x_4, x_5) = \frac{x_1^5 + 4x_5}{5}.$$

D'après le théorème de Pólya (formule (3.24)) le nombre l'orbites est donné par :

$$\begin{aligned} \left| Map(\mathcal{X}, \mathcal{Y}) / C_5 \right| &= Z_{C_5}(|\mathcal{Y}|, |\mathcal{Y}|, |\mathcal{Y}|, |\mathcal{Y}|, |\mathcal{Y}|) = Z_{C_5}(3, 3, 3, 3, 3) \\ &= \frac{3^5 + 4 \cdot 3}{5} = \frac{243 + 12}{5} = \frac{255}{5} = 51. \end{aligned}$$

3.8 Théorème de Pólya appliqué aux problèmes de coloration : Version pondérée

Étant donné un objet constitué de n éléments à colorier (ex. collier constitué de n perles, cube constitué de 6 faces, ...). \mathcal{X} est l'ensemble de ces n éléments, $\mathcal{Y} = \{y_1, y_2, \dots, y_k\}$ est l'ensemble de k couleurs disponibles, et $\text{Map}(\mathcal{X}, \mathcal{Y})$ est l'ensemble de k^n colorations.

Question 3.1. *de combien de façons réellement différentes pouvons nous colorier les éléments de \mathcal{X} avec les couleurs de \mathcal{Y} ?*

Question 3.2. *de combien de façons réellement différentes pouvons nous colorier les éléments de \mathcal{X} avec les couleurs de \mathcal{Y} telles que n_1 éléments soient de couleur y_1 , n_2 éléments soient de couleur y_2 , ... et n_k éléments soient de couleur y_k ?*

La réponse à la première question est le nombre d'orbites par l'action de G . Il suffit d'appliquer, comme dans le paragraphe précédent, le corollaire 3.3. Mais la réponse à la deuxième question revient à compter le nombre d'orbites avec une certaine contrainte. La réponse est dans le polynôme indicateur de couleurs de G .

Vocabulaire

L'**indicateur d'une coloration** ϕ noté ind_ϕ est le monôme $y_1^{n_1} y_2^{n_2} \dots y_k^{n_k}$, où

$$n_i = |\phi^{-1}(\{y_i\})| \text{ pour tout } i = 1, \dots, k,$$

qui est le nombre d'éléments de couleur y_i par la coloration ϕ . L'**indicateur d'une orbite** \mathcal{O} noté $\text{Ind}_{\mathcal{O}}$ est égal à l'indicateur d'une coloration de cette orbite. L'**indicateur de coloration du groupe** G noté $\text{Ind}_G(y_1, y_2, \dots, y_k)$ est un polynôme égal à la somme des indicateurs des orbites sous l'action de G .

Application du théorème de Pólya (version pondérée)

La fonction de poids d'une couleur est :

$$\begin{aligned} w : \mathcal{Y} &\longrightarrow \mathbb{Z}[y_1, y_2, \dots, y_k] \\ y &\longmapsto y \end{aligned}$$

La fonction de poids d'une coloration est :

$$\begin{aligned} w : \text{Map}(\mathcal{X}, \mathcal{Y}) &\longrightarrow \mathbb{Z}[y_1, y_2, \dots, y_k] \\ \phi &\longmapsto \prod_{x \in \mathcal{X}} w(\phi(x)) = \prod_{y \in \mathcal{Y}} w(y)^{|\phi^{-1}(\{y\})|} = \prod_{y \in \mathcal{Y}} y^{|\phi^{-1}(\{y\})|} = \text{ind}_\phi \end{aligned}$$

Nous avons donc,

$$\sum_{\mathcal{O} \in \text{Map}(\mathcal{X}, \mathcal{Y})/G} W(\mathcal{O}) = \sum_{\mathcal{O} \in \text{Map}(\mathcal{X}, \mathcal{Y})/G} \text{Ind}_{\mathcal{O}} = \text{Ind}_G(y_1, y_2, \dots, y_k). \quad (3.25)$$

Mais d'après le théorème de Pólya, (équation 3.16), cette valeur est égale à :

$$\begin{aligned} \sum_{\mathcal{O} \in \text{Map}(\mathcal{X}, \mathcal{Y})/G} W(\mathcal{O}) &= Z_G \left(\sum_{y \in \mathcal{Y}} w(y), \sum_{y \in \mathcal{Y}} w(y)^2, \dots, \sum_{y \in \mathcal{Y}} w(y)^n \right) \\ &= Z_G \left(\sum_{y \in \mathcal{Y}} y, \sum_{y \in \mathcal{Y}} y^2, \dots, \sum_{y \in \mathcal{Y}} y^n \right). \end{aligned}$$

D'où le résultat suivant :

Corollaire 3.4.

$$\text{Ind}_G(y_1, y_2, \dots, y_k) = Z_G \left(\sum_{y \in \mathcal{Y}} y, \sum_{y \in \mathcal{Y}} y^2, \dots, \sum_{y \in \mathcal{Y}} y^n \right) \quad (3.26)$$

Ce corollaire nous permet de calculer le polynôme $\text{Ind}_G(y_1, y_2, \dots, y_k)$ qui nous permet de répondre à la question 3.2, vu que le nombre de colorations ϕ telles que n_i éléments soient de couleurs y_i pour $i = 1, \dots, k$ est le coefficient du monôme $\text{ind}_\phi = y_1^{n_1} y_2^{n_2} \dots y_k^{n_k}$ dans le polynôme $\text{Ind}_G(y_1, y_2, \dots, y_k)$.

3.8.1 Coloration de collier

3 perles : une rouge et deux bleues

Comme : $Z_{C_3}(x_1, x_2, x_3) = \frac{x_1^3 + 2x_3}{3}$. Alors

$$\begin{aligned} \text{Ind}_{C_3}(r, b) &= Z_{C_3}(r + b, r^2 + b^2, r^3 + b^3) = \frac{(r + b)^3 + 2(r^3 + b^3)}{3} \\ &= \frac{r^3 + 3r^2b + 3rb^2 + b^3 + 2r^3 + 2b^3}{3}. \end{aligned}$$

Le coefficient de rb^2 dans $\text{Ind}_{C_3}(r, b)$ est 1. Donc il existe une unique coloration du collier avec une perle rouge et deux perles bleues.

5 perles : trois rouge et deux bleues

Comme $Z_{C_5}(x_1, x_2, x_3, x_4, x_5) = \frac{x_1^5 + 4x_5}{5}$. Alors :

$$\begin{aligned} \text{Ind}_{C_5}(r, b) &= Z_{C_5}(r + b, r^2 + b^2, r^3 + b^3, r^4 + b^4, r^5 + b^5) = \frac{(r + b)^5 + 4(r^5 + b^5)}{5} \\ &= \frac{r^5 + 5r^4b + 10r^3b^2 + 10r^2b^3 + 5rb^4 + b^5 + 4r^5 + 4b^5}{5}. \end{aligned}$$

Le coefficient de r^3b^2 est 2 donc il existe seulement 2 colorations avec trois perles rouges et deux perles bleues.

5 perles : deux rouges, deux bleues et une jaune

$$\begin{aligned} \text{Ind}_{C_5}(r, b, j) &= Z_{C_5}(r + b + j, r^2 + b^2 + j^2, r^3 + b^3 + j^3, r^4 + b^4 + j^4, r^5 + b^5 + j^5) \\ &= \frac{(r + b + j)^5 + 4(r^5 + b^5 + j^5)}{5}. \end{aligned}$$

Le développement du multinôme $(r + b + j)^5$ est donné par :

$$(r + b + j)^5 = \sum_{x+y+z=5} \binom{5}{x, y, z} r^x b^y j^z.$$

Le coefficient de $r^2 b^2 j$ dans le multinôme est $\binom{5}{2, 2, 1} = \frac{5!}{2!2!1!} = \frac{2 \cdot 3 \cdot 4 \cdot 5}{4} = 30$.

Donc le coefficient dans le polynôme $Ind_{C_5}(r, b, j)$ est $\frac{30}{5} = 6$.

Il existe donc six colorations de ce type.

4 Classes de conjugaison et produit semi-direct

Le lemme de Burnside dit que le nombre de colorations réellement différentes est donné par la moyenne des colorations fixes, mais il ne dit pas comment les calculer. Le théorème de Pólya dit que ce nombre est égal à l'évaluation du polynôme indicateur de cycles par le nombre de couleurs. Mais le calcul du polynôme peut être très complexe.

Ce chapitre, assez court, présentera des outils très utiles, voire essentiels, pour pouvoir appliquer le lemme de Burnside ou le théorème de Pólya.

Supposons tout au long du chapitre, que G soit un groupe fini d'élément neutre e , et que H soit un sous-groupe quelconque de G .

4.1 Classes de conjugaison

Une classe de conjugaison est un cas particulier d'orbite.

Définition 4.1. La classe de conjugaison d'un élément $h \in G$, notée C_h , est l'orbite de h sous l'action de G sur lui même par conjugaison. C'est à dire :

$$C_h = \{g \cdot h \cdot g^{-1} : g \in G\}.$$

Deux éléments appartenant à une même classe de conjugaison sont appelés conjugués, ou l'un est le conjugué de l'autre.

L'intérêt des classes de conjugaison, est que dans certains problèmes, l'étude du groupe peut se ramener à l'étude de ses classes de conjugaison, vu que les éléments conjugués partagent des propriétés communes. Et donc réduire considérablement la complexité du problème.

Lemme 4.1. Si G est un groupe de permutations de $\mathcal{X} = \{1, 2, \dots, n\}$, alors deux permutations de G sont conjuguées si et seulement si elles ont le même type.

Démonstration. Soit $\sigma \in G$ se décomposant en m cycles $\gamma_1, \gamma_2, \dots, \gamma_m$, et soit $\tau \in G$. Comme les cycles sont disjoints, alors :

$$\tau\sigma\tau^{-1} = \tau\gamma_1\gamma_2 \cdots \gamma_m\tau^{-1} = (\tau\gamma_1\tau^{-1})(\tau\gamma_2\tau^{-1}) \cdots (\tau\gamma_m\tau^{-1}).$$

Soit $\gamma \in \{\gamma_1, \gamma_2, \dots, \gamma_m\}$, un k -cycle quelconque avec $\gamma = (x_1, \dots, x_k)$. Il s'agit de prouver maintenant que $\tau\gamma\tau^{-1}$ est aussi un k -cycle.

Calculer $\tau\gamma\tau^{-1}(x)$ pour tout $x \in \mathcal{X}$, est équivalent à calculer $\tau\gamma\tau^{-1}(\tau(x))$ pour tout $x \in \mathcal{X}$. Nous avons :

$$\tau\gamma\tau^{-1}(\tau(x)) = \tau\gamma\tau^{-1}\tau(x) = \tau\gamma(x).$$

Si $x \in \gamma$: alors il existe $i \in \llbracket 1, k \rrbracket$ tel que $x_i = x$.

$$\tau\gamma(x) = \tau\gamma(x_i) = \begin{cases} \tau(x_{i+1}) & \text{si } i < k, \\ \tau(x_1) & \text{si } i = k. \end{cases}$$

Si $x \notin \gamma$: alors $\tau\gamma(x) = \tau(x)$ donc $\tau(x)$ est fixe par $\tau\gamma\tau^{-1}$

On en déduit que $\tau\gamma\tau^{-1} = (\tau(x_1), \tau(x_2), \dots, \tau(x_k))$ qui est un k -cycle. \square

Nous allons utiliser ce résultat dans le [chapitre 5](#) pour partitionner les groupes de permutations en classes de conjugaison. Puis appliquer le lemme de Burnside ou le théorème de Pólya sur ces classes.

Pour simplifier l'écriture, nous utiliserons la notation suivante :

Notation 4.1. Si C est une classe de conjugaison, on note :

$$|Fix(C)| = \sum_{\sigma \in C} |Fix(\sigma)|.$$

4.2 Sous-groupe normal

Maintenant que nous connaissons les classes de conjugaison, nous pouvons définir le sous-groupe normal. Nous avons vu dans le [chapitre 2](#) que tout groupe agit sur lui-même par conjugaison. L'action par conjugaison de G sur lui-même est :

$$\begin{aligned} G \times G &\longrightarrow G \\ (g, h) &\longmapsto ghg^{-1}. \end{aligned}$$

Soit N un sous-groupe de G .

Définition 4.2. On dit que N est normal dans G et on écrit $N \triangleleft G$ si et seulement si N est stable par l'action de conjugaison de G sur lui-même. Autrement dit, si et seulement si pour tout $n \in N$ et pour tout $g \in G$, alors $gng^{-1} \in N$.

Exemple 4.1. Le sous-groupe $\{e\}$ de G réduit à l'élément neutre est normal. En effet, pour tout $g \in G$:

$$geg^{-1} = gg^{-1} = e \in \{e\}.$$

Exemple 4.2. Si G est abélien, alors tous ses sous-groupes sont normaux. En effet, si N est un sous-groupe quelconque de G , alors pour tout $g \in G$ et pour tout $n \in N$:

$$gng^{-1} = gg^{-1}n = en = n \in N.$$

Définition 4.3 (Indice de sous-groupe). L'indice de H dans G noté $[G : H]$ est le nombre de classes à gauche (resp. à droite) suivant H . Autrement dit,

$$[G : H] = |\{xH, x \in G\}| = |\{Hx, x \in G\}|.$$

Où $xH = \{xh, h \in H\}$ (resp. $Hx = \{hx, h \in H\}$) est appelée la classe à gauche (resp. à droite) de x modulo H ou suivant H .

proposition 4.1. Tout sous-groupe de G d'indice 2 est normal.

Démonstration. Par définition de l'indice, il existe deux classes à gauche modulo H , soient H et gH , et deux classes à droite modulo H , soient H et Hg , pour un g quelconque dans G . Autrement dit, $\{H, gH\}$ et $\{H, Hg\}$ sont deux partitions de G donc :

$$gH = Hg \iff gHg^{-1} = H \iff ghg^{-1} \in H \text{ pour tout } h \text{ dans } H.$$

On en déduit que H est normal dans G . □

Théorème 4.1 (De Lagrange). L'ordre de H divise celui de G .

Démonstration. Il est facile de prouver que toutes les classes à gauche modulo H sont de cardinalité $|H|$, et qu'elles forment une partition de G . En plus, par définition, leur nombre est $[G : H]$. On en déduit que :

$$|G| = |H| \times [G : H].$$

□

La preuve du théorème de Lagrange donne le résultat suivant :

Corollaire 4.1. L'indice d'un sous-groupe H de G est donné par $[G : H] = \frac{|G|}{|H|}$.

4.2.1 Normalité dans le groupe diedral

Rappelons que le groupe diedral D_n est le groupe des isométries d'un polygone régulier à n sommets, $n \geq 3$. (revoir l'exemple 1.2 du chapitre 1 pour plus de détails).

proposition 4.2 (Normalité de C_n). Le groupe cyclique C_n d'ordre n est un sous-groupe normal dans le groupe diedral D_n d'ordre $2n$.

Démonstration. Il est facile de voir que C_n est un sous-groupe de D_n . Il suffit de prouver qu'il est normal. D'après le corollaire 4.1, $[D_n : C_n] = \frac{|D_n|}{|C_n|} = \frac{2n}{n} = 2$. Donc C_n est d'indice 2 dans D_n . Et d'après la proposition 4.1, C_n est normal dans D_n . □

proposition 4.3 (Contre exemple). Dans D_n , le sous-groupe $C_2 = \{id, s\}$ n'est pas normal.

Démonstration. Soit $r \in D_n$ la rotation d'angle $2\pi/n$, et s la réflexion par rapport à l'axe montré sur la figure 4.1. Cette figure montre l'effet de l'opération $r \circ s \circ r^{-1}$ sur un polygone quelconque à n sommets (même si sur la figure il a la forme d'un hexagone mais il ne l'est pas forcément).

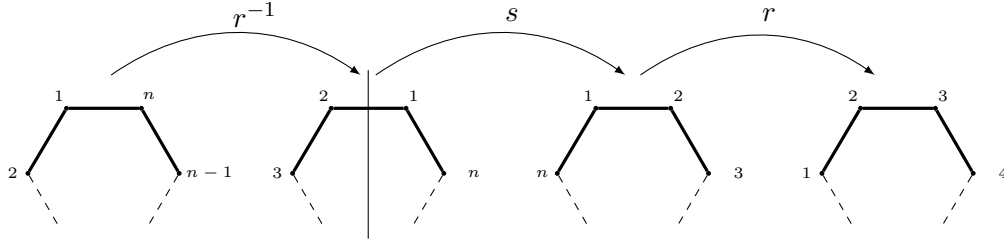


FIGURE 4.1 – L'opération $r \circ s \circ r^{-1}$ sur une partie d'un polygone à n sommets.

La figure suivante montre l'effet de l'opération s sur le même polygone :

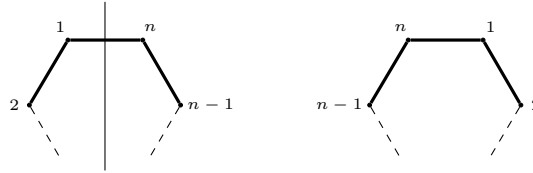


FIGURE 4.2 – La réflexion s sur la même partie du polygone précédent.

Les illustrations montrent que $r \circ s \circ r^{-1} \neq s$ et $r \circ s \circ r^{-1} \neq id$ donc $r \circ s \circ r^{-1} \notin C_2$. On déduit que C_2 n'est pas normal dans D_n . \square

4.3 Produit semi-direct

Définition 4.4 (Produit semi-direct). On dit que G est le produit semi-direct de H et d'un sous-groupe normal N , si et seulement si pour tout $g \in G$, il existe une unique paire $(n, h) \in N \times H$ telle que $g = nh$. On écrit $G = N \rtimes H$ ou $G = H \ltimes N$.¹

proposition 4.4. Le groupe diedral d'ordre $2n$ est le produit semi-direct du groupe cyclique C_n et le groupe d'ordre 2 C_2 .

Démonstration. D'après la proposition 4.2, C_n est un sous-groupe normal dans D_n . Posons :

$$C_n = \{id, r, r^2, \dots, r^{n-1}\} \text{ et } C_2 = \{id, s\}.$$

On sait que les éléments du groupe diedral D_n sont les éléments de C_n et leurs composées avec la réflexion s . Prouvons que pour tout $\sigma \in D_n$, il existe une paire unique $(h, n) \in C_2 \times C_n$ vérifiant $\sigma = h \circ n$.

Si $\sigma \in C_n$: la paire (id, σ) vérifie la condition car $id \in C_2$. Elle est unique car σ est unique dans C_n .

1. Les symboles \ltimes et \rtimes sont différents, le coté du sous-groupe normal est ouvert.

Si $\sigma \notin C_n$: alors il existe $i \in \{1, 2, \dots, n-1\}$ tel que $\sigma = s \circ r^i$. La paire est donc (s, r^i) . Cette paire est unique car les r^i sont tous différents.

Donc D_n est le produit semi-direct du groupe normal C_n et de C_2 . \square

Exemple 4.3. Pour $n = 4$, nous avons présenté le groupe diédral D_4 dans l'exemple 1.2 du chapitre 1. La table suivante donne les éléments de D_4 et la paire correspondante :

$\sigma \in D_4$	id	r	r^2	r^3	s	$s \circ r$	$s \circ r^2$	$s \circ r^3$
$(h, n) \in C_2 \times C_4$	(id, id)	(id, r)	(id, r^2)	(id, r^3)	(s, id)	(s, r)	(s, r^2)	(s, r^3)
Permutation	1234	2341	3412	4123	1432	4321	3214	2143

TABLE 4.1 – Les éléments de D_4 .

5 Applications

Les exemples vus dans les chapitres précédents étaient des exemples simples sur des colliers avec 3 et 5 perles. Ce chapitre présentera des exemples plus élaborés. Nous ferons des dénombrements en appliquant le lemme de Burnside et le théorème de Pólya. Nous verrons que les deux méthodes sont étroitement liées dans le cas des colorations sans contraintes. Mais en ajoutant des contraintes comme, par exemple, imposer qu'un certain nombre d'éléments ait une certaine couleur, le plus pratique est d'utiliser le polynôme indicateur de couleurs.

Nous utiliserons les outils présentés dans le [chapitre 4](#). À savoir, les classes de conjugaison et le produit semi-direct.

5.1 Jetons transparents hexagonaux

Le jeton

Un jeton transparent hexagonal est un hexagone transparent composé de six triangles équilatéraux dont chacun est de couleur différente. On travaillera donc avec un ensemble de six couleurs et on notera \mathcal{C} l'ensemble de colorations possibles.

Le groupe de symétrie

Comme le jeton est transparent, alors il possède, en plus des rotations, des réflexions. Le groupe de symétrie est donc le groupe diédral de l'hexagone D_6 . Il est d'ordre 12.

Le résultat du calcul à la main des rotations et des réflexions de l'hexagone est donné par la table [5.1](#) suivante :

Rotation	Cycles	Monôme	Réflexion	Cycles	Monôme
id	$(1)(2)(3)(4)(5)(6)$	x_1^6	s	$(1, 2)(3, 6)(4, 5)$	x_2^3
r	$(1, 2, 3, 4, 5, 6)$	x_6	$s \circ r$	$(1)(2, 6)(3, 5)(4)$	$x_1^2 x_2^2$
r^2	$(1, 3, 5)(2, 4, 6)$	x_3^2	$s \circ r^2$	$(1, 6)(2, 5)(3, 4)$	x_2^3
r^3	$(1, 4)(2, 5)(3, 6)$	x_2^3	$s \circ r^3$	$(1, 5)(2, 4)(3)(6)$	$x_1^2 x_2^2$
r^4	$(1, 5, 3)(2, 6, 4)$	x_3^2	$s \circ r^4$	$(1, 4)(2, 3)(5, 6)$	x_2^3
r^5	$(1, 6, 5, 4, 3, 2)$	x_6	$s \circ r^5$	$(1, 3)(2)(4, 6)(5)$	$x_1^2 x_2^2$

TABLE 5.1 – Les douze éléments de D_6 .

Exemples

La figure 5.1 montre quatre jetons dont les colorations se dérivent de celle du jeton le plus à gauche en appliquant les opérations r , $s \circ r^3$ et $s \circ r^2$ respectivement.

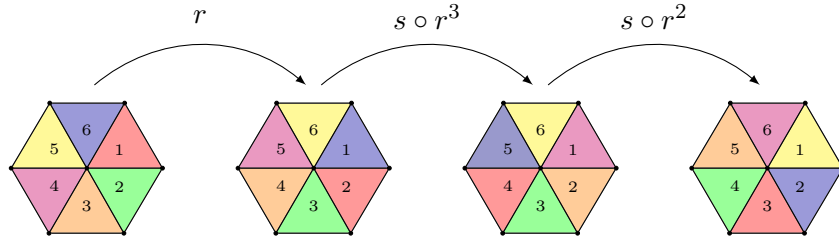


FIGURE 5.1 – 4 colorations équivalentes d'un hexagone.

La figure 5.2 montre des jetons non-équivalents.

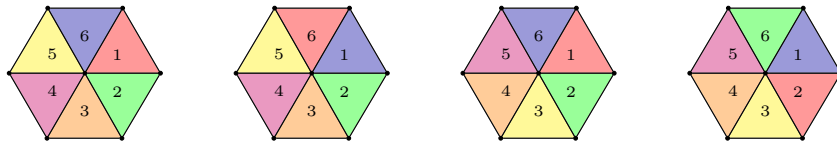


FIGURE 5.2 – 4 colorations non-équivalentes d'un hexagone.

Application du lemme de Burnside

Pour colorier les six faces du jeton, nous avons à disposition :

$$\begin{aligned}
 \binom{6}{1} &= 6 \text{ couleurs pour la face 1,} & \binom{5}{1} &= 5 \text{ couleurs pour la face 2,} \\
 \binom{4}{1} &= 4 \text{ couleurs pour la face 3,} & \binom{3}{1} &= 3 \text{ couleurs pour la face 4,} \\
 \binom{2}{1} &= 2 \text{ couleurs pour la face 5,} & \binom{1}{1} &= 1 \text{ couleur pour la face 6.}
 \end{aligned}$$

Ce qui fera au total $6 \times 5 \times 4 \times 3 \times 2 \times 1 = 6! = 720$ colorations possibles. C'est à dire, $|\mathcal{C}| = 720$. On cherche à calculer :

$$|\mathcal{C}/D_6| = \frac{1}{|D_6|} \sum_{\sigma \in D_6} |Fix(\sigma)|.$$

D'après le lemme 3.6, une coloration est fixe par σ si et seulement si elle est stable sur les cycles de σ . Or, chaque élément est de couleur différente, donc les éléments d'un même cycle ne peuvent pas avoir la même couleur, on en déduit que pour tout $\sigma \neq id : Fix(\sigma) = \emptyset$. Ainsi :

$$|\mathcal{C}/D_6| = \frac{|Fix(id)|}{12} = \frac{720}{12} = 60.$$

Application du théorème de Pólya

L'ensemble des triangles à colorier est $\mathcal{X} = \{1, 2, 3, 4, 5, 6\}$. Celui des couleurs est $\mathcal{Y} = \{y_1, y_2, y_3, y_4, y_5, y_6\}$.

D'après la table 5.1, on déduit que le polynôme indicateur de cycles est :

$$Z_{D_6}(x_1, x_2, x_3, x_4, x_5, x_6) = \frac{x_1^6 + 3x_1^2x_2^2 + 4x_2^3 + 2x_3^2 + 2x_6}{12}. \quad (5.1)$$

Donc le polynôme indicateur de couleurs est :

$$\begin{aligned} Ind_{D_6}(y_1, y_2, y_3, y_4, y_5, y_6) &= Z_{D_6}\left(\sum_{y \in \mathcal{Y}} y, \sum_{y \in \mathcal{Y}} y^2, \dots, \sum_{y \in \mathcal{Y}} y^n\right) \\ &= \frac{1}{12} \left((y_1 + y_2 + y_3 + y_4 + y_5 + y_6)^6 \right. \\ &\quad + 3(y_1 + y_2 + y_3 + y_4 + y_5 + y_6)^2 (y_1^2 + y_2^2 + y_3^2 + y_4^2 + y_5^2 + y_6^2)^2 \\ &\quad + 4(y_1^2 + y_2^2 + y_3^2 + y_4^2 + y_5^2 + y_6^2)^3 \\ &\quad + 2(y_1^3 + y_2^3 + y_3^3 + y_4^3 + y_5^3 + y_6^3)^2 \\ &\quad \left. + 2(y_1^6 + y_2^6 + y_3^6 + y_4^6 + y_5^6 + y_6^6) \right) \end{aligned}$$

Il s'agit de trouver le coefficient de $y_1 y_2 y_3 y_4 y_5 y_6$. Il est clair que le seul terme qui le contient est le premier terme du polynôme car les autres ont des puissances plus grandes que 1. Le développement du multinôme $(y_1 + y_2 + y_3 + y_4 + y_5 + y_6)^6$ est donné par :

$$(y_1 + y_2 + y_3 + y_4 + y_5 + y_6)^6 = \sum_{k_1 + \dots + k_6 = 6} \binom{6}{k_1, \dots, k_6} y_1^{k_1} y_2^{k_2} y_3^{k_3} y_4^{k_4} y_5^{k_5} y_6^{k_6}.$$

Donc le coefficient de $y_1 y_2 y_3 y_4 y_5 y_6$ dans ce multinôme est $\binom{6}{1, \dots, 1} = 6! = 720$.

D'où le coefficient dans $Ind_{D_6}(y_1, y_2, y_3, y_4, y_5, y_6)$ est $\frac{720}{12} = 60$.

Rappel

Le développement du multinôme de Newton est donné par :

$$(x_1 + x_2 + \dots + x_m)^n = \sum_{k_1 + k_2 + \dots + k_m = n} \binom{n}{k_1, k_2, \dots, k_m} x_1^{k_1} x_2^{k_2} \dots x_m^{k_m}.$$

La valeur du coefficient multinomial est donnée par :

$$\binom{n}{k_1, k_2, \dots, k_m} = \frac{n!}{k_1! \cdot k_2! \cdot \dots \cdot k_m!}.$$

5.2 Coloration des solides de Platon

Les solides de Platon sont les polytopes réguliers de dimension 3. Il en existe exactement cinq : le tétraèdre, le cube, l'octaèdre, l'icosaèdre et le dodécaèdre.

Les éléments à colorier sont les faces. Si un solide de Platon possède n faces, alors le groupe sous-jacent est un sous-groupe de \mathfrak{S}_n .

5.2.1 Dualité entre solides de Platon

La dualité entre solides de Platon est telle que :

- à chaque face de la forme primale est associé un et un seul sommet de la forme duale.
- deux faces sont voisines dans la forme primale si et seulement si les deux sommets correspondant dans la forme duale soient reliés par une arête.

Une symétrie du primal est une permutation de ses facettes le laissant invariant, et donc une permutation des sommets du dual le laissant invariant, et une telle permutation entraîne une permutation de facettes du dual le laissant inchangé, donc une symétrie du dual.

Une conséquence de cette dualité est que deux formes duales ont les mêmes symétries.

5.2.2 Le tétraèdre

Le tétraèdre possède 4 faces triangulaires et 4 sommets, il est le dual de lui-même. Le groupe sous-jacent s'appelle *le groupe tétraédral*, noté T . Nous verrons qu'il est d'ordre 12 et qu'il est isomorphe au groupe alterné A_4 .

La figure 5.3 suivante est une illustration du tétraèdre régulier.

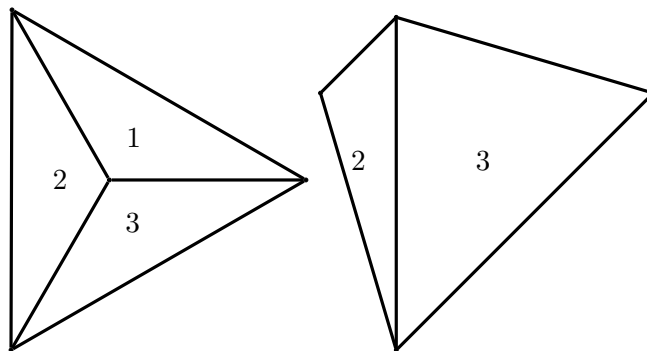


FIGURE 5.3 – Illustration de deux positions d'un tétraèdre.

Groupe de rotations du tétraèdre

Rotations d'axes passant par le centre d'une face et le sommet opposé : il existe quatre axes de ce type. Les angles de rotation possibles sont $2\pi/3$ et $-2\pi/3$. Ce type de rotation fixe une face et les trois faces restantes forment un cycle car chacune s'envoie sur sa voisine (voisine gauche ou droite). Donc le type de la permutation correspondante est donc $(1^1 3^1)$. Ces huit rotations ($4 \text{ axes} \times 2 \text{ angles}$) forment la classe de conjugaison notée C_1 .

Rotations d'axes joignant les milieux des arêtes opposées : Il existe trois paires d'arêtes opposées donc 3 axes. L'angle de rotation est π donc le nombre de rotations est 3. Ces rotations engendrent deux transpositions d'où le type est (2^2) . Elles forment la classe de conjugaison notée C_2 .

Le nombre de permutations du groupe T en comptant l'identité est donc $1 + 8 + 3 = 12$. La table 5.2 suivante donne le type, le nombre de colorations fixes ainsi que le monôme par classe de conjugaison. $|Fix(\sigma)|$ est calculé grâce au corollaire 3.2.

Classe de conjugaison C	C_{id}	C_1	C_2
$ C $	1	8	3
Type de $\sigma \in C$	(1^4)	$(1^1 3^1)$	(2^2)
$ Fix(\sigma) , \sigma \in C$	k^4	k^2	k^2
$Z_\sigma, \sigma \in C$	x_1^4	$x_1 x_3$	x_2^2

TABLE 5.2 – Monôme et $|fixateur|$ par classe de conjugaison de T .

La table 5.3 suivante montre que toutes les permutations sont paires, donc $T \cong A_4$.

$\sigma \in T$	Cycles	# cycles paires	$\sigma \in T$	Cycles	# cycles paires
1234	$(1)(2)(3)(4)$	0	4132	$(1, 4, 2)(3)$	0
1342	$(1)(2, 3, 4)$	0	3124	$(1, 3, 2)(4)$	0
1423	$(1)(2, 4, 3)$	0	2314	$(1, 2, 3)(4)$	0
3241	$(1, 3, 4)(2)$	0	2143	$(1, 2)(3, 4)$	2
4213	$(1, 4, 3)(2)$	0	3412	$(1, 3)(2, 4)$	2
2431	$(1, 2, 4)(3)$	0	4321	$(1, 4)(2, 3)$	2

TABLE 5.3 – Parités des éléments du groupe tétraedral.

D'après la table 5.2, le polynôme indicateur de cycles est donné par :

$$Z_T(x_1, x_2, x_3, x_4) = \frac{1}{|T|} \sum_{\sigma \in T} Z_{\sigma}(x_1, x_2, x_3, x_4) = \frac{x_1^4 + 8x_1x_3 + 3x_2^2}{12}.$$

2 couleurs

Avec deux couleurs la solution est donnée selon le théorème de Pólya par :

$$Z_T(2, 2, 2, 2) = \frac{2^4 + 8 \cdot 2 \cdot 2 + 3 \cdot 2^2}{12} = \frac{16 + 32 + 12}{12} = \frac{60}{12} = 5.$$

Il existe 5 colorations réellement différentes pour colorier un tétraèdre avec 2 couleurs. La figure 5.4 est une illustration des cinq colorations sur le patron du tétraèdre.

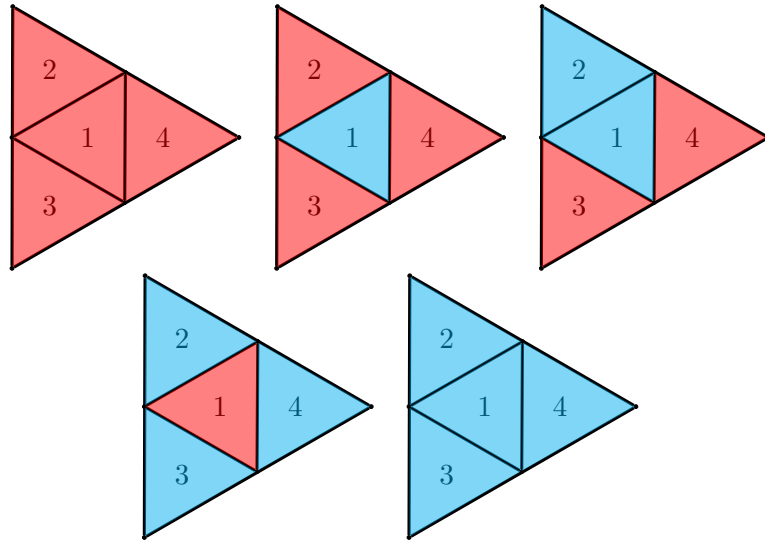


FIGURE 5.4 – Les cinq colorations différentes du tétraèdre avec 2 couleurs.

3 couleurs

Même chose avec 3 couleurs :

$$Z_T(3, 3, 3, 3) = \frac{3^4 + 8 \cdot 3 \cdot 3 + 3 \cdot 3^2}{12} = \frac{81 + 72 + 27}{12} = \frac{180}{12} = 15.$$

La figure 5.5 suivante illustre les 15 colorations.

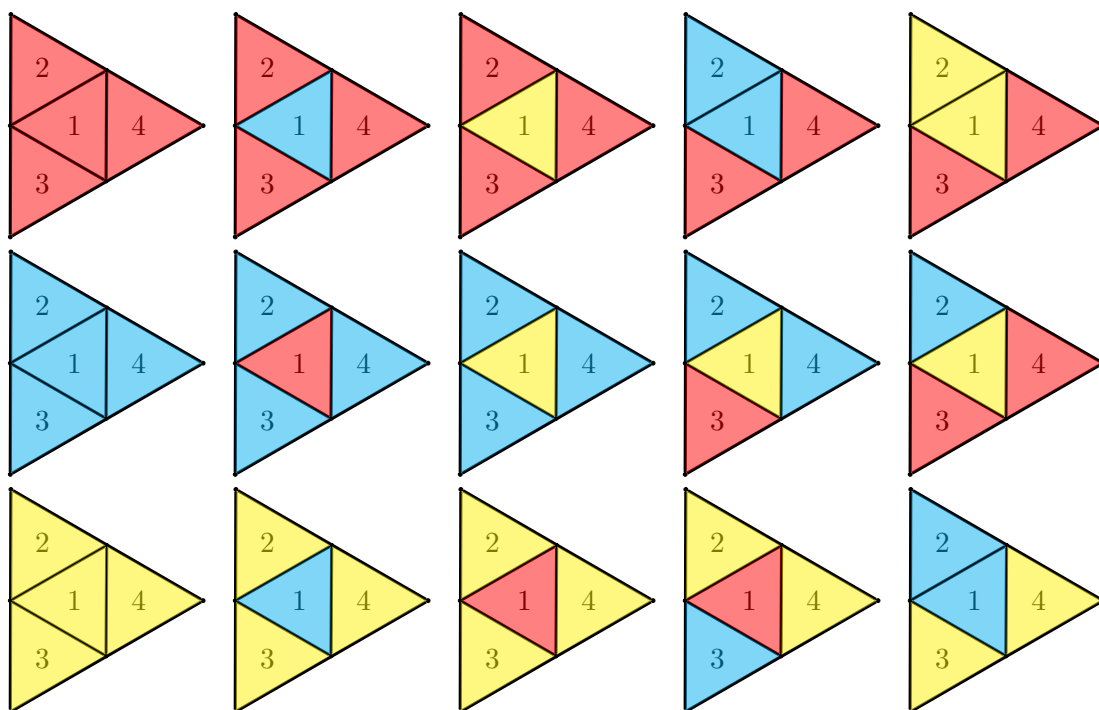


FIGURE 5.5 – Les 15 colorations différentes du tétraèdre avec 3 couleurs.

k couleurs avec le lemme de Burnside et le théorème de Pólya

Pour k couleurs, le lemme de Burnside et le théorème de Pólya donnent : (les cardinalités des fixateurs sont données par la table 5.2)

$$\begin{aligned}
 |\mathcal{C}/T| &= \frac{1}{|T|} \sum_{\sigma \in T} |Fix(\sigma)| = \frac{|Fix(C_{id})| + |Fix(C_1)| + |Fix(C_2)|}{12} \\
 &= \frac{k^4 + 8k^2 + 3k^2}{12} = \frac{k^4 + 11k^2}{12}. \\
 Z_T(k, k, k, k) &= \frac{k^4 + 8kk + 3k^2}{12} = \frac{k^4 + 11k^2}{12}.
 \end{aligned}$$

La formule générale est la même avec les deux méthodes. Les différentes valeurs de k forment une suite que l'on note \mathcal{A}_T . Les premiers termes à partir de $k = 0$ sont 0, 1, 5, 15, 36, 75, 141, 245, ... L'annexe B.1, donne une liste des 48 premiers termes.

5.2.3 Le cube et l'octaèdre

Le cube et l'octaèdre sont deux formes duales, les sous-groupes sous-jacents sont isomorphes. Nous noterons dans cette section les groupes de symétrie du cube et de l'octaèdre par *Cube* et *Octa* respectivement.

Groupes de symétrie

Nous analyserons les rotations du cube et nous déduirons celles de l'octaèdre. Le cube admet trois types d'axes de rotations.

Rotations d'axes passant par les centres de deux faces opposées : Comme il existe six faces, alors le nombre de paires de faces opposées est trois, donc trois axes de ce type. Les angles de rotation sont $\pi/2$, π et $-\pi/2$. Ces rotations au nombre de 9, fixent les deux faces par lesquelles passe l'axe.

Les six rotations d'angles $\pi/2$ ou $-\pi/2$ envoient chaque face sur sa voisine (gauche ou droite) créant ainsi un cycle de longueur 4 et formant une classe de conjugaison que l'on note C_1 , elle est de type $(1^2 4^1)$. La classe duale C_1 est de type (4^2) .

Les trois rotations d'angles π permutent les faces opposées créant ainsi deux transposition et formant une classe de conjugaison de type $(1^2 2^2)$ que l'on note C_2 . La classe duale C_2 est de type (2^4) .

Rotations d'axes passant par les milieux de deux arêtes opposées : Comme il existe 12 arêtes, alors le nombre d'axes de ce type est 6. L'angle de rotation est π . La figure 5.6 montre, en bleu, un axe de ce type. La rotation d'un demi-tour envoie les trois faces visibles sur les trois faces cachées entraînant une bijection entre les deux ensembles de 3 faces, et créant ainsi trois transpositions. Ces six rotations forment une classe de conjugaison de type (2^3) que l'on note C_3 .

Dans le dual, le type est (2^4) . Donc avec les trois rotations duales de même type déjà vues, la classe de conjugaison duale C_1 compte neuf permutations.

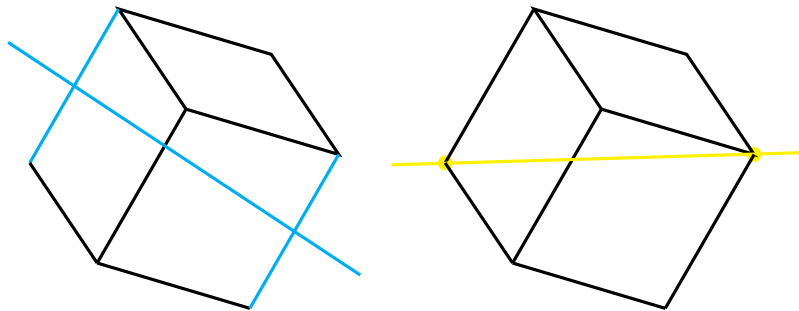


FIGURE 5.6 – Deux types d'axes de rotation du cube.

Rotations d'axes passant par deux sommets opposés : Comme le nombre de sommets est 8, alors il existe 4 axes de ce type, la figure 5.6 en montre, en jaune, un exemple. Les angles sont $\pi/3$ et $-\pi/3$. Si l'axe passe par les sommets s_1 , s_2 , alors les trois faces reliées par s_1 forment un cycle car chacune est envoyée sur sa voisine gauche ou droite. Même chose pour les trois autres faces reliées par s_2 . Ces rotations au nombre de 8 sont de type (3^2) , le type dual est $(1^2 3^2)$. Elles forment la classe de conjugaison que l'on note C_4 . La classe duale est notée C_3 .

Avec la rotation identité, le nombre total de rotations est $1 + 6 + 3 + 6 + 8 = 24$. Les tables 5.4 et 5.5 suivantes résument ce que nous venons de dire et donnent le monôme associé à chaque opération σ , ainsi que le nombre de colorations fixes $|Fix(\sigma)|$ calculé grâce au corollaire 3.2.

Classe de conjugaison C	C_{id}	C_1	C_2	C_3	C_4
$ C $	1	6	3	6	8
Type de $\sigma \in C$	(1^6)	$(1^2 4^1)$	$(1^2 2^2)$	(2^3)	(3^2)
$ Fix(\sigma) , \sigma \in C$	k^6	k^2	k^4	k^3	k^2
$Z_\sigma, \sigma \in C$	x_1^6	$x_1^2 x_4$	$x_1^2 x_2^2$	x_2^3	x_3^2

TABLE 5.4 – Monôme et $|fixateur|$ par classe de conjugaison de *Cube*.

Classe de conjugaison C	C_{id}	C_1	C_2	C_3
$ C $	1	6	9	8
Type de $\sigma \in C$	(1^8)	(4^2)	(2^4)	$(1^2 3^2)$
$ Fix(\sigma) , \sigma \in C$	k^8	k^2	k^4	k^3
$Z_\sigma, \sigma \in C$	x_1^8	x_4^2	x_2^4	$x_1^2 x_3^2$

TABLE 5.5 – Monôme et $|fixateur|$ par classe de conjugaison de *Octa*.

Les tables nous permettent de déduire les polynômes indicateurs de cycles associés à *Cube* et *Octa* respectivement :

$$Z_{Cube}(x_1, \dots, x_6) = \frac{1}{|Cube|} \sum_{\sigma \in Cube} Z_\sigma(x_1, \dots, x_6) = \frac{x_1^6 + 3x_1^2 x_2^2 + 6x_1^2 x_4 + 6x_2^3 + 8x_3^2}{24}.$$

$$Z_{Octa}(x_1, \dots, x_8) = \frac{1}{|Octa|} \sum_{\sigma \in Octa} Z_\sigma(x_1, \dots, x_8) = \frac{x_1^8 + 8x_1^2 x_3^2 + 9x_2^4 + 6x_4^2}{24}.$$

Colorations avec au plus k couleurs

D'après le théorème de Pólya, le nombre de colorations différentes du cube et de l'octaèdre avec au plus k couleurs est donné par $Z_{Cube}(k, \dots, k)$ pour le cube et $Z_{Octa}(k, \dots, k)$ pour l'octaèdre.

Les différentes valeurs de k à partir de $k = 0$, donnent des suites que l'on note respectivement \mathcal{A}_{Cube} et \mathcal{A}_{Octa} . Les termes généraux sont donnés par :

$$\mathcal{A}_{Cube}(k) = \frac{k^6 + 3k^2 k^2 + 6k^2 k + 6k^3 + 8k^2}{24}. \quad (5.2)$$

$$\mathcal{A}_{Octa}(k) = \frac{k^8 + 8k^2 k^2 + 9k^4 + 6k^2}{24}. \quad (5.3)$$

Les premières valeurs sont 0, 1, 10, 57, 240, 800 pour le cube. Donc le nombre de colorations réellement différentes du cube avec 2 couleurs est 10. Avec 3 couleurs

est 57. Avec 4 couleurs le nombre est 240.

Pour l'octaèdre, la suite commence par 0, 1, 23, 333, 2916, 16725, par exemple le nombre de colorations avec 3 couleurs est 333.

L'annexe B.2 donne une liste des 30 premiers termes pour chaque suite.

Coloration du cube avec deux couleurs

Le nombre de colorations non-équivalentes du cube avec deux couleurs est $\mathcal{A}_{Cube}(2) = 10$. La figure suivante les illustre sur le patron du cube :

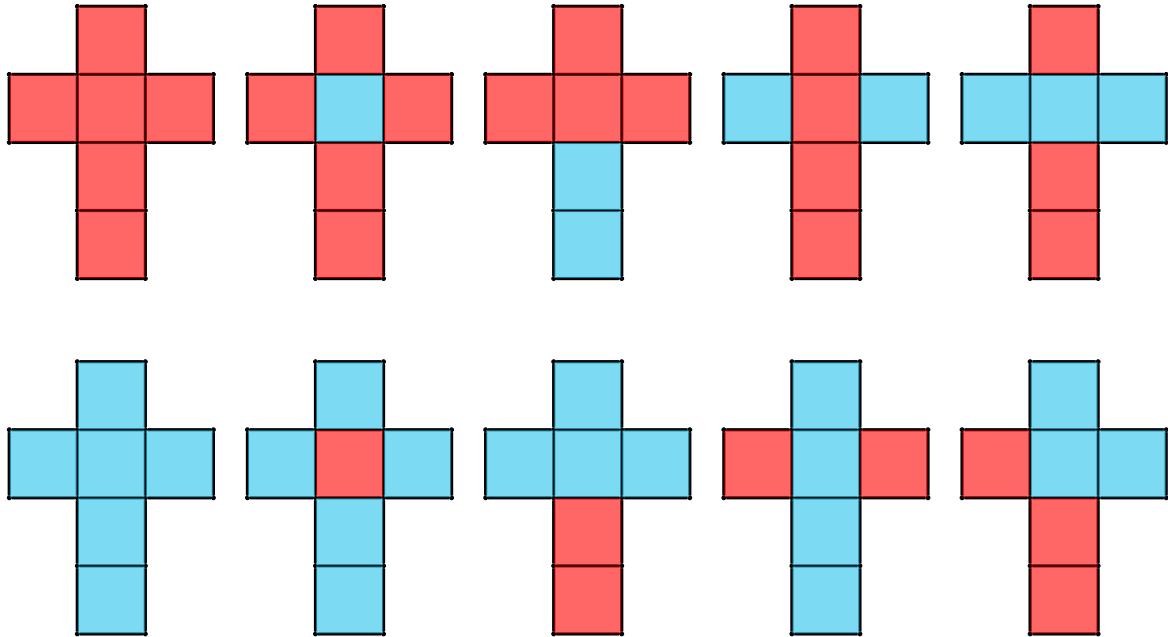


FIGURE 5.7 – Les dix colorations non-équivalentes du cube avec deux couleurs.

5.2.4 Le dodécaèdre et l'icosaèdre

Le dodécaèdre régulier est constitué de douze pentagones réguliers et l'icosaèdre régulier de vingt triangles équilatéraux. Les deux formes sont duales. Notons dans la suite *Dode* et *Ico* les groupes de symétrie du dodécaèdre et de l'icosaèdre respectivement. La figure 5.8 suivante montre deux positions différentes d'un dodécaèdre régulier dont les faces sont numérotées de 1 à 12 :

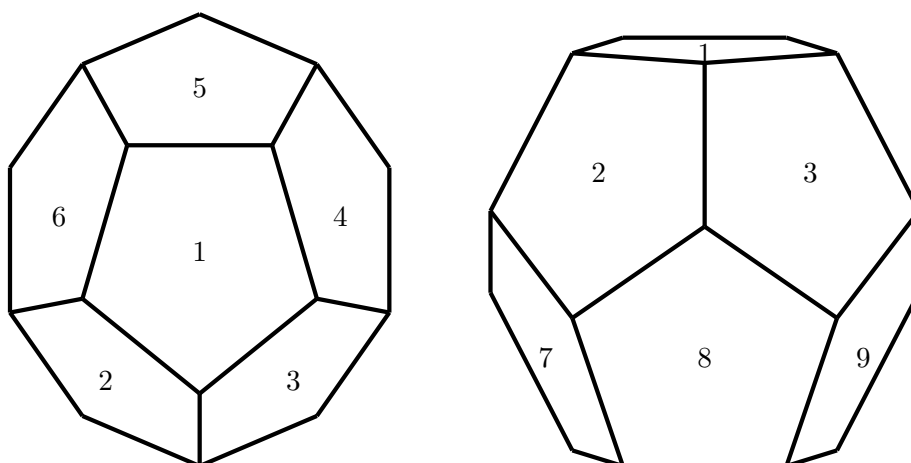


FIGURE 5.8 – Deux positions différentes d'un dodécaèdre régulier.

La figure 5.9 suivante montre un icosaèdre régulier tel que les sommets 1, 2, ..., 12 correspondent aux faces 1, 2, ..., 12 respectivement du dodécaèdre de la figure 5.8.

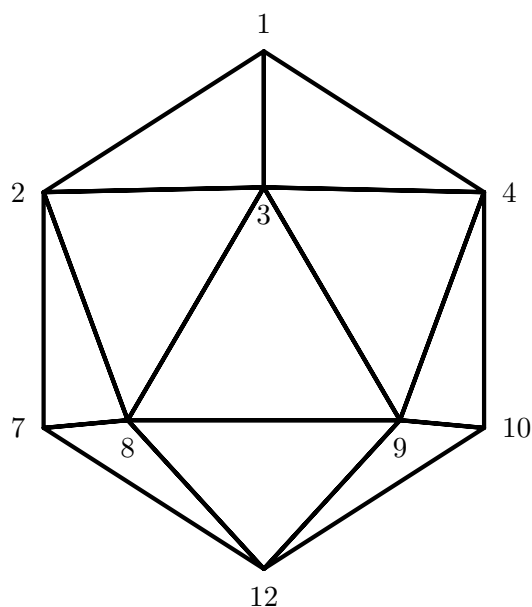


FIGURE 5.9 – Le dual du dodécaèdre de la figure 5.8.

La table 5.6 suivante montre l'opposé de chaque face du dodécaèdre de la figure 5.8 (ou l'opposé de chaque sommet de l'icosaèdre de la figure 5.9).

face	1	2	3	4	5	6
face opposée	12	10	11	7	8	9

TABLE 5.6 – paires de faces opposées du dodécaèdre de la figure 5.8.

Groupes de symétrie

Pour trouver le groupe de chacun des deux solides, nous analyserons les rotations du dodécaèdre et nous déduirons l'équivalent pour l'icosaèdre.

Rotations d'axes passant par les centres de deux faces opposées : Comme il existe douze faces, chacune possède une opposée, donc le nombre de paires de faces opposées est 6 ce qui donne 6 axes. Ce type d'axes admet 4 angles de rotations à savoir $2\pi/5$, $4\pi/5$, $6\pi/5$ et $8\pi/5$.

Exemple 5.1. Dans l'exemple de la figure 5.8, position de gauche, si l'axe passe par les centres des faces 1 et 12. Et si l'angle est $2\pi/5$, alors la permutation résultante est donnée par les cycles $(1)(2, 3, 4, 5, 6)(7, 8, 9, 10, 11)(12)$, son type est $(1^2 5^2)$.

De façon générale, ce type de rotation fixe deux faces et les dix autres faces forment deux couronnes chacune de cinq faces. D'après le corollaire 3.1, une permutation circulaire différente de l'identité, dont la longueur est un nombre premier p , est un p -cycle. Nous avons donc deux 5-cycles, donc le type est $(1^2 5^2)$. Tandis que dans le dual, les vingt faces forment quatre couronnes chacune de cinq faces donc le type dual est (5^4) . Le nombre de permutations de ce type est donné par 6 axes \times 4 angles = 24 permutations. Ces permutations forment la classe de conjugaison que l'on note C_f dans *Dode* (resp. C_s dans *Ico*).

Rotations d'axes passant par deux sommets opposés : Le nombre de paires de sommets opposés est 10, donc 10 axes. Les angles de rotation possibles sont $2\pi/3$ et $-2\pi/3$. Ces rotations engendrent quatre cycles triangulaires donc le type est (3^4) . Et forment la classe de conjugaison que l'on note C_s . Comme l'axe passe par deux sommets, alors 2 sommets sont fixes et les 18 autres sommets forment six cycles de longueur 3. Donc le type de la classe de conjugaison duale C_f est $(1^2 3^6)$. Le nombre de permutations de ce type est 20 (10 axes \times 2 angles).

Exemple 5.2. Dans l'exemple de la figure 5.8, position de droite, si l'axe passe par le sommet reliant les faces 2, 3 et 8. Et si l'angle est $2\pi/3$, alors la permutation résultante est donnée par les cycles $(1, 7, 9)(2, 8, 3)(4, 6, 12)(5, 11, 10)$. Son type est (3^4) . La figure 5.10 montre l'effet de cette rotation sur les sommets. On peut voir trois cycles de longueur 3 et un point fixe. La même chose se passe pour les dix sommets restants. D'où, le type dual est $(1^2 3^6)$.

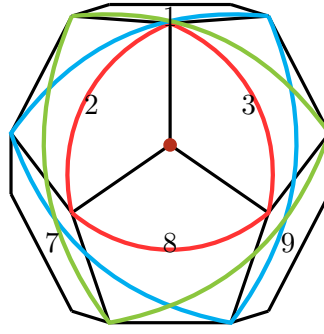


FIGURE 5.10 – Trois cycles de sommets de longueur 3 d'un dodécaèdre.

Rotations d'axes passant par les milieux de deux arêtes opposées : Comme il existe 30 arêtes, alors le nombre d'axes est 15. L'angle de rotation est π . La figure 5.11 montre six faces du dodécaèdre et un axe de ce type. Quelque soit la numérotation des faces, et quelque soit la paire d'arêtes définissant l'axe, la rotation d'un demi-tour envoie les six faces visibles sur les six faces cachées formant ainsi six transpositions. Ceci entraîne l'envoi de dix sommets sur les dix autres, formant dix transpositions de sommets. Ces permutations au nombre de 15 (une pour chaque axe), forment la classe de conjugaison que l'on note C_a pour *Dode* et *Ico*, dont les types sont respectivement (2^6) et (2^{10}) .

Exemple 5.3. La permutation résultante d'un demi-tour autour de l'axe de la figure 5.11 est donnée par les cycles : $(1, 12)(2, 11)(3, 10)(4, 9)(5, 8)(6, 7)$.

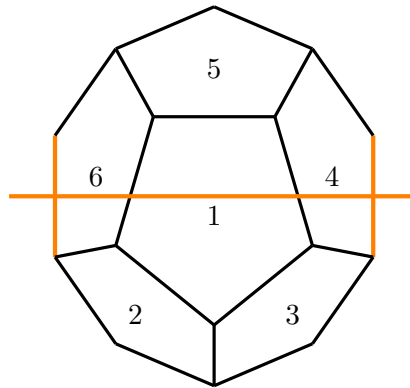


FIGURE 5.11 – Axe de rotation passant par les milieux de deux arêtes opposées.

Le nombre total de rotations y compris l'identité est $1 + 24 + 20 + 15 = 60$. Le table 5.7 donne le nombre de colorations fixes par chaque permutation de *Dode* et *Ico* calculé grâce au corollaire 3.2 (dans notre cas $|Fix(\sigma)| = k^{|\text{cycles de } \sigma|}$), ainsi que le monôme associé.

Groupe	<i>Dode</i>				<i>Ico</i>			
Classe de conjugaison C	C_{id}	C_f	C_s	C_a	C_{id}	C_f	C_s	C_a
$ C $	1	24	20	15	1	20	24	15
Type de $\sigma \in C$	(1^{12})	$(1^2 5^2)$	(3^4)	(2^6)	(1^{20})	$(1^2 3^6)$	(5^4)	(2^{10})
$ Fix(\sigma) , \sigma \in C$	k^{12}	k^4	k^4	k^6	k^{20}	k^8	k^4	k^{10}
$Z_\sigma, \sigma \in C$	x_1^{12}	$x_1^2 x_5^2$	x_3^4	x_2^6	x_1^{20}	$x_1^2 x_3^6$	x_5^4	x_2^{10}

TABLE 5.7 – Monôme et $|fixateur|$ par classe de conjugaison de *Dode* et *Ico*.

proposition 5.1. *Les groupes de symétrie du dodécaèdre et de l'icosaèdre sont isomorphes au groupe alterné A_5 .*

Démonstration. D'après la table 5.7, aucune permutation ne possède un nombre impair de cycles de longueur paire, donc les 60 permutations formant le groupe de symétrie du dodécaèdre (resp. de l'icosaèdre) sont paires.

Or, le groupe alterné A_5 est un groupe de 60 permutations toutes paires, donc $Dode \cong A_5$ et $Ico \cong A_5$. \square

Posons $X_{12} = (x_1, \dots, x_{12})$, et $X_{20} = (x_1, \dots, x_{20})$. D'après la table 5.7, les polynômes indicateur de cycles sont :

$$\begin{aligned}
Z_{Dode}(X_{12}) &= \frac{1}{|Dode|} \sum_{\sigma \in Dode} Z_\sigma(X_{12}) = \frac{x_1^{12} + 24x_1^2 x_5^2 + 15x_2^6 + 20x_3^4}{60} \\
Z_{Ico}(X_{20}) &= \frac{1}{|Ico|} \sum_{\sigma \in Ico} Z_\sigma(X_{20}) = \frac{x_1^{20} + 20x_1^2 x_3^6 + 15x_2^{10} + 24x_5^4}{60}
\end{aligned}$$

Colorations avec au plus k couleurs

Avec le lemme de Burnside Soit \mathcal{C} l'ensemble de toutes les colorations. Les cardinalités des fixateurs sont donnés par la table 5.7. Alors :

$$\begin{aligned}
|\mathcal{C}/Dode| &= \frac{1}{|Dode|} \sum_{\sigma \in Dode} |Fix(\sigma)| \\
&= \frac{|Fix(C_{id})| + 24|Fix(C_f)| + 20|Fix(C_s)| + 15|Fix(C_a)|}{60} \\
&= \frac{k^{12} + 24k^4 + 20k^4 + 15k^6}{60} = \frac{k^{12} + 15k^6 + 44k^4}{60}
\end{aligned}$$

Avec le théorème de Pólya

$$\mathcal{Z}_{Dode}(k, k, \dots, k) = \frac{k^{12} + 24k^2 k^2 + 15k^6 + 20k^4}{60} = \frac{k^{12} + 15k^6 + 44k^4}{60}$$

Comme dans les exemples précédents, les deux méthodes donnent la même formule générale. Les différentes valeurs de k forment une suite que l'on note \mathcal{A}_{Dode} .

Cette suite augmente très vite. Les cinq premiers termes sont 0, 1, 96, 9099, 280832, 4073375.

Pour l'icosaèdre, la suite correspondante se note \mathcal{A}_{Ico} . Le calcul donne :

$$\begin{aligned}\mathcal{A}_{Ico}(k) &= \frac{1}{|Ico|} \sum_{\sigma \in Ico} |Fix(\sigma)| = Z_{Ico}(k, k, \dots, k) \\ &= \frac{k^{20} + 20k^{12} + 15k^{10} + 24k^4}{60}.\end{aligned}$$

Pour $k = 0, 1, 2, 3, 4, 5$, les termes sont 0, 1, 19104, 58305015, 18331048448, 1589541015875. L'annexe B.3 donne les 30 premiers termes des deux suites.

Remarque 5.1. *Sans contraintes sur les colorations, les deux méthodes sont de même complexité.*

Colorations du dodécaèdre : 6 faces rouges et 6 faces bleues

Posons $\mathcal{X} = \{1, 2, \dots, 12\}$ l'ensemble de faces à colorier, et $\mathcal{Y} = \{r, b\}$ l'ensemble des deux couleurs rouge et bleue. Le nombre de colorations non équivalentes telles que 6 faces soient rouges et 6 faces soient bleues est exactement le coefficient de r^6b^6 dans l'indicateur de couleurs du groupe *Dode*. Nous avons :

$$\begin{aligned}Ind_{Dode}(b, r) &= Z_{Dode}(r + b, r^2 + b^2, \dots, r^{12} + b^{12}) \\ &= \frac{(r + b)^{12} + 24(r + b)^2(r^5 + b^5)^2 + 15(r^2 + b^2)^6 + 20(r^3 + b^3)^4}{60}.\end{aligned}$$

Le développement des monômes donne (voir le triangle de Pascal dans l'annexe A) :

$$\begin{aligned}(r + b)^{12} &= r^{12} + 12r^{11}b + 66r^{10}b^2 + 220r^9b^3 + 495r^8b^4 + 792r^7b^5 + \textcolor{red}{924r^6b^6} \\ &\quad + 792r^5b^7 + 495r^4b^8 + 220r^3b^9 + 66r^2b^{10} + 12rb^{11} + b^{12}.\end{aligned}$$

$$\begin{aligned}24(r + b)^2(r^5 + b^5)^2 &= 24(r^{10} + 2r^5b^5 + b^{10})(r^2 + 2rb + b^2) \\ &= 24(r^{10} + b^{10})(r + b)^2 + 24 \cdot 2r^7b^5 + \textcolor{red}{24 \cdot 4r^6b^6} + 24 \cdot 2r^5b^5.\end{aligned}$$

$$\begin{aligned}15(r^2 + b^2)^6 &= 15r^{12} + 15 \cdot 6r^{10}b^2 + 15 \cdot 15r^8b^4 + \textcolor{red}{15 \cdot 20r^6b^6} + 15 \cdot 15r^4b^8 \\ &\quad + 15 \cdot 6r^2b^{10} + 15b^{12}.\end{aligned}$$

$$20(r^3 + b^3)^4 = 20r^{12} + 20 \cdot 4r^9b^3 + \textcolor{red}{20 \cdot 6r^6b^6} + 20 \cdot 4r^3b^9 + 20b^{12}.$$

Le monôme contenant r^6b^6 est donné par :

$$\frac{924r^6b^6 + 24 \cdot 4r^6b^6 + 15 \cdot 20r^6b^6 + 20 \cdot 6r^6b^6}{60} = \frac{1440r^6b^6}{60} = 24r^6b^6.$$

Le coefficient $\binom{12}{6} = 924$ est le nombre de toutes les colorations du dodécaèdre avec 6 faces rouges et 6 faces bleues. Mais d'après le théorème de Pólya, seulement 24 sont non équivalentes.

5.3 Sudoku

5.3.1 Sudoku classique

Le Sudoku classique est une grille 9×9 divisée en neuf blocks 3×3 , et remplie par les chiffres $1, 2, 3, \dots, 9$ tels que les neuf chiffres doivent figurer sur chaque ligne, chaque colonne et chaque block.

Trois blocks verticaux constituent une pile, et trois blocks horizontaux constituent une bande. La table 5.8 est une illustration d'une grille de Sudoku classique où les neuf blocks sont en gras, une pile est en rouge et une bande est en jaune. On remarque que l'intersection d'une pile et d'une bande est un block.

1	2	3	7	8	9	4	5	6
4	5	6	1	2	3	7	8	9
7	8	9	4	5	6	1	2	3
3	4	8	9	1	5	6	7	2
6	7	2	3	4	8	9	1	5
9	1	5	6	7	2	3	4	8
2	3	1	8	9	7	5	6	4
5	6	4	2	3	1	8	9	7
8	9	7	5	6	4	2	3	1

TABLE 5.8 – Illustration d'une pile, une bande et des neuf blocks sur un Sudoku classique.

On peut voir que l'échange entre deux lignes au sein d'une même bande ne viole pas les contraintes du Sudoku. Le résultat est une nouvelle grille de Sudoku dont la solution peut être obtenue à partir de la première en inversant les deux lignes. On dit que les deux grilles sont équivalentes.

Il existe d'autres transformations laissant la grille de Sudoku intrinsèquement la même (c.à.d la nouvelle grille est équivalente à la première), comme l'échange entre deux bandes. Idem pour les colonnes et les piles. Nous verrons toutes les opérations dans la suite.

5.3.2 Mini-Sudoku

Le mini-Sudoku est un Sudoku tel que la grille est de taille 4×4 divisée en quatre blocks 2×2 . Les chiffres sont 1, 2, 3 et 4. Un exemple est la grille suivante :

1	2	3	4
3	4	1	2
2	1	4	3
4	3	2	1

TABLE 5.9 – Un mini-Sudoku.

5.3.3 Définition formelle du Sudoku $n^2 \times n^2$

Une grille de Sudoku $n^2 \times n^2$ avec $n \geq 1$, est constituée de $n^2 \times n^2$ cases. Nous numérotérons l'ensemble des n^4 cases par des couples d'entiers. Soit donc $\mathcal{X} = \{1, \dots, n^2\}^2$ l'ensemble des cases et soit aussi $\mathcal{Y} = \{1, \dots, n^2\}$ l'ensemble de chiffres disponibles.

Vocabulaire

Une **case** est une paire $(i, j) \in \mathcal{X}$. Une **ligne** $L_i \subset \mathcal{X}$ est l'ensemble des cases $\{(i, 1), \dots, (i, n^2)\}$. Une **colonne** $C_j \subset \mathcal{X}$ est l'ensemble des cases $\{(1, j), \dots, (n^2, j)\}$ pour $i, j \in \{1, \dots, n^2\}$.

Une **bande** B_i est l'union des n lignes $L_{ni-(n-1)}, L_{ni-(n-2)} \dots L_{ni}$. Une **pile** P_j est l'union des n colonnes $C_{nj-(n-1)}, C_{nj-(n-2)} \dots C_{nj}$, pour $i, j \in \llbracket 1, n \rrbracket$.

Un **block** est l'intersection d'une bande et d'une pile. La **diagonale** est l'ensemble de cases $\{(i, i), i = 1, 2, \dots, n^2\}$.

L'application grille de Sudoku

Une grille de Sudoku est une application $f : \mathcal{X} \rightarrow \mathcal{Y}$ telle que l'image d'une ligne, d'une colonne ou d'un block par f est l'ensemble \mathcal{Y} .

Le problème consiste à compter le nombre de grilles de Sudoku réellement différentes à symétries près.

n=1 C'est le cas du Sudoku trivial. La grille est réduite à une seule case dont le chiffre est 1, comme le montre la table 5.10 suivante :

1

TABLE 5.10 – Le sudoku trivial.

Cette grille est unique.

n=2 C'est le cas du mini-Sudoku. Dans l'exemple de la table 5.9, nous avons bien pour tout $i \in \llbracket 1, 4 \rrbracket$, $f(L_i) = \{1, 2, 3, 4\} = \mathcal{Y}$ et $f(C_i) = \{1, 2, 3, 4\} = \mathcal{Y}$.

Les blocks $B_i \cap P_j$ pour $i, j \in \llbracket 1, 2 \rrbracket$ ont pour image par f l'ensemble \mathcal{Y} . Donc la grille de la table 5.9 est une grille de Sudoku valide.

n=3 C'est le Sudoku classique.

5.3.4 Groupe de symétrie du Sudoku

Deux grilles de Sudoku sont équivalentes si et seulement si l'une est l'image de l'autre par symétrie. Une symétrie du Sudoku est une transformation qui, appliquée à une quelconque grille de Sudoku valide, donne une grille de Sudoku valide.

La table 5.11 suivante donne les transformations de base S , et le sous-groupe engendré $\langle S \rangle$ ¹ :

S (ensemble de transformations)	$\langle S \rangle$	$ \langle S \rangle $
Rénumérotations des chiffres	$\cong \mathfrak{S}_{n^2}$	$(n^2)!$
Permutations de bandes	$\cong \mathfrak{S}_n$	$n!$
Permutations de piles	$\cong \mathfrak{S}_n$	$n!$
Permutations des n lignes dans chacune des n bandes	$\cong (\mathfrak{S}_n)^n$	$n!^n$
Permutations des n colonnes dans chacune des n piles	$\cong (\mathfrak{S}_n)^n$	$n!^n$
La réflexion par rapport à la diagonale	$\cong C_2$	2

TABLE 5.11 – Les éléments générateurs du groupe de symétrie du Sudoku $n^2 \times n^2$.

Notation 5.1. On note le produit direct des n groupes symétriques \mathfrak{S}_n par :

$$(\mathfrak{S}_n)^n = \underbrace{\mathfrak{S}_n \times \mathfrak{S}_n \cdots \times \mathfrak{S}_n}_{n \text{ fois}}.$$

Deux types de transformations

Il faut distinguer une transformation de grille qui est une permutation des $n^2 \times n^2$ cases, et une transformation de chiffres, qui est une permutation des n^2 chiffres.

Notation 5.2. On note $Sudo_n$ le groupe de toutes les transformations (cases et chiffres) du Sudoku $n^2 \times n^2$. Et on note $Grid_n$, le sous-groupe de $Sudo_n$ contenant juste les transformations des cases.

Le groupe $Sudo_n$ est le produit direct de \mathfrak{S}_{n^2} et de $Grid_n$. Ses éléments sont de la forme $(\sigma, g) \in \mathfrak{S}_{n^2} \times Grid_n$.

proposition 5.2. Si $g \in Grid_n$ est une transformation de cases, alors

$$|Fix(\sigma, g)| = |Fix(\gamma, g)| \text{ pour tous } \sigma, \gamma \in \mathfrak{S}_{n^2}.$$

1. En général, si G est un groupe, alors le sous-groupe engendré par une partie $S \subset G$ est un sous-groupe de G formé des éléments de S et de leurs composées. Autrement dit, c'est le plus petit sous-groupe contenant S . Il se note $\langle S \rangle$.

Crâce à la proposition 5.2, on peut écrire :

$$\begin{aligned}
\frac{1}{|Sudo_n|} \sum_{(\sigma, g) \in Sudo_n} |Fix(\sigma, g)| &= \frac{1}{n^2! \times |Grid_n|} \sum_{\sigma \in \mathfrak{S}_{n^2}} \sum_{g \in Grid_n} |Fix(\sigma, g)| \\
&= \frac{1}{n^2! \times |Grid_n|} (n^2!) \left(\sum_{g \in Grid_n} |Fix(\sigma, g)| \right) \\
&= \frac{1}{|Grid_n|} \sum_{g \in Grid_n} |Fix(\sigma, g)|.
\end{aligned}$$

Il suffit de considérer donc l'action du groupe $Grid_n$ sur les grilles de Sudoku pour appliquer le lemme de Burnside.

Théorème 5.1. [6] *Le groupe $Grid_n$ de symétrie du Sudoku $n^2 \times n^2$ est le produit semi direct :*

$$Grid_n \cong \left(((\mathfrak{S}_n)^n \rtimes \mathfrak{S}_n) \times ((\mathfrak{S}_n)^n \rtimes \mathfrak{S}_n) \right) \rtimes C_2.$$

La preuve de ce théorème est très longue, et utilise le fait que le groupe $Grid_n$ est isomorphe au groupe des automorphismes du groupe symétrique. Elle se trouve dans [6]. Un cas particulier est la proposition suivante :

proposition 5.3 (Cas particulier). [1] *Le groupe de symétrie du Sudoku 4×4 sans rénumérotation de chiffres, est donné par :*

$$Grid_2 \cong (D_4 \times D_4) \rtimes C_2.$$

Corollaire 5.1 (Du théorème 5.1). *Sans rénumérotation de chiffres, le nombre de symétries du Sudoku $n^2 \times n^2$ est donné par :*

$$|Grid_n| = (n!)^{2n+2} \times 2.$$

Les cardinalités pour $n = 2, 3, 4$ sont données par :²

$$\begin{aligned}
n = 2, \quad |Grid_2| &= (2!)^{2 \times 2 + 2} \times 2 = 2^6 \times 2 = 2^7 = 128, \\
n = 3, \quad |Grid_3| &= (3!)^{2 \times 3 + 2} \times 2 = 6^8 \times 2 = 3.359.232, \\
n = 4, \quad |Grid_4| &= (4!)^{2 \times 4 + 2} \times 2 = 24^{10} \times 2 = 126.806.761.930.752.
\end{aligned}$$

Russell et Jarvis [9], ont dénombrer les grilles de Sudoku 9×9 , en découvrant qu'il existe, dans $Grid_3$, seulement 275 classes d'équivalence dont le fixateur est non vide. Donc au lieu de travailler sur 3.359.232 permutations, ils ont travaillé seulement sur 275. Et ils ont trouvé que la solution était 5.472.730.538 grilles non-équivalentes parmi 18.383.222.420.692.992 au total.

2. Les points dans les nombres sont utilisés juste pour faciliter leur lecture.

6 Programmation

Ce chapitre est une brève description du code qui a été implémenté pendant notre étude.

6.1 Langage et installation

Le code a été écrit en **Python3**. La bibliothèque externe utilisée est la bibliothèque **Sympy** pour les polynômes. Cette bibliothèque doit être installée par l'utilisateur. Cependant, si l'utilisateur veut accélérer les calculs, il doit installer **Cython**.

6.2 Descriptions des classes

Magma, Group et SymmetryGroup sont des classes non-instanciables. Elles devaient être abstraites mais nous n'avons pas eu le temps de le faire. La classe SymmetricGroup est un plus, elle n'est pas utilisée, mais si l'utilisateur le souhaite, il pourra l'utiliser.

SymmetryGroup est la classe la plus importante, elle représente un groupe de symétrie quelconque. Elle hérite de Group, et elle engendre tous les groupes de symétrie (*voir* [Figure 6.1](#) pour l'UML). La table [6.1](#) suivante montre toutes les classes représentant un groupe de symétrie. Les exemples du code sont à écrire dans le fichier `__init__.py`, où les imports sont déjà fait.

Classe	Objet	Instanciation
CyclicGroup	Collier à n perles	<code>G = CyclicGroup.CyclicGroup(n)</code>
DiedralGroup	Polygone à n sommets	<code>G = DiedralGroup.DiedralGroup(n)</code>
TetraedralGroup	Tétraèdre	<code>G = TetraedralGroup.TetraedralGroup()</code>
CubicGroup	Cube	<code>G = CubicGroup.CubicGroup()</code>
OctahedralGroup	Octaèdre	<code>G = OctahedralGroup.OctahedralGroup()</code>
SudokuGroup	Sudoku $n^2 \times n^2$	<code>G = SudokuGroup.SudokuGroup(n)</code>

TABLE 6.1 – Les six groupes implémentés.

La construction est immédiate sauf pour le SudokuGroup (détails dans la suite du chapitre).

6.3 Diagramme de classe

Pour des raisons rédactionnelles, nous avons abrégé les noms de classes sur l'UML. Ainsi, les noms des classes se finissant par un grand **G**, se finissent en réalité par **Group**.

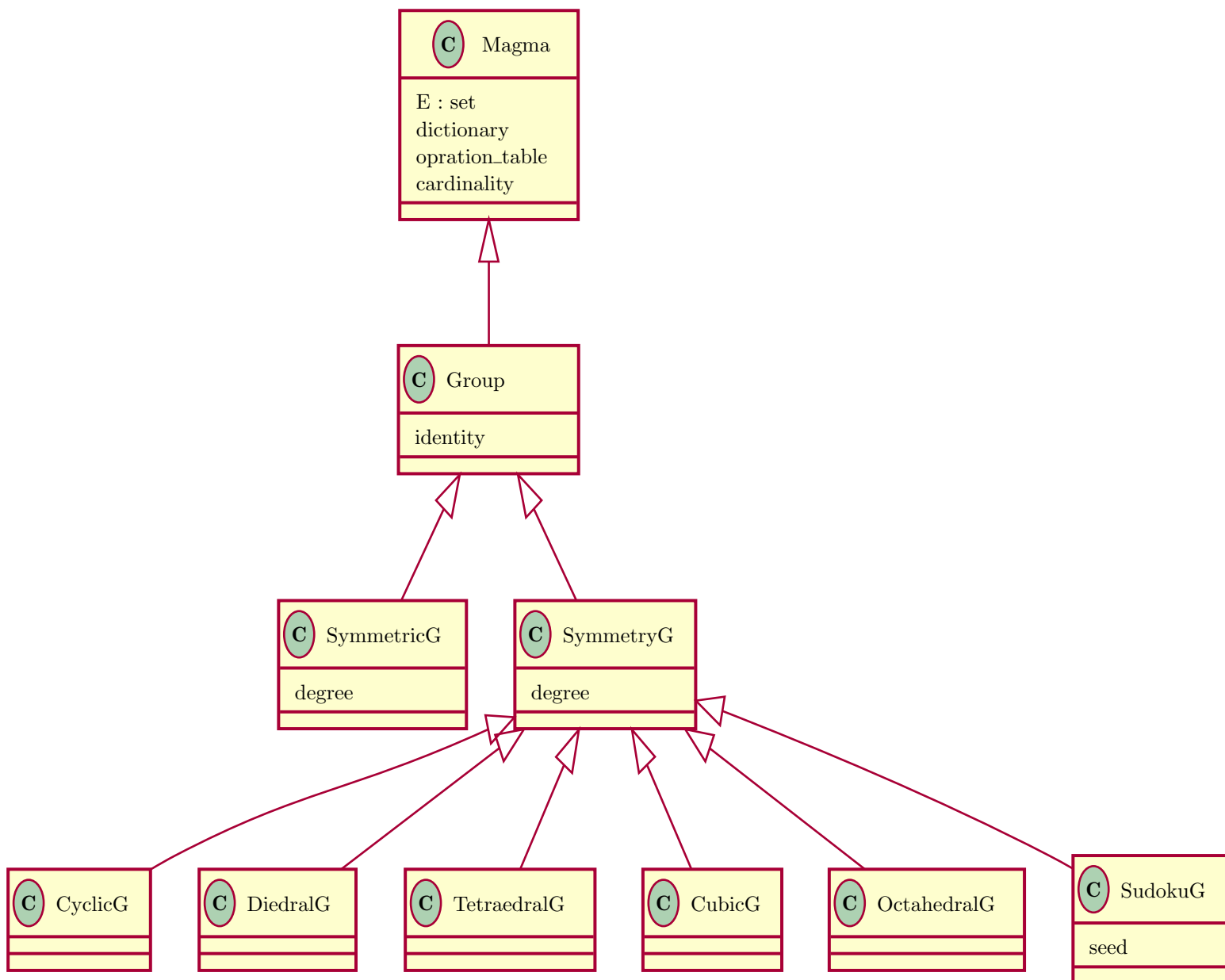


FIGURE 6.1 – Diagramme de classe.

Signification des champs **E** est l'ensemble des éléments du Magma. **operation_table** est une liste de listes représentant la loi de composition interne (plus de détails dans la docstring et la doctest du code). **dictionary** est utilisé pour accéder à un élément dans `operation_table` par son indice (complexité en $O(1)$). **cardinality** est la cardinalité du magma. **identity** est l'élément neutre du groupe. **degree** est le degré du groupe de permutation, qui représente la taille de ses permutations. Finalement, **seed** signifie que le Sudoku est de taille $\text{seed}^2 \times \text{seed}^2$.

6.4 Exécution et utilisation

6.4.1 Exécution

Dans le répertoire racine. L'exécution se fait dans un terminal avec la ligne de commande :

```
python3 __init__.py
```

6.4.2 Utilisation de CyclicGroup, DihedralGroup, CubicGroup et OctahedralGroup

Après avoir initialisé le groupe l'utilisateur peut :

- voir tous les éléments du groupe (qui sont des permutations).
- décomposer les permutations en cycles.
- voir le polynôme indicateur de cycles.
- appliquer le lemme de Burnside sur les colorations avec au plus k couleurs ou avec exactement k couleurs. (Sinon l'utilisateur peut créer lui même l'ensemble de colorations selon ses contraintes).
- appliquer le théorème de polya sans contraintes de poids.

Exemple 1 : Coloration de colliers

```
NB_PEARLS = 9
NB_COLORS = 3
colorations = Util.all_colorations(NB_PEARLS, NB_COLORS)
G = CyclicGroup(NB_PEARLS)
print(G.polynome)
print(G.orbits_number(colorations))
```

Out : $\frac{x_1^9 + 2x_3^3 + 6x_9}{9}$
2195

Exemple 2 : Coloration de cubes

```
NB_FACES = 6
NB_COLORS = 5
colorations = Util.all_colorations(NB_FACES, NB_COLORS)
G = CubicGroup.CubicGroup()
print(G.polynome)
print(G.orbits_number(colorations))
```

Out : $\frac{x_1^6 + 3x_1^2x_2^2 + 6x_1^2x_4 + 6x_2^3 + 8x_3^2}{24}$
800

6.4.3 Utilisation de SudokuGroup

Nous avons vu dans le chapitre précédent (corollaire 5.1), que l'ordre du $\text{SudokuGroup}(n)$ sans rénumérotation de chiffres est de taille $(n!)^{2n+2} \times 2$. Notre code le construit rapidement pour $n = 2$. Mais pour $n = 3$, le temps d'exécution n'est pas encore estimé (plusieurs heures).

Le programme affiche en un peu plus d'une seconde tous les éléments sous forme de permutations ou de produits de cycles. Il peut aussi afficher le polynôme. Mais il ne peut pas dénombrer les grilles.

Exemple 1 : Ordre du groupe

```
import time
t1 = time.time()
G = SudokuGroup.SudokuGroup(2)
print(G.cardinality)
t2 = time.time()
print(t2 - t1)
```

Out : 128

1.3681156635284424

Exemple 2 : Indicateur de cycles

```
import time
t1 = time.time()
G = SudokuGroup.SudokuGroup(2)
print(G.polynome)
t2 = time.time()
print(t2 - t1)
```

Out :
$$\frac{x_1^{16} + 4x_1^8x_2^4 + 12x_1^4x_2^6 + 16x_1^2x_2x_4^3 + 27x_2^8 + 52x_4^4 + 16x_8^2}{128}$$

1.5655910968780518

6.5 Complexité dans \mathfrak{S}_n

La construction de \mathfrak{S}_n est très coûteuse, mais la cythonisation donne les résultats suivants :

n	1	2	3	4	5	6	7	8
temps	0.0	0.0	0.0	0.000999s	0.021993s	0.329908s	16.944397	1h 10min

TABLE 6.2 – Temps de construction de \mathfrak{S}_n en Cython.

Remarque 6.1. *La classe Magma possède la méthode `is_groupe()` qui teste si un ensemble muni d'une loi de composition interne est un groupe. Nous l'avons utilisée pour tester tous les groupes implémentés. Mais une fois les tests validés, nous les avons enlevés pour gagner en efficacité car ils sont très coûteux. Ainsi, les temps d'exécution enregistrés correspondent à l'exécution sans ce test.*

Conclusion

Le dénombrement d'objets non équivalents trouve ses applications dans une multitude de problèmes. Nous avons pu résoudre le problème de coloration des colliers, des polygones et des cinq solides de Platon. Nous avons présenté le problème de dénombrement des Sudokus, et nous avons implémenté le groupe correspondant mais nous n'avons pas eu le temps de le résoudre.

Pour appliquer le lemme de Burnside, il faut compter le nombre d'objets fixes par chaque transformation, mais ce n'est pas simple ! Nous avons prouvé, dans le cas le plus simple des colorations avec k couleurs, que le nombre de colorations fixes par une permutation se décomposant en c cycles, est égal à k^c . Mais la décomposition en cycles de toutes les permutations nous donne aussi le polynôme indicateur de cycles qui nous permet d'appliquer le théorème de Pólya. Et donc appliquer le lemme de Burnside ou le théorème de Pólya dans ce cas revient à faire le même calcul.

Dans le cas des colorations avec contraintes, nous avons appliqué la version pondérée du théorème de Pólya en considérant que le poids d'une couleur est la couleur elle-même. Et nous avons vu qu'il est très élégant et facile à appliquer.

Nous n'avons pas eu le temps d'appliquer la version pondérée du lemme de Burnside sur des problèmes de dénombrements, mais nous l'avons utilisé pour prouver le théorème de Pólya.

A Triangle de Pascal

$n \backslash k$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0
2	1	2	1	0	0	0	0	0	0	0	0	0	0	0	0
3	1	3	3	1	0	0	0	0	0	0	0	0	0	0	0
4	1	4	6	4	1	0	0	0	0	0	0	0	0	0	0
5	1	5	10	10	5	1	0	0	0	0	0	0	0	0	0
6	1	6	15	20	15	6	1	0	0	0	0	0	0	0	0
7	1	7	21	35	35	21	7	1	0	0	0	0	0	0	0
8	1	8	28	56	70	56	28	8	1	0	0	0	0	0	0
9	1	9	36	84	126	126	84	36	9	1	0	0	0	0	0
10	1	10	45	120	210	252	210	120	45	10	1	0	0	0	0
11	1	11	55	165	330	462	462	330	165	55	11	1	0	0	0
12	1	12	66	220	495	792	924	792	495	220	66	12	1	0	0
13	1	13	78	286	715	1287	1716	1716	1287	715	286	78	13	1	0
14	1	14	91	364	1001	2002	3003	3432	3003	2002	1001	364	91	14	1

TABLE A.1 – 15 premières lignes du triangle de Pascal.

B Suites des solides de Platon

B.1 Tétraèdre

k	$\mathcal{A}_T(k)$	k	$\mathcal{A}_T(k)$
0	0	24	28176
1	1	25	33125
2	5	26	38701
3	15	27	44955
4	36	28	51940
5	75	29	59711
6	141	30	68325
7	245	31	77841
8	400	32	88320
9	621	33	99825
10	925	34	112421
11	1331	35	126175
12	1860	36	141156
13	2535	37	157435
14	3381	38	175085
15	4425	39	194181
16	5696	40	214800
17	7225	41	237021
18	9045	42	260925
19	11191	43	286595
20	13700	44	314116
21	16611	45	343575
22	19965	46	375061
23	23805	47	408665

TABLE B.1 – 48 premiers termes de la suite du tétraèdre.

B.2 Cube et octaèdre

k	$\mathcal{A}_{Cube}(k)$	k	$\mathcal{A}_{Octa}(k)$
0	0	0	0
1	1	1	1
2	10	2	23
3	57	3	333
4	240	4	2916
5	800	5	16725
6	2226	6	70911
7	5390	7	241913
8	11712	8	701968
9	23355	9	1798281
10	43450	10	4173775
11	76351	11	8942021
12	127920	12	17930628
13	205842	13	34009053
14	319970	14	61518471
15	482700	15	106823025
16	709376	16	179003456
17	1018725	17	290715793
18	1433322	18	459239463
19	1980085	19	707740861
20	2690800	20	1066780100
21	3602676	21	1576090341
22	4758930	22	2286660783
23	6209402	23	3263156073
24	8011200	24	4586706576
25	10229375	25	6358105625
26	12937626	26	8701451551
27	16219035	27	11768273973
28	20166832	28	15742185508
29	24885190	29	20844101741

TABLE B.2 – 30 premiers termes des suites du cube et de l’octaèdre.

B.3 Dodécaèdre et icosaèdre

k	$\mathcal{A}_{Dode}(k)$	k	$\mathcal{A}_{Ico}(k)$
0	0	0	0
1	1	1	1
2	96	2	19104
3	9099	3	58305015
4	280832	4	18331048448
5	4073375	5	1589541015875
6	36292320	6	60936714712224
7	230719293	7	1329875789342373
8	1145393152	8	19215381585043456
9	4707296613	9	202627852665826365
10	16666924000	10	1666667002500004000
11	52307593239	11	11212500968169821067
12	148602435840	12	63896002861637417472
13	388302646355	13	316749404048506332527
14	944900450144	14	1394470942725031163552
15	2162441849625	15	5542094593525693379625
16	4691253854208	16	20148763754343689748480
17	9710376716137	17	67737190305504286291801
18	9280531603808	18	212470603993104380231328
19	36888593841475	19	626499558365070376194559
20	68266682784000	20	1747626668034560000064000
21	122597146773927	21	4636973826571971618071163
22	214250072367584	22	11757158315731708261273760
23	365243777747861	23	28602597196225003820653709
24	608672505286656	24	66999811976199361219239936
25	993410807578125	25	151582450315380096435703125
26	1590482688592096	26	332135814952001763200326816
27	2501577352194831	27	706519304637019743120476499
28	3870304539076864	28	1462208743424537405574699520
29	5896913202648987	29	2949909602636539324506874983

TABLE B.3 – 30 premiers termes de la suite du dodécaèdre et de l'icosaèdre.

Bibliographie

- [1] CARLOS ARCOS, GARY BROOKFIELD, and MIKE KREBS. Mini-sudokus and groups. April 2010.
- [2] N. G. De Bruijn. Generalization of pólya's fundamental theorem in enumerative combinatorial analysis. December 1958.
- [3] William Burnside. Theory of groups of finite order. 1897.
- [4] Louis Comtet. *Analyse combinatoire*. Presses universitaires de France, 1970.
- [5] Frobenius and Ferdinand George. Ueber die nach einem congruenz aus zwei endlichen gruppen de doppelmodul. 1887.
- [6] Kyle Oddson. Counting and coloring sudoku graphs. Winter 2019.
- [7] George Pólya. Kombinatorische anzahlbestimmungen für gruppen, graphen und chemische verbindungen. 68(1), 1937.
- [8] Howard Redfield. The theory of group-reduced distributions. 49(3), 1927.
- [9] Ed Russell and Frazer Jarvis. There are 5472730538 essentially different sudoku grids. September 2005.
- [10] R. M. Wilson and J. H. Van Lint. *COURSE IN COMBINATORICS*. 1993.