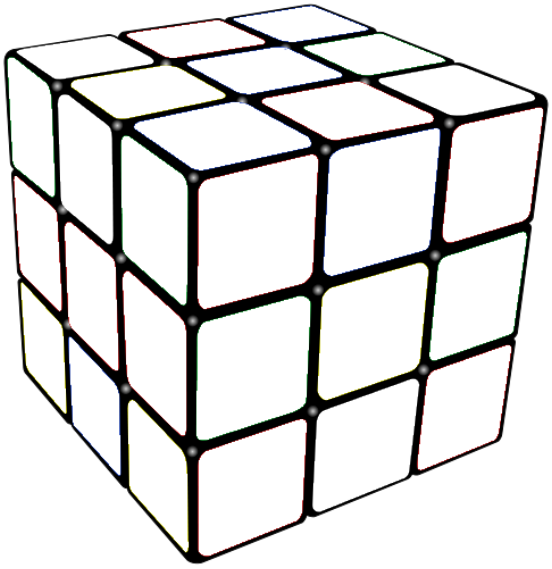
La théorie des groupes appliquée au Rubik's cube

Guillaume Carraux

Professeur accompagnant : Daniel Erspamer



Lycée-Collège de l'Abbaye
1890 St-Maurice

Septembre 2020

Résumé

Un Rubik's cube™est un puzzle très difficile. Dans ce travail, nous tenterons de montrer la structure mathématique qui se cache derrière un Rubik's cube et nous présenterons la théorie des groupes, comme un outil pour étudier de tels systèmes.

Tout d'abord, nous présenterons les bases de la théorie des groupes. Un groupe est un ensemble d'éléments liés par une opération et qui respecte certaines propriétés. A partir de cela, nous créerons des outils afin d'analyser un certain système : dans notre cas, c'est le Rubik's cube.

Ensuite, nous verrons les notions de bases d'un Rubik's cube, puis comment nous le transformerons en un groupe que nous pourrons ensuite étudier. Ce groupe tiendra compte de l'orientation de chaque pièce et de leur permutation (ou position sur le cube).

Finalement, nous construirons les éléments nécessaires pour le théorème fondamental concernant l'étude du Rubik's cube, puis nous le prouverons. Ce théorème décrit quand un état du cube est soluble ou non. Un programme informatique a été créé dans l'objet de ce travail et est utilisé pour poser les hypothèses du théorème.

source de l'image sur la page de titre : `https://www.pinterest.dk/pin/422986589980325562/`

Table des matières

Introduction

Il suffit de modifier une seule pièce d'un Rubik's cube pour que personne ne puisse résoudre le casse-tête. En effet, un Rubik's cube est loin d'être un simple puzzle dû à sa complexité mathématique. Beaucoup de recherches ont été faites, mais nous sommes encore loin de l'avoir entièrement analysé. Néanmoins, la majeure partie des énigmes rencontrées ont déjà été élucidées à l'aide de la théorie des groupes. Par exemple, Il a été prouvé avec cette théorie qu'il existe onze moyens différents de rendre un Rubik's cube impossible à résoudre.

La théorie des groupes permet à l'homme d'aborder et d'étudier des sujets demandant beaucoup d'abstraction. Un cube composé de plus petits cubes ne semble pas très abstrait, le système derrière lui l'est pourtant. D'ailleurs, ce système est un excellent exemple utilisé en théorie des groupes dû à sa polyvalence et sa complexité, qui est mise en lumière par la difficulté que l'on a en essayant de le résoudre. Si l'on demande à une personne sachant démêler ce casse-tête , elle répondra certainement qu'elle a appris des formules par cœur. Les méthodes de résolutions de ce type sont privilégiées car elle sont très rapides, et plus simple à apprendre. Néanmoins, avec de telles solutions, nous négligeons la plus grande partie de ce puzzle : la partie mathématique. L'application de la théorie des groupes permet de comprendre cette partie.

Dans ce travail, nous chercherons donc à former une intuition pour la compréhension du Rubik's cube à l'aide de bases de la théorie des groupes. L'étude de cette dernière permet d'aborder des systèmes élaborés et abstraits, pour les rendre plus simples à l'aide d'outils que nous créons nous-même. À travers l'application de la théorie des groupes sur le Rubik's cube, nous comprendrons en quoi un si petit jouet est en fait un objet mathématique complexe et mystérieux.

Chapitre 1

Théorie des groupes

Cette partie traverse les fondamentaux de la théorie des groupes dont nous avons besoin pour la suite. Tout n'est pas prouvé, mais l'idée intuitive est suffisante pour comprendre les notions introduites.

1.1 Groupe

Qu'est-ce qu'un groupe ? *Un groupe* est un ensemble d'éléments, qu'ils soient des nombres, des lettres, des fruits, des meubles,...Un groupe doit aussi avoir une opération, qui nous permet de joindre deux éléments pour en obtenir un troisième. Cette opération est définie pour chaque paire d'éléments du groupe. L'opération se nomme aussi *loi de composition*.

La notation de l'opération entre deux éléments a et b est libre, mais on retrouve souvent $a \circ b$ (a composé avec b), $a * b$ ou $a + b$. Le symbole de l'opération est libre, comme le nom des éléments. Lorsqu'il n'y a pas de risque de se tromper, nous pouvons simplement écrire ab au lieu de $a \circ b$ (ou tout autre symbole d'opération). Une lettre majuscule, le plus souvent G, est utilisée pour nommer le groupe.

Un groupe doit respecter 4 axiomes fondamentaux, suffisamment stricts pour pouvoir en tirer des informations, et suffisamment libres pour s'appliquer à une grande quantité d'ensembles. Les 4 axiomes sont, pour un groupe G :

1. *composition interne* : $a, b \in G \Rightarrow a \circ b \in G$
   L'opération doit renvoyer un élément du groupe. Lorsque l'on crée un groupe, il semble logique que l'opération ne renvoie pas un nouvel élément que nous devons inventer.
2. *associativité* : $a, b, c \in G \Rightarrow (a \circ b) \circ c = a \circ (b \circ c)$
   Il n'y a pas de priorité $a \circ b$ ou $b \circ c$ en premier. Cela nous permet d'écrire plus simplement $a \circ b \circ c$ pour alléger la notation.
3. *élément neutre* : $\exists e \in G \mid a \circ e = e \circ a = a,\ \forall a \in G$
   Ce terme prend en général la forme $1, 0, e, E$ ou i. On le trouve parfois sous le nom d'élément neutre.
4. *inverse* : $\forall a \in G, \exists a^{-1} \in G \mid a \circ a^{-1} = a^{-1} \circ a = e$, où e est l'élément neutre.
   L'inverse peut prendre une forme différente de a^{-1}. Par exemple, si a est un nombre et que l'opération est l'addition, nous écrivons plutôt $-a$ comme inverse de a.

Attention, a^{-1} ne prend pas le même sens qu'en algèbre, il représente l'élément qui, composé avec a, renvoie l'élément neutre. $a^{-1} = 1/a$ ne fait du sens uniquement lorsque a est un nombre avec multiplication comme opération. De plus, un élément peut être son propre inverse. Par exemple, si l'élément est une rotation de 180 degrés d'un carré, appliquer deux fois cette élément est équivalent à une rotation de 0 degré, donc l'élément neutre.

Notons qu'un groupe n'est pas forcément commutatif. On dit de ce type de groupe qu'il est *abélien*. Un groupe G est commutatif si et seulement si $\forall a, b \in G, ab = ba$. L'addition est commutative, mais la division ne l'est pas ($3/5 \neq 5/3$). La majorité des groupes ne sont pas abéliens.

exemple de groupe

Afin de clarifier cette notion très importante, construisons ensemble un groupe simple.

Le groupe des entiers relatifs sous addition est un excellent exemple pour introduire la notion de groupe. Voyons comment ce groupe peut se construire tout seul : Nous voulons un groupe G avec l'addition comme opération. Le troisième axiome fondamental dit qu'il faut un élément neutre, qui est le nombre 0 dans le cas de l'addition. En réalité, 0 suffit à lui tout seul pour faire un groupe. Néanmoins, l'étude de ce groupe ne nous apporte rien de plus que nous savons déjà. Un tel groupe est dit *trivial*.

Ajoutons donc des éléments dans notre groupe G, prenons 1. En suivant le premier axiome, si l'on additionne deux éléments quelconques du groupe, nous devons obtenir un élément qui en fait aussi partie. Si l'on prend $1 + 0$, on retrouve 1, qui est déjà dans le groupe. Si l'on prend $1 + 1$ on trouve 2. Il nous faut donc ajouter l'élément 2 dans notre groupe pour respecter les axiomes. Ensuite, en additionnant 1 et 2, on obtient 3, qu'il faut aussi ajouter au groupe, et ainsi de suite. Nous avons maintenant tous les entiers positifs.

Malheureusement, l'axiome des inverses n'est pas respecté, nous devons donc ajouter -1 comme inverse de 1, -2 comme inverse de 2,.... De plus, nos connaissances de l'arithmétique de base nous permettent de dire que l'addition est associative. Comme les quatres axiomes fondamentaux sont respectés, nous avons prouvé que les entiers relatifs sous l'addition est un groupe, noté $(\mathbb{Z}, +)$.

1.2 Groupe de symétrie

Le type de groupe suivant nécessite une notion nécessaire pour la suite : les permutations. Définissons donc en premier lieu ce terme.

Pour un ensemble de n éléments quelconques, prenons $\{1, 2, 3, \ldots, n\}$, *une permutation* de cet ensemble est un réarrangement de l'ordre de ses éléments. Nous pouvons aussi exprimer une permutation graphiquement pour une meilleure compréhension.. Pour $n = 5$, ceci est un exemple de permutation.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix}$$

La ligne supérieure indique la place d'origine, la ligne inférieure indique la place finale. Dans cette permutation, le 1 va à la place du 4, le 2 ne change pas,...

Notons que la permutation ci-dessous est la même que cette dernière, à l'exception des symboles utilisés.

$$\begin{pmatrix} \alpha & \beta & \gamma & \delta & \epsilon \\ \delta & \beta & \epsilon & \gamma & \alpha \end{pmatrix}$$

En effet, si l'on remplace dans la première permutation les symboles 1,2,3,4 et 5 respectivement par α,β,γ,δ et ϵ, on retrouve exactement la même permutation. Les déplacements restent les mêmes, donc la structure mathématique de la permutation ne change pas.

Le groupe de symétrie S_n d'un ensemble de n éléments est l'ensemble des permutations possibles des éléments de cet ensemble. L'opération d'un tel groupe est la composition de permutations. En d'autres termes, lorsque nous voulons composer une permutation a avec une permutation b, nous effectuons b, puis a, et nous observons comment les éléments ont été permutés. [1]

Prenons par exemple $n = 2$ et regardons l'ensemble des permutations possibles sur l'ensemble $\{1, 2\}$. La première est l'élément neutre : $\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$. Chaque élément se renvoie lui-même, donc l'application de cette permutation ne change rien. Par convention, appelons cette permutation e.

La seule autre permutation possible est $\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$. Lorsque uniquement deux éléments sont échangés, nous appelons cette permutation une transposition, souvent notée τ.
Il ne reste aucune autre permutation possible, nous avons donc nos éléments du groupe $S_2 = \{e, \tau\}$.

Nous allons maintenant montrer, non pas rigoureusement, mais par l'intuition que S_n respecte les 4 axiomes fondamentaux, pour tout n entier naturel.

1. 1^{er} axiome : composition interne. Une permutation de n éléments suivie d'une seconde permutation sur les mêmes n éléments ne peut qu'être une autre permutation de ces n éléments. Nous changeons leur ordre deux fois à la suite, ce qui revient à faire un certain changement d'ordre qui atteint le même résultat, qui reste une permutation.

2. 2^e axiome : associativité. La permutation d'un ensemble A de n éléments peut être considéré comme une fonction de A sur A (une fonction qui renvoie l'emplacement final du paramètre de la fonction. Dans l'exemple effectué plus haut, $P(1) = 4$, si P est la fonction qui représente cette permutation). Effectuer une permutation après une autre devient simplement une composition de deux fonctions sur l'ensemble A. Or, nous savons que la composition de fonction est associative, donc la composition de permutations est associative.

3. 3^e axiome : élément neutre. C'est la permutation où rien ne change, par

1. En général, les permutations s'effectuent de droite à gauche (ici b puis a). Dans le cas du Rubik's cube, nous les lirons et effectuerons de gauche à droite par convention. S_n est non-abélien pour $n > 2$, il est donc important de ne pas se tromper de sens.

exemple $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$ dans S_5. Il est évident que ce type de permutation existe toujours, et que l'effectuer avant ou après une autre permutation σ ne changera rien à σ.

4. 4^e axiome : inverses. Une permutation $\sigma \in S_n$ est bijective, donc un inverse σ^{-1} doit aussi exister. Or, cet inverse agit aussi sur un nombre d'éléments n, donc $\sigma^{-1} \in S_n$, pour tout $\sigma \in S_n$

Le nombre d'éléments d'un groupe G, noté $|G|$, se nomme son *ordre*. Le nombre d'éléments se trouvant dans S_n est le nombre de permutations possibles de n éléments, donc $|S_n| = n!$.

L'ordre d'un groupe peut aussi être infini, et dans ce cas les mêmes règles s'appliquent.

1.3 Groupe cyclique

Un autre type de groupe est le *groupe cyclique* de n éléments ($n \geq 0$), noté $\mathbb{Z}_n$. Le groupe est composé des éléments $\{0, 1, 2, 3, \ldots, n-1\}$ et l'opération liée à ce groupe est l'addition modulo n (si la somme de nos deux éléments est plus grande ou égale à n, nous y soustrayons n jusqu'à obtenir un nombre positif inférieur à n).

Le groupe $\mathbb{Z}_3$, par exemple, est composé des éléments $\{0, 1, 2\}$ et l'opération, la somme modulo 3 de ces nombres, ne dépasse jamais 2 : $2 + 1 = 0 \pmod 3$.

1.4 Décomposition en cycle

Une permutation est parfois compliquée à décrire, c'est pourquoi une notation plus légère a été créée, comprenant toutes les informations nécessaires. Au lieu d'écrire $\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 3 & 6 & 1 & 4 \end{pmatrix}$, on écrira (1 2 5)(4 6). Voici un exemple de transcription en cycles. Prenons la permutation ci-dessus. Regardons ce que renvoie le premier élément : 2. Puis 2 devient 5. Enfin 5 redevient 1. Le premier cycle est alors (1 2 5). Le prochain élément que l'on n'a pas encore utilisé est 3, qui devient 3, le cycle est déjà fini. Nous avons maintenant (1 2 5)(3). Il reste 4 qui devient 6, puis 6 devient 4. Ajoutons donc le dernier cycle pour avoir (1 2 5)(3)(4 6). Enlevons finalement le cycle de 1 élément, qui ne nous intéresse pas car il ne change rien. Le résultat final est (1 2 5)(4 6).

L'ensemble des éléments se trouvant dans une parenthèse est un *cycle*. Un cycle de n éléments est un *n-cycle*. Le cycle (1 2 5) signifie que si l'on applique la permutation σ sur l'élément 1 plusieurs fois de suite, on obtient $\sigma(1) = 2$, puis $\sigma(\sigma(1)) = 5$, puis $\sigma(\sigma(\sigma(1))) = 1$, où le cycle recommence.

1.5 Signe d'une permutation

Le signe d'une permutation est le nombre -1 ou 1. On peut le déterminer en étudiant la décomposition en cycle de cette permutation. [2]

Voyons un exemple : Soit α une permutation, telle que sa décomposition en cycle est (1 3 4)(2 6). Prenons pour chaque cycle le nombre d'éléments puis soustrayons 1, puis effectuons la somme de ces nombres. Dans le cas de α, le premier est un 3-cycle et le deuxième un 2-cycle. Le nombre final est $(3-1)+(2-1)=3$.
3 est impair, donc la permutation α est impaire et son signe est -1. Si le nombre était pair, la permutation serait paire et son signe serait 1. On écrit aussi $sign(\alpha) = -1$.

1.6 Sous-groupes et classes suivant un sous-groupe

Un sous-groupe H de G est un sous ensemble de G et est aussi un groupe : Deux éléments de H composés ensemble doivent renvoyer un élément de H (l'opération du sous-groupe est la même que celle du groupe). Un sous-groupe est toujours associatif, car le groupe d'origine l'est. (par l'absurde, si H n'était pas associatif, G ne le serait pas, donc ne serait pas un groupe). Le sous-groupe doit contenir l'élément neutre (qui est donc la même que celle de G). Finalement, le sous-groupe doit contenir les inverses de ses éléments.

Nous pouvons donc appliquer tout ce que nous savons des groupes aux sous-groupes, car ils respectent les conditions.

Notons que l'élément neutre est toujours un sous-groupe de son groupe d'origine (que l'on appelle le sous-groupe trivial), et le groupe G est aussi toujours un sous-groupe de G. $H \leq G$ signifie que H est un sous-groupe de G. [3]

Prenons par exemple le groupe des nombres relatifs sous l'addition : $(\mathbb{Z}, +)$. Un de ses nombreux sous-groupes est noté $(2\mathbb{Z}, +)$, qui représente les nombres pairs $(2*0, 2*1, 2*(-1), 2*2, \dots)$. La somme de deux nombres pairs donne un nombre pair, il est associatif car son groupe d'origine l'est, il contient l'élément neutre (0) et l'inverse des nombres pairs y sont aussi. Nous pouvons agir de même pour $3\mathbb{Z}$, $4\mathbb{Z}$,... : $n\mathbb{Z}$, $n = 1, 2, 3....$ Nous avons ici prouvé que le sous-ensemble $(2\mathbb{Z}, +)$ du groupe $(\mathbb{Z}, +)$ est un de ses sous-groupes.

Un sous-groupe est aussi un outil pour séparer le groupe en parties, que l'on appelle les classes suivant un sous-groupe.

Ces classes sont uniques pour un certain sous-groupe. Voyons comment les déterminer : Soit un groupe G, et un sous-groupe $H < G$. Prenons un élément a à l'extérieur de H, puis composons a avec tous les éléments de H. Nous obtenons l'ensemble $aH = \{ah \mid h \in H\}$. Ici, notons un fait important : si l'on choisit un élément $b \in aH$, et que l'on construit bH (selon les mêmes règles que pour aH), nous pouvons observer que $aH = bH$, pour n'importe quel $b \in aH$!

Cette propriété tient car pour un élément quelconque $b \in aH$, b est de forme $b = ah$, $h \in H$ car $aH = \{ah | h \in H\}$. Construisons maintenant $bH = \{(ah)h_2 | h_2 \in H\}$. Or, $\{hh_2 \mid h_2 \in H\} = hH = H$, donc $bH = ahH = aH$, $\forall b \in aH$. Afin de se

2. On dit aussi qu'une permutation est paire si son signe est 1, impaire si son signe est -1.

3. En écrivant $H \leq G$, on admet que H peut être G lui-même. Pour éviter cela, nous pouvons noter $H < G$.

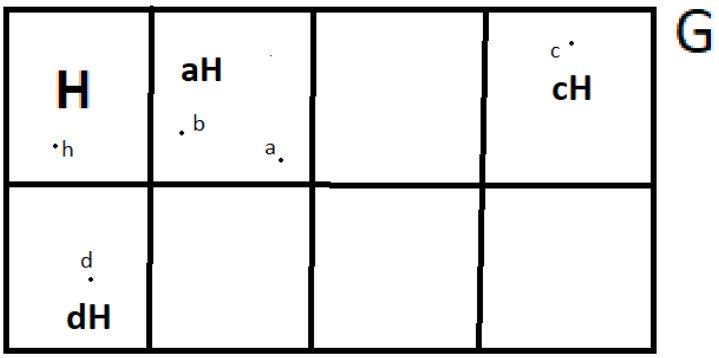


FIGURE 1.1 – représentation graphique d'un découpage d'un groupe en classes suivant un sous-groupe. Le découpage continue avec d'autres classes telles que cH, dH,...

représenter le découpage du groupe plus simplement, le lecteur peut se référer à la figure 1.1, qui représente le groupe G, découpé en plusieurs classes.

Cela signifie que l'élément choisi pour construire aH n'est pas important, et que la composition d'un élément de aH avec un élément de H donnera toujours un élément dans aH.

Ensuite tant qu'il reste des éléments ne faisant pas partie de H ou d'un des ensembles créés, composons les avec H pour créer une nouvelle classe. [4]

Le résultat final est notre groupe G partagé en plusieurs sous-ensembles, que l'on appelle les *classes suivant le sous-groupe* H. Il est important de noter que ces classes ne partagent aucun élément entre elles, car un élément c dans une classe aH, après composition avec tous les éléments de H, ne peut que recréer aH et non une autre classe. De plus, chaque classe a le même nombre d'éléments que H car ces classes sont de la forme $aH = \{ah \mid h \in H\}$, donc un élément a composé avec un élément de H. Nous obtenons un résultat différent pour un h différent (car si $ah_1 = ah_2$ et $h_1 \neq h_2$, nous pouvons composer par l'inverse de a la première équation : $a^{-1}ah_1 = a^{-1}ah_2$ pour obtenir $h_1 = h_2$. Donc h_1 et h_2 doivent être le même élément). Nous avons ici montré que toutes les classes suivant H ont le même nombre d'éléments que H.

Peu importe quels éléments ont été choisis à chaque fois, nous finissons toujours avec les mêmes ensembles. Il y a toutefois deux types de classes suivant H. Dans la description du procédé ci-dessus, nous avons créé les *classes à gauche* car nous avons composé H à h à gauche (aH), il est aussi possible de composer à droite pour obtenir les *classes à droite* suivant H (Ha). Il existe ces deux types de classe car G n'est pas forcément abélien, donc $aH \neq Ha$ dans la majorité des groupes, ce qui nous amène à créer des classes différentes. [5]

4. Si l'on prend un élément intérieur à H et que nous le composons à H, l'ensemble final ne pourra être que H.

5. Cette partie ainsi que le paragraphe suivant ne sont pas entièrement prouvés afin que cette introduction à la théorie des groupes reste une introduction. Nous ne posons ici que les concepts de base.

Pour un sous-groupe $H < G$, nous pouvons donc décomposer G en un certain nombre de classes suivant H. Notons que H fait partie de l'ensemble des classes car on peut le construire comme ces dernières.

1.6.1 Théorème de Lagrange

Une conséquence majeure de l'existence des classes suivant un sous-groupe est le théorème de Lagrange : soit un groupe G, et un sous-groupe $H \leq G$, le théorème établit que $|G| = n|H|$ où $n \in \mathbb{N}$ est le nombre de classes (à gauche ou à droite) suivant H.[6]

Ce théorème se démontre simplement : les classes ont toutes le même nombre d'éléments que H, elles ne partagent aucun élément et chaque élément du groupe G appartient à une classe, donc $|H|$ doit être un multiple de G.

Ce théorème est un outil pratique pour trouver les sous-groupes d'un certain groupe. Par exemple, nous savons que si $|G| = p$ (p est un nombre premier), G ne peut avoir que des sous-groupes d'ordre 1 et p (les seuls nombres qui peuvent diviser p). Or, le seul groupe d'ordre 1 est le groupe trivial $\{e\}$, et le seul sous-groupe d'ordre p dans G est G lui-même car notre sous-groupe doit contenir tous les élément de G pour avoir p éléments.

1.7 Produit direct de groupes

Soient deux groupes G_1 et G_2, nous pouvons composer ces groupes avec l'analogue du produit cartésien pour la théorie des groupes : le produit direct. Le produit direct de G_1 et G_2 est $G_1 \times G_2 = \{(g_1, g_2) \mid g_1 \in G_1 \text{ et } g_2 \in G_2\}$. Le produit direct de G_1 et G_2 est donc l'ensemble des paires que l'on peut former avec les éléments de G_1 et de G_2. Dans ce nouveau groupe créé par G_1 et G_2, l'opération de ce nouveau groupe vient de l'opération des groupes d'origine : Pour tout (a_1, b_1) et (a_2, b_2) dans $G_1 \times G_2$ (donc $a_1, a_2 \in G_1$ et $b_1, b_2 \in G_2$), l'opération est définie par $(a_1, b_1) \circ (a_2, b_2) = (a_1 a_2, b_1 b_2)$. La loi de composition entre a_1 et a_2 est celle de G_1 et la loi de composition entre b_1 et b_2 est celle de G_2.

Vérifions que le produit direct de deux groupes est toujours un groupe :

1. Composition interne : Dans $(a_1 a_2, b_1 b_2)$, $a_1 a_2 \in G_1$ car G_1 est un groupe et $b_1 b_2 \in G_2$ car G_2 est un groupe. Nous avons donc bien un élément de la forme (g_1, g_2) tel que $g_1 \in G_1$ et $g_2 \in G_2$
2. Associativité : De la même manière, le groupe est associatif car il est composé d'autres groupes, qui sont eux-mêmes associatifs. Montrons simplement cela : $((a_1, b_1) \circ (a_2, b_2)) \circ (a_3, b_3) = ((a_1 a_2) a_3, (b_1 b_2) b_3)$ par définition, puis, car G_1 et G_2 sont des groupes : $((a_1 a_2) a_3, (b_1 b_2) b_3) = (a_1 (a_2 a_3), b_1 (b_2 b_3))$. Finalement : $(a_1 (a_2 a_3), b_1 (b_2 b_3)) = (a_1, b_1) \circ ((a_2, b_2) \circ (a_3, b_3)$.
3. Elément neutre : L'élément neutre de $G_1 \times G_2$ est celui comprenant l'élément neutre de G_1 et de G_2, prenons respectivement e_1 et e_2. $(e_1, e_2) \circ (a_1, b_1) = (e_1 a_1, e_2 b_1) = (a_1, b_1)$. (La démonstration est équivalente pour la composition avec l'élément neutre par la droite)

6. Le théorème est parfois formulé autrement : si $H \leq G$, alors $|H|$ divise $|G|$

4. Inverse : L'élément inverse d'un élément (a, b) est (a^{-1}, b^{-1}). Nous pouvons le voir ici : $(a, b) \circ (a^{-1}, b^{-1}) = (aa^{-1}, bb^{-1}) = (e_1, e_2)$ (Ici aussi, la preuve est équivalente pour la composition dans l'autre sens.)

Le même principe s'applique pour plus de deux groupes : G_1, G_2, ..., G_n. De la même manière que précédemment, nous pouvons créer le produit direct de ces n groupes :

$$G_1 \times G_2 \times \cdots \times G_n = \{(g_1, g_2, \ldots, g_n) \mid g_1 \in G_1, g_2 \in G_2, \ldots, g_n \in G_n\}$$

L'ordre de $G_1 \times G_2 \times G_3 \times \cdots \times G_n$ est le produit des ordres de chaque groupe : $|G_1 \times G_2 \times G_3 \times \cdots \times G_n| = |G_1||G_2||G_3| \ldots |G_n|$. C'est le cas par la propriété du cardinal du produit cartésien (Pauli, 2019).

Lorsque nous effectuons le produit d'un groupe G avec lui-même, nous pouvons noter $G^2 = G \times G$

Chapitre 2

Le Rubik's cube

Avant d'aborder l'application de la théorie des groupes au Rubik's cube, voyons quelques notions et notations.

2.1 notions de base

Qu'est-ce qu'un Rubik's cube ? Historiquement, c'est un célèbre puzzle inventé en 1974 par le Hongrois Ernö Rubik. Mathématiquement, un Rubik's cube est une excellente application de la théorie des groupes. Ce puzzle est un complexe mélange de beaucoup de notions de la théorie des groupes.

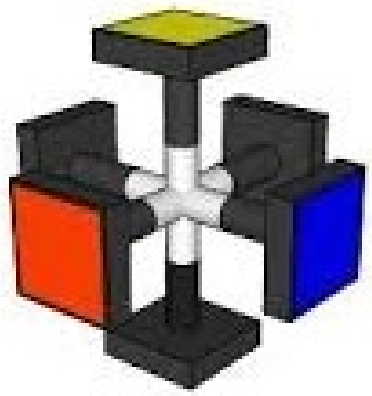


FIGURE 2.1 – Mécanisme intérieur du Rubik's cube. Les centres sont fixes et les autres pièces peuvent tourner.

Avant de le lier à la théorie des groupes, observons son fonctionnement. Le cube est composé de 26 *petits cubes* ($3*3*3-1$, «-1» correspond a l'emplacement central du cube), dont 12 arêtes (petits cubes avec 2 couleurs), 8 coins (petits cubes avec 3 couleurs) et 6 cubes centraux (petits cubes avec une seule couleur). Il est important de noter que les 6 faces du Rubik's cube sont déterminées par les faces centrales qui, elles, ne peuvent pas réellement se déplacer. La figure 2.1 montre le mécanisme

intérieur standard d'un cube. [1]

Les centres font partie de la base du cube, ils ne vont donc pas bouger [2]. Les autres pièces peuvent permuter librement car elles sont bloquées autour de ces centres. Les pièces coins ne peuvent se trouver que dans un coin car aucune rotation ne peut en mettre un à la place d'une arête. De même pour les pièces arêtes, elles ne peuvent que se retrouver dans un emplacement d'arête.

Le but de ce puzzle est de regrouper les couleurs, une par face. Nous avons vu que les centres ne bougent pas, nous pouvons donc les utiliser pour déterminer la couleur de chaque face.

Prenons un Rubik's cube devant nous. Afin de ne pas se perdre, nous prendrons toujours la même configuration initiale : Le Rubik's cube est résolu, la face blanche se trouve vers le haut et la face bleue vers la droite, nous avons forcément la face rouge face à nous. [3] La figure 2.2 illustre la position initiale.

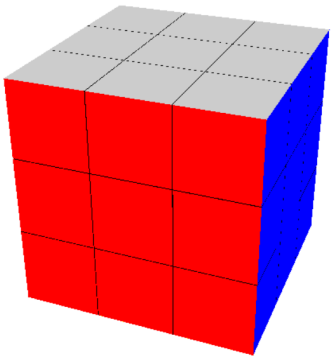


FIGURE 2.2 – Position initiale : blanc [4]en haut, bleu à droite, rouge en face

2.1.1 notation de Singmaster

La notation que nous utilisons pour décrire les mouvements de base du Rubik's cube est la notation de Singmaster, inventée par David Breyer Singmaster en 1978 (Frey et Singmaster, 1982). Chaque face a une lettre majuscule qui définit sa rotation dans le sens des aiguilles d'une montre. Une rotation dans le sens inverse est dénotée par la même lettre suivie de «$^{-1}$». Ces lettres sont les abréviations des mots anglais de chaque face :

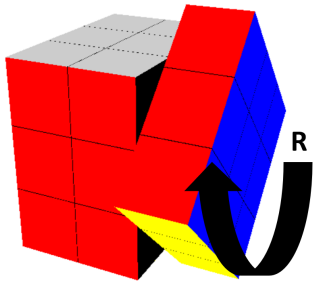
— Rotation de la face supérieure (face blanche) : U (= up)
— Rotation de la face de droite (face bleue) : R (= right)
— Rotation de la face avant (face rouge) : F (= front)

1. Certains nouveaux Rubik's cubes fonctionnent à l'aide d'aimants, ce qui rend la rotation plus rapide.

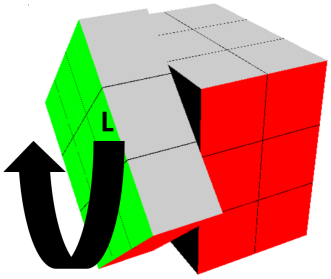
2. En réalité ils peuvent bouger, mais ils resteront toujours à la même place relativement aux autres centres. Nous n'utiliserons que des rotations des faces et non des centres, alors ces centres ne changerons jamais de position

3. Dans un Rubik's cube standard, les couleurs se font face de la manière suivante : blanc en face du jaune, vert en face du bleu et rouge en face du orange. D'autres cubes portent des couleurs différentes. La couleur n'est utilisée ici qu'à des fins de simplification, elle n'est pas réellement importante.

4. Ici, la face blanche est légèrement grisée pour contraster avec la page blanche.



(a) R : rotation de la face de droite



(b) L : rotation de la face de gauche

FIGURE 2.3 – Deux faces opposées tournent dans le sens des aiguilles d'une montre, mais vont dans un sens différent

— Rotation de la face inférieure (face jaune) : D (= down)
— Rotation de la face de gauche (face verte) : L (= left)
— Rotation de la face arrière (face orange) : B (= back)

Les couples de faces opposées (U-D, R-L, F-B) tournent dans un sens opposé car la rotation est dans le sens des aiguilles d'une montre lorsqu'on tient la face devant nous. Donc si l'on tourne le cube de 180 degrés pour avoir la face opposée devant nous, une rotation dans le sens des aiguilles d'une montre de celle-ci devient une rotation dans le sens inverse si l'on n'avait pas tourné pas le Rubik's cube de 180 degrés. La figure 2.3 illustre l'opposition du sens de rotation entre R et L.

Les inverses de ces mouvements sont donc U^{-1}, R^{-1}, F^{-1}, D^{-1}, L^{-1} et B^{-1}. Lorsque nous effectuons deux fois la même rotation à la suite, par exemple deux fois U, nous écrivons U^2 au lieu de UU. Effectuer trois fois une même rotation revient à faire son inverse ($U^3 = U^{-1}$), et l'effectuer quatre fois est équivalent à ne rien faire.

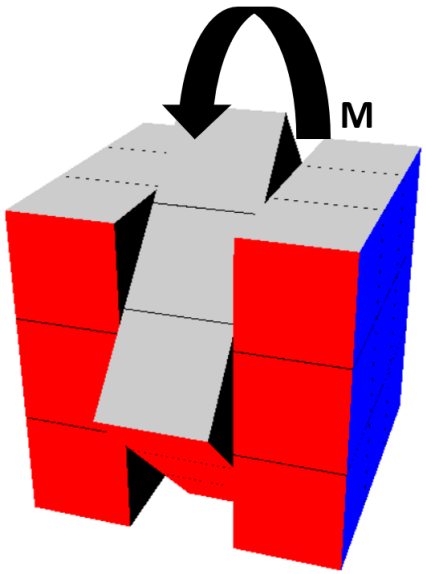


FIGURE 2.4 – Rotation M : entre R et L, dans le sens de L

D'autres rotations moins fréquentes sont les rotations des tranches centrales,

mais celles-ci peuvent être retrouvées à l'aide de deux rotations de base (exemple : figure 2.4).

Ces rotations de tranche centrale sont :
— Rotation de la tranche centrale entre U et D dans le sens de D : E (= equator)
— Rotation de la tranche centrale entre R et L dans le sens de L : M (= middle)
— Rotation de la tranche centrale entre F et B dans le sens de F : S (= standing)

Finalement, trois autres rotations simples existent, mais elles ne sont que rarement écrites : les rotations du cube entier : X, (rotation dans le sens de R), Y (rotation dans le sens de U) et Z (rotation dans le sens de F). [5]

2.2 Construction du groupe

Les éléments du groupe formé ici sont principalement inspirés du livre de Mulholland (2011) . Voyons d'abord tous les arrangements possibles d'un Rubik's cube [6]. Nous avons observé plus haut que chaque coin ne peut se retrouver que dans un emplacement de coin. Les permutations de ces coins forment donc le groupe de symétrie S_8 (car 8 éléments permutent librement entre eux). De même pour les arêtes, elles ne peuvent que permuter entre elles douze. Les permutations des 12 arêtes forment le groupe de symétrie S_{12}.

Le groupe décrivant l'ensemble des permutations possible des pièces du cube est le produit direct de S_{12} avec S_8.

Néanmoins, un Rubik's cube ne permute pas uniquement, chaque pièce (sauf les centres [7]) peut avoir plusieurs orientations différentes. Chaque coin peut (sans changer de place, toutes les permutations ont déjà été prisent en compte) avoir trois orientations possibles (figure 2.5). Nous pouvons observer que l'ensemble des orientations de ce coin forment le groupe $\mathbb{Z}_3$: Le coin peut varier entre trois états (orientations), que nous pouvons appeler état 0, état 1 et état 2. Lorsqu'on le fait tourner trois fois dans le même sens, le coin revient à son état initial, comme si l'on ajoute à chaque fois 1 (mod 3).

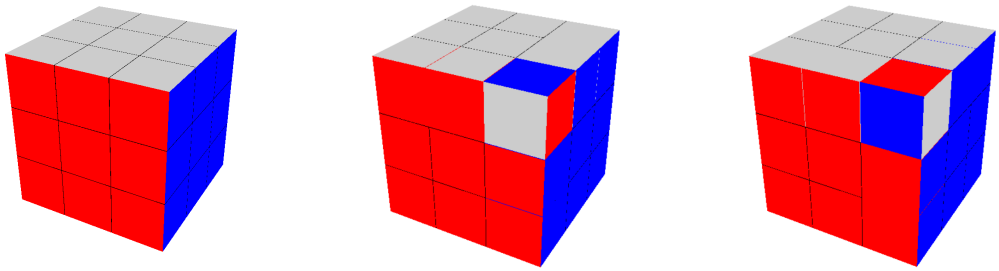


FIGURE 2.5 – Les trois orientations possibles d'un coin

5. Elles sont parfois notées $\mathcal{R}$ au lieu de X, $\mathcal{U}$ au lieu de Y et $\mathcal{F}$ au lieu de Z (par rapport au sens et à l'axe de rotation de R, U et F)

6. Tous les arrangements possibles prennent aussi en compte les arrangements que l'on ne peut obtenir avec des rotations de face, mais où il est nécessaire de démonter le Rubik's cube et le remonter dans la configuration souhaitée.

7. Les centres peuvent en réalité tourner sur eux-mêmes, mais cela ne nous intéresse pas car d'un point de vue visuel, le cube n'est pas changé.

Nous avons ensuite 8 coins, qui peuvent s'orienter librement, le groupe permettant toutes les orientations possibles de chaque coin est alors $\mathbb{Z}_3^8$ (produit direct de 8 fois le même groupe). Agissons de même avec les arêtes : Nous avons 12 arêtes, qui ont chacune deux orientations possibles. Pour une certaine arête, le groupe $\mathbb{Z}_2$ décrit ses orientations. Pour décrire l'ensemble des orientations des 12 arêtes, nous trouvons alors le groupe $\mathbb{Z}_2^{12}$.

Il suffit maintenant de coller tous les morceaux. Nous avons déjà le groupe $S_{12} \times S_8$ qui décrit l'ensemble des permutations des petits cubes. Ajoutons alors $\mathbb{Z}_3^8$ et $\mathbb{Z}_2^{12}$ pour obtenir tous les états possibles du cube :

$$RC_3^* = S_{12} \times S_8 \times \mathbb{Z}_3^8 \times \mathbb{Z}_2^{12}$$

Il ne manque qu'un élément pour transformer l'ensemble de combinaisons du cube RC_3^* en un groupe : une opération. Lorsqu'une combinaison α est composée avec une combinaison β, le résultat est l'état du cube après un enchainement de ces deux combinaisons. On ne peut pas réellement «enchainer des combinaisons» car une combinaison est un état et non une action. Cependant, on peut imaginer le processus utilisé afin de passer d'un Rubik's cube résolu à la combinaison désirée (par exemple une suite de rotations de faces du cube) et appliquer le procédé de α suivi de celui de β. Par exemple, si α est une rotation de la face supérieure et β une rotation de la face de droite, $\alpha\beta$ est la rotation de la face supérieure suivie de la rotation de la face de droite.

La construction du groupe RC_3^* est terminée. RC_3^* est en effet un groupe car les éléments qui le constituent (S_{12}, S_8, $\mathbb{Z}_3^8$ et $\mathbb{Z}_2^{12}$) sont eux-mêmes des groupes. Nous avons prouvé à la section 1.7 que le produit direct de groupes était lui aussi un groupe.

L'élément neutre E de RC_3^* est le Rubik's cube résolu car il ne faut rien faire pour passer d'un cube résolu à lui-même. L'action «ne rien faire» peut être effectuée avant ou après une autre combinaison et cette dernière ne sera évidemment pas changée.

L'inverse d'un mouvement simple, par exemple la rotation d'une face, est la même rotation dans le sens inverse. Pour un mouvement plus complexe, tel un enchainement de plusieurs rotations, faire l'inverse revient à faire toutes les mêmes rotations à l'envers, en commençant par la fin. Par exemple, prenons l'enchainement $\mu = RUF^{-1}D$. On peut déduire que $\mu^{-1} = D^{-1}FU^{-1}R^{-1}$ car si on les enchaine, on obtient l'élément neutre : $\mu\mu^{-1} = (RUF^{-1}D)(D^{-1}FU^{-1}R^{-1}) = RUF^{-1}DD^{-1}FU^{-1}R^{-1}$. Or, $DD^{-1} = E$, il reste alors $RUF^{-1}FU^{-1}R^{-1}$. Ici aussi, $F^{-1}F = E$. Nous pouvons continuer à annuler les paires de mouvements inverses jusqu'à l'élément neutre. [8]

2.3 Groupe entier et groupe légal

Dans la construction du groupe du Rubik's cube effectuée dans la section précédente, nous avons admis toutes les combinaisons possibles du cube, alors qu'elles ne sont pas toutes accessibles avec uniquement des rotations, il faudrait pour certaines d'entre elles démonter le cube puis le remonter dans la combinaison souhaitée. Un état accessible avec des rotations de face est appelé un état légal du cube.

8. Il n'est pas important de comprendre exactement ces rotations. Elles sont néanmoins décrites dans la section 2.1.1 sur la notation de Singmaster.

Le groupe ne contenant que des combinaisons légales est appelé RC_3, alors que celui contenant toutes les combinaisons possibles est RC_3^*. Uniquement un douzième des combinaisons que nous avons observées est accessible à l'aide de rotations de faces (Chen, 2004). L'explication de ce fait se trouve en fin du chapitre 3.

Chapitre 3

Théorème fondamental de la théorie du Rubik's Cube

Nous avons maintenant les outils pour comprendre le théorème fondamental, qui décrit mathématiquement quand une combinaison est légale ou non. il faut néanmoins définir une notation simple pour différencier une combinaison d'une autre. Cette partie est en grande partie inspirée de celle de Mulholland (2011).

Une combinaison du Rubik's cube est définie par :

1. la permutation de ses 8 coins. Un élément ρ du groupe de symétrie S_8 décrit de manière unique cette permutation.
2. la permutation de ses 12 arêtes. Similairement, un élément σ du groupe S_{12} décrit cette permutation.
3. l'orientation de chacun des 8 coins. Dans ce cas, utilisons un 8-uplet, nommé v (en d'autres termes, une séquence de 8 éléments) contenant des nombres entiers entre 0 et 2 (chaque nombre définit une orientation).
4. l'orientation de chacune des 12 arêtes. De la même manière, utilisons un 12-uplet w contenant un 0 ou un 1 pour décrire l'orientation de chaque arête.

Développons chaque point :

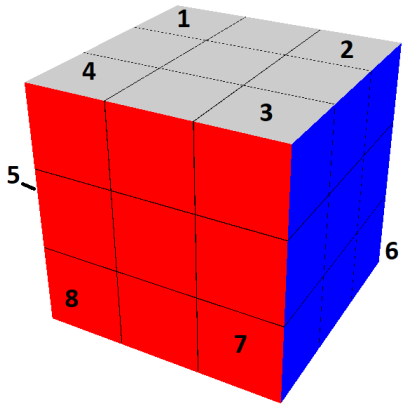
3.1 permutation des coins : ρ

La figure 3.1a décrit le système de numérotation des coins. Elle débute dans le coin supérieur-gauche-arrière puis compte dans le sens des aiguilles d'une montre. Elle continue de la même manière sur la face inférieure.

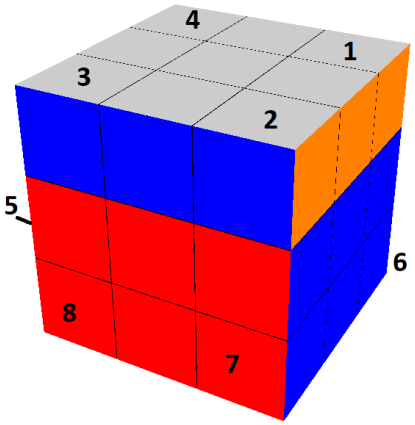
Observons la permutation de ces coins après une rotation d'un quart de tour de la face supérieure dans le sens des aiguilles d'une montre (U en notation de Singmaster), que l'on peut observer sur la figure 3.1b. Avec la décomposition en cycle, nous pouvons écrire $\rho = (1\ 2\ 3\ 4)$. car le coin qui était en 1 est maintenant en 2, celui qui était en 2 est maintenant en 3,...

3.2 permutation des arêtes : σ

La permutation des arêtes est très similaire à la permutation des coins. Observons d'abord le système de numérotation des 12 arêtes sur la figure 3.2. La figure 3.3

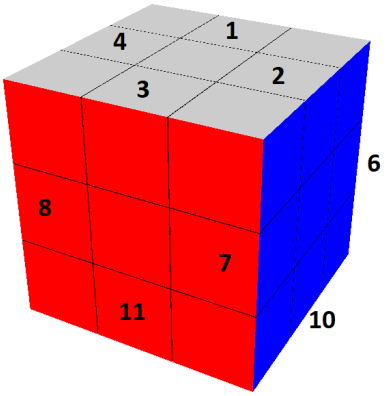


(a) Numérotation des 8 coins. Le numéro 5 est le seul coin non visible avec cette perspective.



(b) Le cube après une rotation U

FIGURE 3.1 – Numérotation des coins du cube



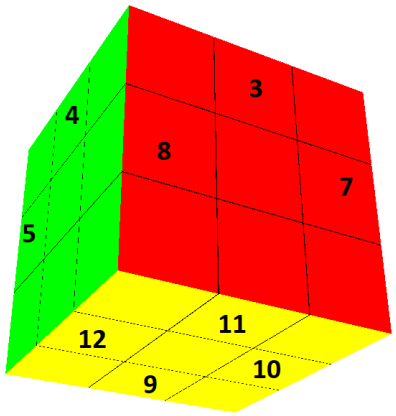


FIGURE 3.2 – Numérotation des arêtes en (a) plongée et (b) contre-plongée.

montre le cas d'une rotation d'un quart de tour de la face avant dans le sens des aiguilles d'une montre (F).

Nous pouvons observer sur la figure 3.3 que la permutation des coins est : $\sigma = (3\ 7\ 11\ 8)$.

3.3 orientation des coins : v

Afin de savoir dans quelle orientation est un coin indépendamment de sa position, un chemin plus complexe est nécessaire. Voici la démarche choisie pour ce travail :

— Dessinons une croix sur une facette de chaque coin. Pour une question de simplicité, les facettes choisies sont toujours les facettes supérieures et inférieures. Le résultat est la figure 3.4a. Ces croix sont fixes, donc elles ne changent pas de position lorsque le cube est permuté.

— Chaque coin a trois facettes : nous allons marquer les facettes de chaque coin

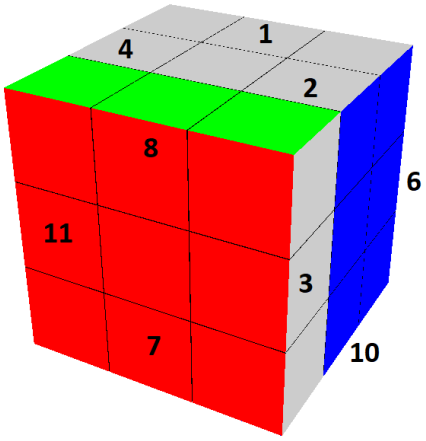
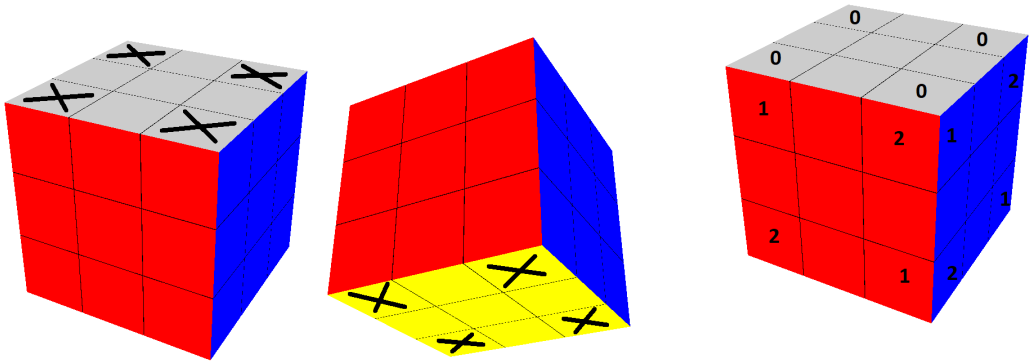


FIGURE 3.3 – Le Rubik's cube après une rotation F



(a) Chaque coin a exactement une facette marquée d'une croix

(b) Les facettes des coins sont toutes marqués des nombres de 0 à 2

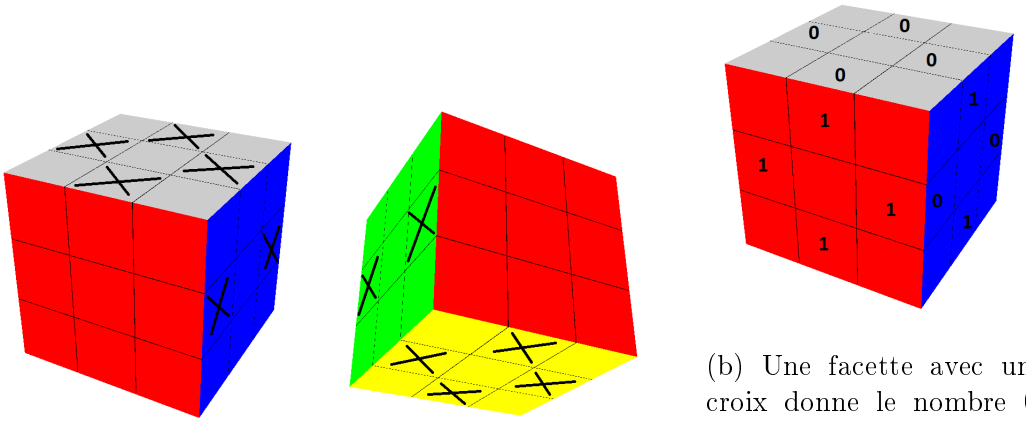
FIGURE 3.4 – Méthode pour décrire la rotation de chaque coin : (a) placer une croix sur une facette de chaque coin et (b) donner un nombre à chaque facette de chaque coin

avec les nombre de 0 à 2 (figure 3.4b). S'il y a une croix sur la facette, c'est un 0, sinon c'est 1 puis 2 dans le sens des aiguilles d'une montre (en plaçant la croix en dessus). Les nombres, contrairement aux croix, ne sont pas fixes. Ils bougent avec les coins afin de toujours rester sur le même coin. [1]

— La préparation est terminée. Pour décrire l'ensemble des orientations des coins, il suffit de regarder quel nombre se trouve sous chaque croix. Avec l'ensemble des 8 croix, nous obtenons un 8-uplet de nombres entre 0 et 2. Lorsque le cube est à son état initial (élément neutre), $v = (0\,;0\,;0\,;0\,;0\,;0\,;0\,;0$ car sous chaque croix se trouve un 0.) [2]

1. Il est nécessaire de placer ces nombres lorsque le cube est dans l'état résolu, car les nombres dépendront ensuite de la pièce d'origine.

2. L'ordre dans lequel les nombres sont inscrit dans le 8-uplet v est le même que celui de la figure 3.1a.



(a) Chaque arête contient exactement une croix

(b) Une facette avec une croix donne le nombre 0, une sans croix donne le nombre 1

FIGURE 3.5 – L'orientation des arêtes est décrite par le nombre (b) qui se trouve sous la croix (a)

3.4 rotation des arêtes : w

Le dernier paramètre de notre cube est l'orientation de chaque arête. Le processus est pratiquement le même que celui utilisé pour l'orientation des arêtes :

— Pour chaque arête, plaçons une croix sur une de ses facette. Encore, le choix est libre mais celui décrit par la figure 3.5a rend le travail plus simple.

— De nouveau, le nombre 0 ou 1 est attribué à chaque facette des arêtes : si une croix se trouve dessous, le nombre 0 lui est attribué, sinon la facette prend le nombre 1. La figure 3.5b résume cela.

Illustrons par un exemple le v et w. La figure 3.6 contient un Rubik's cube après la suite de rotation UR (rotation de la face du haut puis de la face de droite). Seuls les nombres placés sous une croix sont inscrits, car les autres ne nous intéressent pas ici. De plus, les nombres sous des croix où rien n'a bougé ne sont pas non plus importants car nous savons qu'ils sont restés ceux d'origine, que nous connaissons.

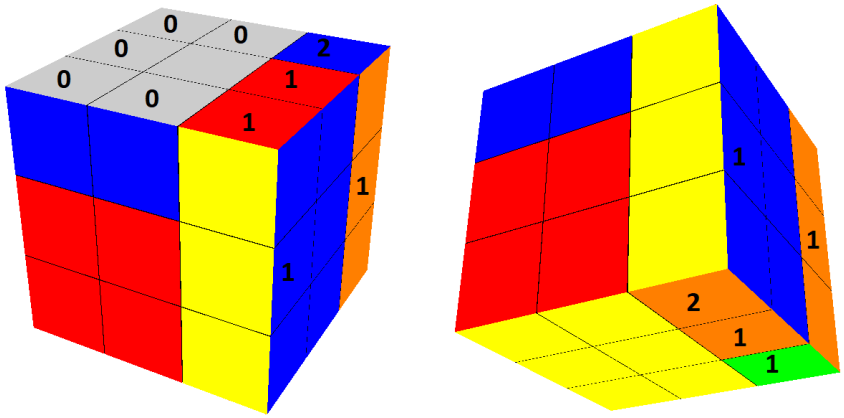


FIGURE 3.6 – Le Rubik's cube après la suite de rotations UR

Ici, $v = (0; 2; 1; 0; 0; 1; 2; 0)$ et $w = (0; 1; 0; 0; 0; 1; 1; 0; 0; 1; 0; 0)$. Le schéma correspond à ce résultat, les nombres non marqués sur le schéma ne sont pas sous une croix ou n'ont pas bougé.

En résumé, un état du Rubik's cube est mathématiquement décrit de la manière suivante : $\lambda \in RC_3^* \Leftrightarrow \lambda = (\rho, \sigma, v, w)$ tel que $\rho \in S_8$, $\sigma \in S_{12}$, $v \in \mathbb{Z}_3^8$ et $w \in \mathbb{Z}_2^{12}$.

Après quelques observations de ces quatre paramètres, certaines règles peuvent être déduites. Pour cela, un ordinateur est plus rapide pour calculer et définir la valeur de ces variables selon l'état actuel du cube. Un programme a été écrit dans le cadre de ce travail afin d'effectuer cette tâche. En annexe se trouve le guide pour l'employer correctement. [3]

Mélangeons le cube avec des mouvements de base et observons les résultats [4], afin d'émettre la conjecture suivante :

Théorème fondamental de la théorie du Rubik's cube
si et seulement si $(\rho, \sigma, v, w) \in RC_3$ (groupe des états légaux du Rubik's cube), alors les propriétés suivantes sont vérifiées :

1. $sign(\rho) = sign(\sigma)$
2. $\sum_{i=1}^{8} v_i = v_1 + \cdots + v_8 \equiv 0 \pmod 3$
3. $\sum_{i=1}^{12} w_i = w_1 + \cdots + w_{12} \equiv 0 \pmod 2$

Ces trois propriétés forment donc le théorème fondamental.

La première propriété affirme que la permutation des coins a le même signe que la permutation des arêtes. Cela signifie que l'on ne peut pas échanger deux arêtes sans bouger les coins, car le signe de la permutation des arêtes serait -1 alors que celui des coins est toujours 1.

La deuxième propriété décrit la rotation des coins : Nous pouvons en déduire que le nombre des coins tournés dans le sens horaire (le nombre 1 apparait sur la croix) moins le nombre de coins dans le sens anti-horaire (le nombre 2 apparait) est un multiple de 3. On le déduit car dans la somme $v_1 + v_2 + v_3 + \cdots + v_8$, ajouter un coin anti-horaire équivaut à ajouter 2, ce qui est équivalent à soustraire 1 en modulo 3. Nous pouvons donc annuler tous les coins horaires et anti-horaires, et le résultat est un multiple de 3.

La dernière propriété explique que les arêtes sont tournées par paires. Il ne peut pas y avoir un nombre impair d'arêtes retournées car la somme de ces dernières (celles qui valent 1) est un nombre pair.

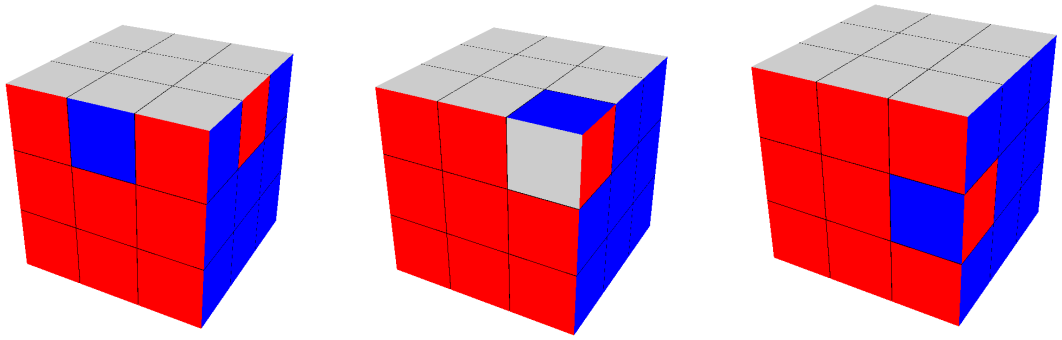
La preuve du théorème se trouve en annexe.

3.5 1 combinaison sur 12 est légale

A l'aide du théorème fondamental, nous pouvons maintenant savoir quand une certaine configuration du cube est légale ou pas : elle doit respecter les trois pro-

3. Le dossier contenant le programme se trouve dans le même dossier que ce document, et un guide d'utilisation se trouve en annexe. Le lecteur est encouragé à l'utiliser pour réitérer l'expérience faite ci-dessous.

4. Une partie de ces résultats est montrée en annexe.



(a) Deux arêtes ont été interverties

(b) Un coin unique est mal orienté

(c) Une seule arête est retournée

FIGURE 3.7 – Variations possibles de RC_3

priétés du théorème fondamental. Nous savons aussi que RC_3 est un groupe, donc un sous-groupe de RC_3^*.

Un élément de RC_3 suit donc les trois propriétés. Regardons les possibilités d'éléments qui ne suivent pas une des propriétés :

— $sign(\rho) \neq sign(\sigma)$: Lorsque deux coins sont intervertis, le signe de la permutation des coins est -1 alors que le signe de la permutation des arêtes est resté 1. Cela fonctionne aussi si ce sont deux arêtes qui sont interverties (figure 3.7a).
— $\sum_{i=1}^{8} v_i = 1 \pmod 3$ ou $\sum_{i=1}^{8} v_i = 2 \pmod 3$: C'est le cas notamment lorsqu'un seul coin est mal orienté. (figure 3.7b)
— $\sum_{i=1}^{12} w_i = 1 \pmod 2$: Un nombre impair d'arêtes est retourné. (figure 3.7c)

En combinant ces variations, 11 autres sous-ensembles de RC_3^* sont possibles (deux choix pour la propriété 1, trois choix pour la 2 et deux choix pour la 3 moins RC_3 : $2*3*2-1 = 11$). Ce sont les classes suivant le sous-groupe RC_3. Le groupe de tous les mouvements possibles peut donc être divisé en 12 parties. Par le théorème de Lagrange, $|RC_3^*| = 12|RC_3|$. Cela veut dire qu'une configuration du Rubik's cube pris au hasard a une chance sur 12 d'être un état légal.

De plus, par les propriétés des classes suivant un sous-groupe, si l'on utilise des mouvements légaux depuis une certaine classe, on reste toujours dans la même classe. Il est donc impossible de passer d'une classe à l'autre avec des simples rotations de face.

3.6 Ordre de RC_3 et RC_3^*

L'ordre d'un produit direct de groupes est le produit des ordres de ces groupes. Or, $RC_3^* = S_{12} \times S_8 \times \mathbb{Z}_3^8 \times \mathbb{Z}_2^{12}$, donc $|RC_3^*| = |S_{12}||S_8||\mathbb{Z}_3^8||\mathbb{Z}_2^{12}|$:

$$|RC_3^*| = 12!8!2^{12}3^8 = 43'252'003'274'489'856'000$$

Ensuite, l'ordre de RC_3 est un douzième de l'ordre de RC_3^* :

$$|RC_3^*| = \frac{|RC_3^*|}{12} = 3'604'333'606'207'488'000$$

Cela représente l'ensemble des combinaisons atteignables à l'aide de mouvements de base en partant d'un Rubik's cube résolu.

Nous avons donc étudié les outils de base de la théorie des groupes, que nous avons ensuite appliqués à un Rubik's cube pour en déduire ces propriétés. Une étude plus approfondie de la théorie des groupes permettrait de révéler d'autres grands secrets du Rubik's cube, mais c'est malheureusement trop complexe pour l'échelle de ce travail.

Conclusion

En conclusion, la structure mathématique d'un Rubik's cube est très élaborée. La théorie des groupes est un excellent outil d'analyse pour ce système, mais ce travail n'a montré qu'une infime partie de cet immense monde abstrait. Le Rubik's cube, un si simple appareil, s'est montré d'une grande complexité et diversité. Cet engin s'applique a une multitude de domaines de la théorie des groupes, il est maintenant clair pourquoi il en est souvent un symbole.

Transformer un système, a première vue bien connu, en un groupe peut s'avérer très instructif et, parfois après quelques recherches et expérimentations, révéler de nouvelles informations. En étudiant ses sous-groupes, les permutations de ce groupe et tant d'autres caractéristiques, nous pouvons découvrir une nouvelle manière d'observer un tel système. Dans notre cas, nous avons réussi à trouver un groupe définissant le Rubik's cube, et, entre autres, nous avons utilisé ce groupe afin de savoir quand un certain état est soluble.

La théorie des groupes semble très bien s'appliquer à la réalité. Grâce à elle, nous pouvons découvrir la vraie nature d'objets qui nous semblent simple au premier abord. Le Rubik's cube est un bon exemple d'application, mais est loin d'être le seul. Quelles sont les autres domaines d'applications possibles ? Il serait difficile de tous les citer. Elle peut s'appliquer à la chimie pour étudier certains systèmes de molécules, à la biologie pour regarder le fonctionnement d'un écosystème ou encore la cryptographie, la musique et bien d'autres. Ce travail a introduit cette théorie qui, bien que très abstraite, permet de repousser nos limites de la connaissance.

Bilan personnel

En tant que passionné de mathématiques, le travail accompli de recherche et de compréhension était très intéressant et j'y ai volontiers mis toute mon énergie. J'ai été surpris durant la recherche de documentation sur le sujet par la diversité dans le monde mathématique : nous pouvons trouver des articles sur tout ce que nous cherchons.

L'étude de la théorie des groupes a été en quelques sortes un obstacle à l'avancement du projet, car le cours choisi était trop élaboré relativement à l'échelle de ce travail. Beaucoup, peut-être trop de temps a été consacré à le suivre. Cela m'a tout de même permis de comprendre à un niveau intuitif toutes les notions utilisées dans ce travail, au coût de plusieurs mois d'études. Néanmoins, l'étude de ce domaine a changé ma vision de certains concepts mathématiques et m'a montré à quel point ces derniers s'appliquent à notre réalité.

Le projet de simulation d'un Rubik's cube avec un outil de résolution automatique et des instruments d'analyse a aussi coûté beaucoup de temps. Cela a nécessité d'approfondir mes notions de $C++$. J'ai ensuite décidé de le réécrire en javascript [5] pour rendre son accès plus simple. Cela n'a pris que quelques jours car le javascript est suffisamment proche de $C++$.

Finalement, je suis très heureux du résultat et du processus pour y arriver. J'ai acquis une grande quantité de connaissances qui me serviront beaucoup dans le futur.

5. Le $C++$ et le javascript sont des langages de programmation.

Bibliographie

Chen, J., 2004, Group Theory and the Rubik's Cube, Notes de cours

Frey, A. H. et Singmaster, D., 1982, Handbook of cubik math, Enslow publishers

Heise, R., 2007a, The Heise method, https://www.ryanheise.com/cube/heise_method.html, visité le 30.08.2020

Heise, R., 2007b, Rubik's cube : fundamental techniques, commutators, https://www.ryanheise.com/cube/commutators.html, visité le 27.07.2020

Mulholland, J., 2011, Permutation Puzzles : A Mathematical Perspective

Pauli, S., 2019, Cardinality of Cartesian Products, https://mathstats.uncg.edu/sites/pauli/112/HTML/section-41.html, visité le 25.05.2020

Table des figures

Annexe A

Mode d'emploi pour le programme de simulation du Rubik's cube

Voici un mode d'emploi qui explique brièvement toutes les fonctionnalités du programme :

— Dans le dossier contenant l'application, ouvrez le fichier *cube.html* avec un navigateur tel *Mozilla Firefox*, *Google Chrome* ou *Microsoft Edge*.[1] Il est nécessaire de garder tous les fichiers et dossiers étant dans le même dossier pour le bon fonctionnement du programme.

— Les flèches du clavier permettent de tourner la caméra autour du cube.

— La notation de Singmaster est directement adaptée au clavier, il suffit d'entrer une des lettres ci-dessous pour effectuer cette rotation :

rotations de base :
'U' : rotation de la face du haut ("up")
'R' : rotation de la face de droite ("right")
'F' : rotation de la face avant ("front")
'D' : rotation de la face du bas ("down")
'L' : rotation de la face de gauche ("left")
'B' : rotation de la face de derrière ("back")

rotations de couches centrales :
'M' : rotation de la couche centrale dans le sens de 'L' ("middle")
'E' : rotation de la couche centrale dans le sens de 'D' ("equator")
'S' : rotation de la couche centrale dans le sens de 'F' ("standing")

rotation du cube entier :
'X' : rotation du cube dans le sens de 'R'
'Y' : rotation du cube dans le sens de 'U'
'Z' : rotation du cube dans le sens de 'F'

Rappelons aussi que les touches majuscules signifient un quart de tour dans le

1. Pour des raisons inconnues, le programme ne fonctionne pas avec *Internet Explorer*

sens des aiguilles d'une montre lorsqu'on a la face devant nous. Pour effectuer un tour dans le sens inverse, il faut utiliser la touche minuscule.
Notons que la rotation de la caméra avec les flèches ne change pas la position avant du cube.

— L'option "Rotation automatique" fait tourner en permanence la caméra à une vitesse lente.

— L'option "Mélanger" effectue une suite d'environ 30 mouvements aléatoires.

— L'option "Résoudre" transforme le cube jusqu'à une position résolue. L'algorithme utilisé est la méthode de résolution avancée CFOP, inventé par Jessica Fridrich. [2] D'abord, une croix est formée sur une des six faces. Les coins de la face choisie sont ensuite résolus en même temps que la tranche centrale parallèle à la face d'origine. Ensuite, les pièces de la dernière face sont tournées dans le bon sens et finalement permutées à leur place d'origine.
Un humain est capable d'appliquer cette méthode en apprenant tous ces algorithmes par coeur, mais il est parfois difficile de comprendre la construction interne des algorithmes. En se basant sur la théorie des groupes, Ryan Heise a développé une méthode purement intuitive, avec laquelle nous créons durant la résolution les algorithmes nécessaires (Heise, 2007a).

— L'option "Vitesse" change la vitesse de rotation des mouvements.

— L'option "Afficher l'état actuel" montre ou cache la valeur des paramètres définissant le cube : (ρ, σ, v, w).

2. CFOP signifie Cross F2L OLL PLL

Annexe B

Résultats de l'expérimentation

Afin d'émettre une conjecture sur les quatre éléments (ρ, σ, v, w) qui donne une description mathématique du Rubik's cube, nous avons mélangé à maintes reprises un cube virtuel et observé comment varient nos paramètres. Voici un échantillon représentatif de ces résultats :

itération	ρ	$sign(\rho)$	σ	$sign(\sigma)$
1	(1 2 6) (3 4 7 5)	-1	(3 7 12 5 4 6 9 8 10 11)	-1
2	(1 6 7 5 8 4 2 3)	-1	(1 2 11 12 10) (3 4 7 5 9 6)	-1
3	(1 4 8 2 3 6 5)	1	(1 10 9 7 6 4 11) (2 12 5 8 3)	1
4	(1 3 6 4 7 2 5 8)	-1	(1 3) (2 9 11 5 7 10 6 12) (4 8)	-1
5	(1 5 8 7 2 6)	-1	(1 6 7 3) (2 12) (4 8 10 11 9 5)	-1
6	(1 4 3 6 7) (2 5)	-1	(1 8 5 2 6 12 9 3 7 4)	-1
7	(1 2 5 3 4 7 8)	1	(1 4 8 5 10 6 2 12 7 9) (3 11)	1
8	(1 6 4 7 8 2 3 5)	-1	(1 12) (2 8 11 3 10 9 4 6 5)	-1
9	(1 4) (2 7 3 8)	1	(1 7 11 4 8 2 12 6 10 5 9)	1
10	(1 5) (2 7 3 8) (4 6)	-1	(1 11 5) (2 4 7 10 6 9 8) (3 12)	-1
11	(1 7 6 2 3 8 5)	1	(1 11 12 3 6 5 8 7 9) (2 10 4)	1
12	(1 7 6 5 8 2) (3 4)	1	(1 11 5 7 9 12 8 10 3 2 6)	1

itération	v	$\sum v_i$	w	$\sum w_i$
1	(0,0,1,0,1,1,1,1,1,1,0,1)	8	(2,1,0,0,0,2,0,1)	6
2	(0,1,1,1,0,0,0,0,1,0,0,0)	4	(1,1,1,0,0,1,0,2)	6
3	(0,0,1,0,1,1,0,1,1,0,1,0)	6	(1,2,2,2,1,1,2,1)	12
4	(1,0,1,1,1,1,0,0,1,0,1,1)	8	(1,2,2,1,0,1,2,0)	9
5	(1,1,1,0,1,1,1,0,1,0,1,0)	8	(1,2,0,0,0,1,0,2)	6
6	(1,0,0,0,0,1,0,0,0,1,1,0)	4	(0,2,2,0,0,0,1,1)	6
7	(0,0,0,0,1,0,1,0,1,1,1,1)	6	(0,0,1,1,1,0,0,0)	3
8	(0,0,0,1,0,0,0,0,1,0,0,0)	2	(1,0,1,0,0,0,2,2)	6
9	(0,1,1,1,1,0,1,0,0,1,1,1)	8	(2,0,1,1,1,0,2,2)	9
10	(1,0,0,0,0,1,0,1,0,0,1,0)	4	(0,1,0,2,1,0,2,0)	6
11	(1,1,0,1,1,0,0,1,0,1,0,0)	6	(2,2,2,2,0,0,1,0)	9
12	(0,1,1,1,0,0,0,1,1,1,1,1)	8	(2,2,2,0,0,0,2,1)	9

Annexe C

Démonstration du théorème fondamental

Prouvons que $(\rho, \sigma, v, w) \in RC_3$ est équivalent à :

$$\begin{cases} sign(\rho) = sign(\sigma) \\ \sum_{i=1}^{8} v_i = v_1 + \cdots + v_8 \equiv 0 \bmod 3 \\ \sum_{i=1}^{12} w_i = w_1 + \cdots + w_{12} \equiv 0 \bmod 2 \end{cases}$$

La démonstration se déroule en deux étapes :

1. L'implication : pour chaque état légal du Rubik's cube, les quatre paramètres correspondants ρ, σ, v et w respectent les trois lois du théorème.
2. La réciproque : si ρ, σ, v et w respectent les trois lois, alors le Rubik's cube est dans un état légal.

Partie 1

Prenons un état du Rubik's cube pour lequel les trois conditions sont respectées : l'élément neutre. En effet, Pour cette configuration, nous trouvons que le Rubik's cube est décrit par $(e_\rho, e_\sigma, (0, 0, \ldots, 0), (0, 0, 0, \ldots, 0))$. Le signe de la permutation de l'élément neutre est toujours 1, la somme des éléments de v est 0 et la somme des éléments de w est 0, donc les trois conditions sont respectées.

Montrons maintenant que les mouvements U, R, L, F, D et B vérifient eux aussi les conditions.

Pour R (rotation de la face de droite), nous trouvons que la permutation des coins $\rho = (2\ 6\ 7\ 3)$, la permutation des arêtes $\sigma = (2\ 6\ 10\ 7)$, la rotation des coins $v = (0, 2, 1, 0, 0, 1, 2, 0)$ et la rotation des arêtes $w = (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$. Les conditions sont donc vérifiées : $sign(\rho) = sign(\sigma) = -1$, $\sum_{i=1}^{8} v_i = 0 \pmod 3$ et $\sum_{i=1}^{12} w_i = 0 \pmod 2$.
Les résultats sont similaires pour les 5 autres mouvements. Nous pouvons observer que les permutations de chacun de ces mouvements sont des 4-cycles.

Finalement, il suffit de prouver que si un de ces 6 mouvements est appliqué à un état légal quelconque X, le résultat est aussi légal. Cela est suffisant car l'identité

est un état légal et nous pouvons accéder à toutes les autres combinaisons par ces 6 mouvements. [1]

Procédons pour chaque condition :

1. $sign(\rho) = sign(\sigma)$: Puisque X est un état légal, le signe de ρ est égal au signe de σ. Or, les permutations de chacun des 6 mouvements de base sont un 4-cycle pour les coins et les arêtes. Le signe reste donc le même après un tel mouvement, car dans le calcul du signe, on ajoute le même nombre pour les deux permutations (le nombre 3, en l'occurrence).
2. $\sum_{i=1}^{8} v_i = 0 \pmod 3$: Pour le cas de U (rotation de la face supérieure), les rotations ne changent pas car les croix recouvrent la face supérieure de tous les coins sur U, ils sont donc toujours comptés après la rotation. Pour D (rotation de la face inférieure), le même principe s'applique car les croix sont disposées symétriquement. La preuve se complique pour les 4 autres mouvements.

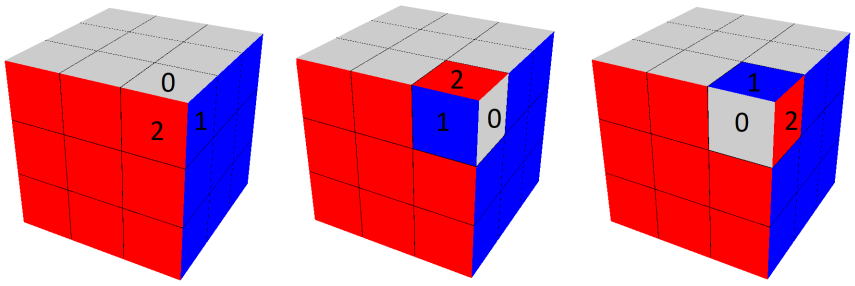


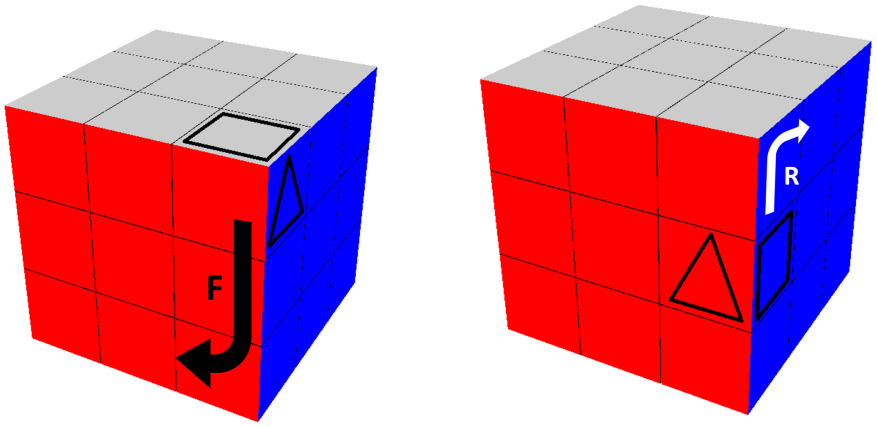
FIGURE C.1 – Les trois états possibles d'un coin.

Prouvons le cas de F : Observons sur la figure C.1 que les coins ne peuvent être que dans trois états particuliers. Ensuite, la figure C.2a illustre que la facette actuellement comptée dans v est celle marquée d'un carré. Après une rotation F, la facette comptée sera celle marquée d'un triangle. Or, pour chacun des cas, $n_{tri} = n_{car} + 1 \pmod 3$. [2]

La situation est similaire pour le coin à l'opposé (en bas à gauche). Dans le cas des deux autres coins, c'est le contraire : après la rotation F, une facette avec une facette de valeur inférieure de 1 sera sous une croix. En résultat, la somme des changements est 0 (mod 3). Nous utilisons la même démonstration pour les mouvements B, R et L. Cette condition reste donc vérifiée.

3. $\sum_{i=1}^{12} w_i = 0 \pmod 2$: La preuve de cette partie ressemble à la précédente. Dans le cas des mouvements F et B (face avant et arrière), rien ne change car les mêmes facettes restent sous les croix.
Prenons maintenant le cas de R (rotation de la face de droite). Comme avant, nous remarquons que la face n'a que deux états possibles.

1. Nous n'avons pas besoin des inverses de U, R, L, F, D et B, car nous pouvons les obtenirs en effectuant trois fois un quart de tour d'un mouvement pour obtenir son inverse.
2. Naturellement, n_{tri} est le nombre qui apparaît sous le triangle et n_{car} celui sous le carré.



(a) La facette marquée d'un triangle sera comptée dans la somme des orientations des coins après une rotation F.

(b) La face marquée d'un carré est maintenant sous une croix. Après un mouvement R, ce sera la facette marquée d'un triangle.

FIGURE C.2 – Après une rotation, une autre facette de la pièce est comptée dans le total

> Prenons la pièce marquée de la figure C.2b. Dans l'état actuel, la facette marquée d'un carré se trouve sous une croix et est donc comptée dans le total. Après une rotation R, la facette marquée d'un triangle sera comptée dans le total. A chaque quart de tour, la facette comptée alterne. Si la somme des parties de w est un multiple de 2 avant F, alors elle le sera aussi après car 4 des nombres passent de 0 à 1 ou de 1 à 0. [3]

Nous avons donc prouvé que toutes les configuration légales respectent les trois conditions.

Partie 2

Pour cette partie de la démonstration, nous partons d'un état respectant les trois conditions, puis nous résolvons le cube avec les mouvements de base. Les algorithmes de résolution utilisés ici ne faisant pas l'objet de ce travail. Frey et Singmaster (1982) ainsi que Heise (2007b) fournissent des explications sur les techniques utilisées. Nous cherchons donc à retrouver les valeurs de l'élément neutre : $(e_\rho, e_\sigma, (0, 0, \ldots, 0), (0, 0, 0, \ldots, 0))$.

Assurons nous tout d'abord que le signe de la permutation des coins et des arêtes est 1. S'il ne l'est pas, il suffit de faire un quart de tour d'une face pour l'inverser. Il est possible de faire changer de place n'importe quel triplet de coins ou d'arêtes du cube sans bouger les autres pièces, à l'aide de commutateurs et de conjugués. Comme la première condition est vérifiée, il est possible de ramener chaque arête et chaque coin à son emplacement d'origine. Il est donc possible de transformer le cube en un autre cube ou les permutations sont l'élément neutre, tout en gardant les autres conditions vérifiées car on utilise uniquement des rotations de face.

3. En termes algébriques, si n des 4 coins passent de 0 à 1, alors $4 - n$ passent de 1 à 0 et la différence totale est $n + (-1)(4 - n) = 2n - 4 = 2(n - 2)$, qui est un multiple de 2.

Ensuite, bien que toutes les pièces soient au bon endroit, elles n'ont pas forcément la bonne orientation. Il est possible de retourner n'importe quel couple d'arête. Or, la troisième condition est encore vérifiée (Un nombre pair d'arêtes est retourné), donc il est possible de tourner toutes les arêtes.

Il ne manque que la bonne orientation des coins. Nous pouvons, pour n'importe quelle paire de coins, en tourner un dans le sens horaire et l'autre dans le sens anti-horaire. Après avoir tourné toutes les paires de coins horaires et anti-horaires, il reste un multiple de 3 de coins horaires ou de coins anti-horaires. Nous pouvons appliquer deux fois le dernier algorithme pour orienter correctement ces triplets de coins.

L'état actuel du cube étant l'élément neutre, la démonstration est terminée.