UNIVERSITÉ DE TOULON

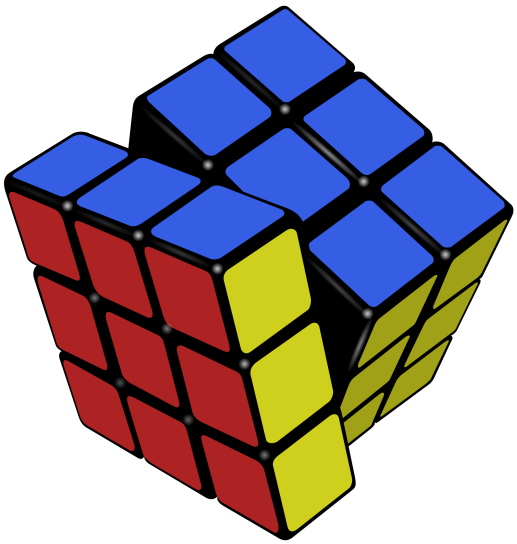
DÉPASSONS L'HORIZON

Mémoire de Licence 3 de Mathématiques

Par Anastasiia CHERNETCOVA

Sous la direction d'Yves AUBRY

Rubik's cube et la théorie des groupes



UFR Sciences & Techniques
Université de Toulon
Année 2021-2022

Table des matières

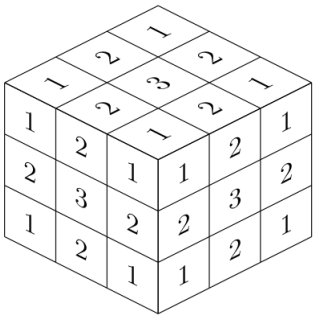
Introduction

Le Rubik's cube apparaît pour la première fois en 1974. Il a été conçu par Erno Rubik, un architecte et un professeur de design hongrois. Le Rubik's cube possède de remarquables propriétés de théorie de groupe. Dans ce mémoire, on cherchera à comprendre la structure du groupe du Rubik's cube.

Le présent mémoire est organisé de la façon suivante : les chapitres 1 et 2 seront consacrés à la construction du groupe du Rubik's cube, le chapitre 3 présentera un résultat fondamental concernant les mouvements autorisés dans le jeu, et la démonstration de ce résultat s'étendra aussi sur le chapitre 4. Dans le chapitre 5, on introduira quelques sous-groupes intéressants du groupe de Rubik et finalement, dans le chapitre 6, on se penchera sur une notion très importante dans la construction du groupe de Rubik : le produit semi-direct.

Mise en situation

Le Rubik's cube se compose de $3 \times 3 \times 3$ petits cubes. Parmi eux, 7 sont fixes (le cube central, qui n'est pas visible et ceux notés par le chiffre 3) et 20 sont mobiles, à savoir les huit coins (notés 1) et les douze arêtes (notés 2). Chacune des 6 faces se décompose en 9 facettes et la facette centrale est immuable. Dans le Rubik's cube original, les couleurs des faces sont : le bleu en face du vert, le rouge en face de l'orange, le blanc en face du jaune. Dans ce mémoire, lorsque l'on évoquera les couleurs, on supposera que l'on a en mains le modèle original.



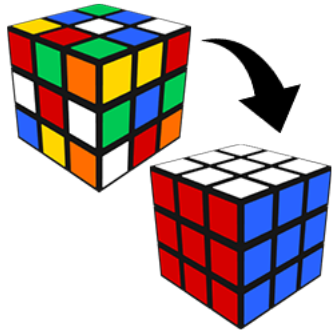
Les coins du cube, notés par le chiffre 1 et les arêtes du cube, notés par le chiffre 2

Le but du jeu est de faire tourner les faces pour le ramener à son état d'origine où chacune des faces est d'une couleur homogène. C'est ce que l'on appelle *résoudre le Rubik's cube*.

Notations et vocabulaire

On appelera *tranche du Rubik's cube* la partie tournante composée de 9 pièces.

On représente chaque face du cube par une lettre. Lorsque l'on regarde directement la face devant nous, on la note F (forward). On appelle alors U (upper) la face d'en haut, L (left) la face de devant, R (right) la face de droite, B (backward) la face arrière, D (downward) la face d'en bas (cf [Sin81], p. 4). Par exemple, si l'on regarde la face blanche directement, F est la face blanche, U est la bleue, L est la orange, R est la rouge, D est la verte et B est la jaune.



Passage d'un état quelconque à l'état résolu

Par abus de notations, on appelera aussi $R \in \{F, U, L, R, B, D\}$ la rotation d'un quart de tour dans le sens des aiguilles d'une montre de la tranche correspondante autour de l'axe $\overrightarrow{OP}$, où O est le centre du Rubik's cube et P est le centre de la face R. On notera R^{-1} la rotation d'une tranche R dans le sens contraire des aiguilles d'une montre autour de l'axe $\overrightarrow{OP}$. On appelera *mouvement élémentaire* la rotation (dans n'importe quel sens) d'une tranche et *mouvement légal* le mouvement composé de mouvements élémentaires.

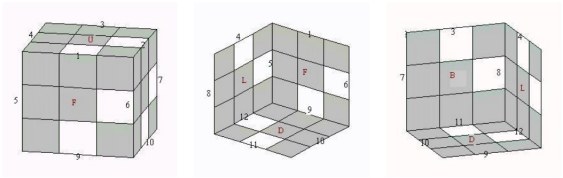
Lorsqu'on a une manoeuvre du Rubik's cube, on lit les instructions de gauche à droite. Par exemple, si on a la manoeuvre UF^{-1}, alors d'abord on applique la rotation U et ensuite F^{-1}.

Chapitre 1

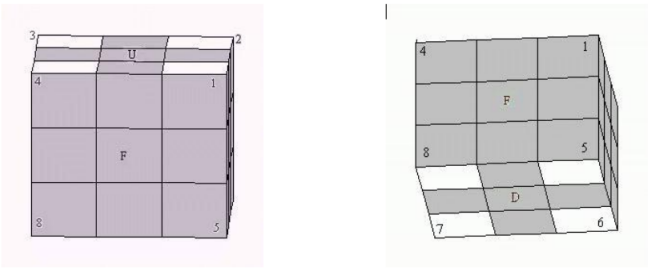
Le groupe du Rubik's cube

Notations

Une fois que l'on a noté les faces, on numérotera les arêtes comme indiqué dans la figure 1.1 et les coins comme indiqué dans la figure 1.2 :



Numérotation d'arêtes



Numérotation de coins

1.1 Le groupe G et son sous-groupe Rub

Le groupe du Rubik's cube $(Rub, \circ)$ est un groupe qui représente la structure du puzzle du Rubik's cube. Chaque élément de Rub correspond à la transformation du Rubik's cube obtenue par rotations successives des 6 faces du Rubik's cube, de ce fait, $Rub = \langle U, F, L, R, B, D \rangle$. Rub est appelé le groupe du Rubik's cube *légal*, ie contenant des transformations induites par rotation des tranches. On note G le groupe du Rubik's cube élargi. Il contient aussi les transformations que l'on peut obtenir en démontant le Rubik's cube.

Un élément de G se décompose naturellement en son action sur les coins et son action sur les arêtes. De plus, ces deux actions sont indépendantes : chaque transformation du Rubik's cube enverra un coin sur l'emplacement d'un autre coin et une arête sur l'emplacement d'une autre arête (cf [Col10], p. 2,

"Dévissage du groupe du Rubik's cube"). On distinguera les coins physiques de leurs emplacements que l'on appelera "sites coin" ou "site arête".

On introduit G_C le sous-groupe d'actions sur les coins et G_A, le sous-groupe d'action sur les arêtes. G est isomorphe au produit direct de G_C et de G_A ([Col10], p. 2, "Dévissage du groupe du Rubik's cube").

1.2 Dénombrement des éléments du groupe de Rubik

On peut calculer le nombre total de transformations (cf [Rio], p. 4, "Dénombrement des configurations au tournevis"). Calculons d'abord le nombre de transformations que l'on peut effectuer sur les coins. On positionne les 8 coins sur les 8 sites coins (sans se soucier de leurs orientations).

— Pour le premier coin, on peut choisir 8 emplacements possibles ;
— Pour le second coin, il reste 7 emplacements possibles ;
— ...
— Pour le dernier coin, il ne reste qu'un seul emplacement possible.

Ainsi il y a $8 \times 7 \times \cdots \times 1 = 8!$ façons de placer les 8 coins sur leur sites. Maintenant on s'occupe de leur orientation. Chaque coin peut être orienté de trois manières différentes, et c'est le cas pour les 8 coins. Donc il y a 3^8 combinaisons possibles.

On peut raisonner de la même façon sur les 12 arêtes qui ont pour chacune 2 orientations possibles. Ainsi il y a 12! façons de placer les arêtes et 2^{12} orientations.

Comme G est isomorphe au produit direct de G_C et de G_A, $| G | = 12! \times 2^{12} \times 8! \times 3^8 \approx 5 \times 10^{20}$. De plus, on a le théorème suivant, que l'on cherchera à démontrer par la suite :

Théorème 1. *Le sous-groupe Rub est d'indice 12 dans G (cf [Col10], p. 2, "Le groupe de Rubik").*

Corollaire. *On a donc* $| Rub | = \frac{1}{12} \times 12! \times 2^{12} \times 8! \times 3^8 \approx 43 \times 10^{18}$.

Il y a environ 43 milliards de milliards d'états que l'on peut atteindre par rotation des tranches.

Chapitre 2

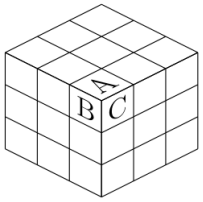
Construction du groupe de Rubik's cube

Dans cette section, nous montrerons que G_C est isomorphe au produit semi-direct interne de $(\mathbb{Z}/3\mathbb{Z})^8$ par $\mathfrak{S}_8$ et G_A au produit semi-direct interne de $(\mathbb{Z}/2\mathbb{Z})^{12}$ par $\mathfrak{S}_{12}$.

Tout élément de G peut s'écrire sous la forme $g = (\pi_C(g), \pi_A(g))$ où $\pi_C : G \to G_C$ et $\pi_A : G \to G_A$ sont deux morphismes de groupe qui laissent fixes A et C, car si l'on agit sur les coins (respectivement les arêtes), on laisse en place les arêtes (respectivement les coins) (cf [Col10], p. 2).

2.1 Mélange des coins

2.1.1 Placement des coins



Les 3 facettes d'un coin

Chaque coin est composé de 3 facettes, comme indiqué dans la figure 2.1. Il y a 8 coins au total et chaque facette peut se trouver sur l'une des trois tranches du cube adjacentes ([Dan14], p. 13, "Corner cubes").

Si l'on regarde les positions des coins sans se soucier de leur orientation, comme il existera toujours une transformation qui enverra un coin sur le site d'un autre coin, on a un morphisme $g \mapsto \sigma_C(g)$ de G_C dans le groupe symétrique $\mathfrak{S}_C$ de l'ensemble C des coins ([Col10], p. 2, "Le groupe des mélanges de coins").

Remarque. *Comme les coins sont au nombre de 8,* $\mathfrak{S}_C \simeq \mathfrak{S}_8$.

Ce morphisme est surjectif et a pour noyau Rot_C le groupe des rotations des coins.

2.1.2 Orientation des coins

Penchons-nous davantage sur ce groupe Rot_C.

Soit $\rho_C : G_C \to \mathbb{Z}/3\mathbb{Z}^8$ l'application qui à g associe le pivotement des coins. L'image d'un $g \in G_C$ sera de la forme $\rho_C(g) = (n_1, \ldots, n_8)$. Plus précisement, supposons que g envoie un coin numéro j sur un coin numéro k. Alors g induira à ce coin l'orientation de n_j tiers de tour ([Joy97], p. 187, "Corner orientations"). Etant donné qu'on peut orienter chaque coin de 0, 1, 2 tiers de tour dans le sens direct

de l'axe partant du centre du cube O et allant vers la pointe du coin S, les facettes des coins sont bien dans le groupe cyclique d'ordre 3 isomorphe à $\mathbb{Z}/3\mathbb{Z}$, car 3 est un nombre premier.

Remarque. *Les orientations des coins induites par les rotations $F, D, F \circ U$ sont indiquées dans la figure 2.1 ([Joy97], p. 187, Example 198) :*

F	$(2,0,0,1,1,0,0,2)$
D	$(0,0,0,0,0,0,0,0)$
$F \circ U$	$(2,0,0,1,1,0,0,2)$

Les orientations des coins induites par les mouvements élémentaires

Par conséquent, tout élément g de G_C peut s'écrire $g = \rho_C(g)\sigma_C(g)$, avec $\rho_C : G_C \to Rot_C$ et $\sigma_C : G_C \to \mathfrak{S}_C$ et cette écriture est unique du fait que $Rot_C \cap \mathfrak{S}_8 = \{id\}$, car la seule permutation des coins qui ne change pas leur orientation et la seule rotation des coins qui ne change pas leurs positions est l'identité. Cela veut dire qu'un mélange de coins se décompose en une permutation des positions des coins suivie d'une rotation de coins.

Remarque. *De ce fait, si h et g sont deux éléments de G, alors*

$$hg = \rho_C(h)\sigma_C(h)\rho_C(g)\sigma_C(g) = \underbrace{\rho_C(h)\sigma_C(h)\rho_C(g)\sigma_C(h)^{-1}}_{\rho_C(hg)}\underbrace{\sigma_C(h)\sigma_C(g)}_{\sigma_C(hg)}.$$

En général, $\rho_C(hg) \neq \rho_C(h)\rho_C(g)$. La relation $\rho_C(hg) = \rho_C(h)\sigma_C(h)\rho_C(g)\sigma_C(h)^{-1}$ est caractéristique d'un produit semi-direct interne de Rot_C par $\mathfrak{S}_C$, comme on le verra dans le chapitre 6.

Le groupe G_C est le produit semi-direct interne de Rot_C par $\mathfrak{S}_C$. Comme Rot_C est isomorphe à $\mathbb{Z}/3\mathbb{Z}^8$, on a donc

$$G_C \simeq \mathbb{Z}/3\mathbb{Z}^8 \rtimes \mathfrak{S}_8.$$

Notons $g = \rho_C(g)\sigma_C(g)$, avec $\rho_C(g) = (n_x)_{x\in C} \in (\mathbb{Z}/3\mathbb{Z})^C$ (à chaque coin on associe sa rotation de n_x tiers de tour). On définit la rotation totale $rt_C(g) := \sum_{x\in C} n_x \in \mathbb{Z}/3\mathbb{Z}$.

Lemme. *L'application $rt_C : (G_C, \circ) \to (\mathbb{Z}/3\mathbb{Z}, +)$ est un morphisme de groupes.*

Pour montrer ce lemme, on aura besoin du résultat suivant :

Remarque. *([Joy97], p. 187, Lemma 199) Pour tout $g, h \in G_C$ tels que $\rho_C(g) = (n_x)_{x\in C}$ et $\rho_C(h) = (n'_x)_{x\in C}$, si l'on note $\rho_C(gh) = (n''_x)_{x\in C}$ on a, pour tout $x \in C$:*

$$n''_x = n_x + n'_{\sigma^{-1}(g)(x)}.$$

Démonstration de la remarque. Le mouvement gh agit d'abord par g et puis par h.

Le mouvement g envoie le coin numéro k sur le $(\sigma(g)_C(k))^e$ site coin et le pivote de n_k tiers de tour. Appelons l'état du cube induit par la transformation g *l'état modifié*. Dans ce cas, le coin numéro k du cube modifié (qui était le coin k avant la transformation g) est le coin qui se trouvait au départ dans la position $\sigma_C(g)^{-1}(k)$.

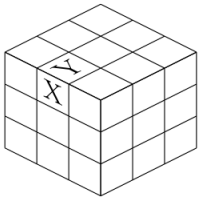
De ce fait, le mouvement h orientera le coin k de $n_{\sigma_C(g)(k)^{-1}}$ tiers de tour, d'où

$$\forall k \in C, n''_k = n_k + n'_{\sigma_C(g)(k)^{-1}}.$$

□

Démonstration du lemme. Soient $g, h \in G_C$, où $g = \rho_C(g)\sigma_C(g)$ et $h = \rho_C(h)\sigma_C(h)$. Notons $gh = \rho_C(gh)\sigma_C(gh)$.

Par la remarque 2.1.2, on a



Les 2 facettes d'une arête

$$gh = \rho_C(g)\sigma_C(g)\rho_C(h)\sigma_C(h) = \underbrace{\rho_C(g)\sigma_C(g)\rho_C(h)\sigma_C(g)^{-1}}_{\rho_C(gh)}\underbrace{\sigma_C(g)\sigma_C(h)}_{\sigma_C(gh)},$$

où $\sigma_C(g)\rho_C(h)\sigma_C(g)^{-1}$ est bien une rotation, étant le conjugué par $\sigma_C(g)$ d'une rotation.

De plus, $\rho_C(gh) = (n''_x)_{x\in C} = n_x + n'_{\sigma_C(g)(x)^{-1}}$ par la remarque 2.1.2.

Donc $rt_C(gh) = \sum_{x\in C}(n_x + n'_{\sigma_C(g)(x)^{-1}})$. Remarquons qu'on a $\sum_{x\in C} n'_{\sigma_C(x)^{-1}} = \sum_{x\in C} n'_x$ (car la somme est commutative et $x \to \sigma_C(x)^{-1}$ est bijective).

Donc $rt_C(gh) = \sum_{x\in c}(n_x + n'_x)$.

Ainsi $rt_X(gg') = \sum_{x\in C} n_x + \sum_{x\in C} n'_x = rt_C(g) + rt_C(g')$, ce qui achève la démonstration.

□

2.2 Mélange des arêtes

On peut faire la même discussion avec les arêtes.

2.2.1 Placement des arêtes

Si l'on regarde les positions des arêtes sans se soucier de leur orientation, on dispose d'un morphisme surjectif

$$\sigma_A : \begin{array}{ccc} G_A & \longrightarrow & \mathfrak{S}_A \\ g & \longmapsto \sigma_A(g), & \end{array} \tag{2.1}$$

où $\mathfrak{S}_A$ le groupe des permutations $\mathfrak{S}_A$ de l'ensemble A des arêtes. Ce morphisme admet pour noyau Rot_A l'ensemble des rotations des arêtes.

2.2.2 Pivotement des arêtes

Par conséquent, soit $\rho_A : G_A \to \mathbb{Z}/2\mathbb{Z}^{12}$ l'application qui à toute transformation g dans G_A associe le pivotement des arêtes. L'image de g par ρ_A sera de la forme $(m_1, \ldots, m_{12})$, où m_j est l'orientation induite à l'arête numéro j par g. Etant donné qu'on peut orienter chaque facette de 0 ou de 1 demies de tour, les facettes des arêtes sont dans un groupe cyclique d'ordre 2, donc isomorphe à $\mathbb{Z}/2\mathbb{Z}$, car 2 est premier.

F	$(1,0,0,0,0,0,0,0,1,0,0,0)$
D	$(0,0,0,0,0,0,0,0,0,0,1,0,1)$
$F \circ U$	$(1,0,1,0,1,0,0,0,1,0,0,0)$

Les pivotements d'arêtes induites par les mouvements élémentaires ([Joy97], p. 188, Example 200)

On écrit $g \in G_A$ de manière unique $g = \rho_A\sigma_A$, où $\rho \in Rot_A$ et $\sigma \in \mathfrak{S}_A$. L'application ρ s'écrit également $\rho = (m_y)_{y\in A} \in (\mathbb{Z}/2\mathbb{Z})^{12}$. On définit la rotation totale $rt_A(g) := \sum_{y\in A} m_y \in \mathbb{Z}/2\mathbb{Z}$.

L'application $rt_A : G_A \to \mathbb{Z}/2\mathbb{Z}$ est un morphisme de groupes comme précédemment. Par ailleurs, G est isomorphe au produit semi-direct de Rot_A par $\mathfrak{S}_A$, ce qui sous-entend que

$$G_A \simeq \mathbb{Z}/2\mathbb{Z}^{12} \rtimes \mathfrak{S}_{12}.$$

Chapitre 3

Théorème fondamental du Rubik's cube

Chaque $g \in G$ se décompose en un produit $\rho_C(g)\sigma_C(g)\rho_A(g)\sigma_A(g)$ où $\rho_C(g) \in Rot_C, \rho_A(g) \in Rot_A, \sigma_C(g) \in \mathfrak{S}_C, \sigma_A(g) \in \mathfrak{S}_A$.

Définissons l'application $E : G \to \{\pm 1\}$ qui à un g décomposé en produit $\rho_C(g)\sigma_C(g)\rho_A(g)\sigma_A(g)$ associe $\varepsilon(\sigma_A(g))\varepsilon(\sigma_C(g))$, où $\varepsilon : \mathfrak{S}_n \to \{\pm 1\}$ est la signature d'une permutation du groupe symétrique à n éléments. L'application E est bien évidemment un morphisme de groupes.

Si l'on combine les morphismes de groupes définis ci-dessus, on obtient le morphisme suivant :

$$rt : G \to \{\pm 1\} \times (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}), \text{ où } rt(g) = (E(g), rt_C \circ \pi_C(g), rt_A \circ \pi_A(g)).$$

Le morphisme rt est surjectif, car tout pivotement et toute permutation des pièces mobiles est réalisable, même de manière illégale. Le noyau de rt, $\mathrm{Ker}(rt)$, est d'indice 12 dans G. Alors

Théorème 2 (Théorème fondamental du Rubik's cube)**.** *$Rub = Ker(rt)$, autrement dit $g \in Rub$ si et seulement si les trois conditions suivantes sont satisfaites :*

$$E(g) = 1 \tag{3.1}$$

$$\sum_{x \in C} n_x = 0 \ [3] \tag{3.2}$$

$$\sum_{y \in A} n_y = 0 \ [2] \tag{3.3}$$

Plus concrétement, ce théorème assure que :

1. On ne peut transposer qu'une seule pièce mobile ;
2. On ne peut pivoter un coin seul ou une arête seule, les pivotements se font toujours par paire. En ce qui concerne les coins, un coin est pivoté d'un tiers de tour tandis que l'autre est pivoté de deux tiers de tour.

On démontrera ce théorème en deux étapes. On vérifiera d'abord que tout élément de *Rub* vérifie les propriétés énoncées ci-dessus et on montrera que tout élément de $\mathrm{Ker}(rt)$ peut s'écrire comme un produit de rotation des tranches du cube.

Proposition 3.0.1. *Le groupe Rub est un sous-groupe de* $\mathrm{Ker}(rt)$.

Démonstration. Soit $g \in Rub$. Il suffit de montrer que $g \in \mathrm{Ker}(E) \cap \mathrm{Ker}(rt_C \cap \pi_C) \cap \mathrm{Ker}(rt_A \cap \pi_A)$

1. Comme chacun des 6 mouvements élémentaires induit à la fois une permutation sur les coins et sur les arêtes, il induit une permutation $\sigma \circ \sigma'$, où σ et σ' sont deux 4-cycles à support disjoints puisque chacun d'entre eux agit sur les coins (respectivement les arêtes) en laissant fixes les arêtes (respectivement les coins). Par conséquent, comme ces deux 4-cycles ont une signature impaire, la signature de $\sigma \circ \sigma'$ est paire.

   Etant donné que g induit un 4-cycle sur les coins et un 4-cycle sur les arêtes, $E(g) = 1$ et g est bien dans $\mathrm{Ker}(E)$.

2. Notons que chaque rotation de tranches tourne 4 pièces arêtes. Il est dans ce cas plus rapide de considérer l'ensemble F des facettes des arêtes. Etant donné que chaque pièce arête comporte deux facettes visibles, $\mid F \mid = 2 \mid A \mid = 24$. Si g agit sur les arêtes, g sera le produit de deux 4-cycles sur les 24 faces. Il suffit de faire tourner une tranche pour s'en coinvaincre. Le premier 4-cycle permute de manière circulaire les facettes des arêtes sur la tranche et le second permute de manière circulaire les facettes adjacentes aux 4 premières. La signature du produit de ces deux quatre cycles est paire. Comme la permutation induite sur les facettes est paire, cela veut dire qu'il y a conservation de l'orientation des arêtes. Donc $g \in \mathrm{Ker}(rt_A \circ \pi_A)$ ([Col10], p. 5, démonstration de la proposition 6).
3. On peut prendre deux faces privilégiées, par exemple la blanche et la jaune. La face blanche est celle du haut (up), la face jaune est celle du bas (down). Si l'on fait tourner une tranche horizontale, on ne fait que permuter les coins sans changer leur orientation. Si l'on fait tourner une tranche verticale, par exemple la bleue, les coins qui ne sont pas sur la tranche ne bougent pas et les coins sur la tranche sont orientés de 1 ou 2 tiers de tour (deux de 1 tiers de tour et deux de 2 tiers de tour). Leur somme est nulle dans $\mathbb{Z}/3\mathbb{Z}$. Par conséquent, $g \in \mathrm{Ker}(rt_C \circ \pi_C)$ ([Col10], p. 5).

On a montré que $g \in \mathrm{Ker}(E) \cap \mathrm{Ker}(rt_A \circ \pi_A) \cap \mathrm{Ker}(rt_C \circ \pi_C)$, ce qui implique que $Rub \subset \mathrm{Ker}(rt)$. □

Chapitre 4

Résolution du Rubik's cube

La démonstration de l'inclusion inverse est purement constructive. On a besoin d'introduire un algorithme de résolution théorique du Rubik's cube.

Cet algorithme consiste à :

— mettre les arêtes à leur place ;

— les retourner 2 à 2 afin de les orienter correctement ;

— appliquer les 2 étapes précédentes aux coins sans toucher aux arêtes.

Notations

Pour deux faces α, β, on notera $y_{\alpha,\beta}$ l'arête commune à ces deux faces. Bien évidemment, l'arête $y_{\beta,\alpha}$ est la même que $y_{\alpha,\beta}$. Pour trois faces α, β, γ, on notera $x_{\alpha,\beta,\gamma}$ le coin commun à ces trois faces. On remarque de manière analogue que $x_{\beta,\gamma,\alpha}$, $x_{\gamma,\beta,\alpha}, \dots$ sont bien sûr les mêmes que le coin $x_{\alpha,\beta,\gamma}$.

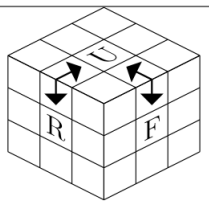
Soit $g \in Rub$ de la forme $g = \rho_C(g)\sigma_C(g)\rho_A(g)\sigma_A(g)$ que l'on notera $\rho_C\sigma_C\rho_A\sigma_A$ pour alléger les notations, avec $\rho_A \in Rot_A, \sigma_A \in \mathfrak{S}_A, \rho_C \in Rot_C, \sigma_C \in \mathfrak{S}_A$.

4.1 Pivotement (rotation) des arêtes

Supposons que σ_A et σ_C sont tous les deux l'identité et $\rho_C = (v_1, \dots, v_8) = (0, \dots, 0)$. Le mouvement

$$h = LFR^{-1}F^{-1}L^{-1}U^2RURU^{-1}R^2U^2R \text{ ([Dan14], } p.18) \tag{4.1}$$

de Rub réoriente les arêtes $y_{U,F}, y_{U,R}$ sans permuter ni changer l'orientation des autres arêtes (cf figure 4.1).



$LFR^{-1}F^{-1}L^{-1}U^2RURU^{-1}R^2U^2R$

Le mouvement pivotant les arêtes $y_{U,F}$ et $y_{U,R}$

Remarque. *Le mouvement qui agit de la sorte n'est pas unique.*

Si y_1 et y_2 sont deux arêtes distinctes, alors il existe $g \in Rub$ envoyant y_1 sur $y_{U,F}$ et y_2 sur $y_{U,R}$. Cela vient de la construction du puzzle du Rubik's cube : si un tel élément n'existait pas, alors il existerait une arête que l'on ne pourrait pas placer à l'endroit d'une autre, et on ne pourrait pas résoudre le Rubik's cube. Il s'en suit que ghg^{-1} réoriente y_1 et y_2 sans permuter ni retourner les autres arêtes.

On rappelle que $\mathrm{Ker}(\sigma_A \circ \pi_A)$ contient les éléments qui laissent invariantes les positions des arêtes mais qui peuvent éventuellement modifier leur orientation. On note Rot_A^0 les éléments de Rot_A de rotation totale nulle.

On a le résultat suivant :

Lemme.

$$\pi_A : Rub \cap \mathrm{Ker}(\sigma_A \circ \pi_A) \to Rot_A^0$$

est une surjection ([Col10], p. 6, Lemme 7).

En d'autres termes, toute réorientation d'arêtes peut être réalisée de manière légale.

Démonstration. On a vu ci-dessus que pour tout couple (y_1, y_2), il existe $g \in Rub$ tel que ghg^{-1} retourne y_1 et y_2 sans déranger les autres arêtes. On rappelle que $Rub \cap \mathrm{Ker}(\sigma_A \circ \pi_A)$ contient toutes les rotations d'arêtes légales.

L'ensemble $\pi_A(Rub \cap \mathrm{Ker}(\sigma_A \circ \pi_A))$ contient les retournement d'arêtes quelconques. Les éléments de cet ensemble sont les générateurs de Rot_A^0. En effet, toute transformation de Rot_A^0 est composée d'un nombre pair de retournement d'arêtes ([Col10], p. 6, "Orientation des bords"), étant donné que la rotation totale doit être nulle modulo 2.

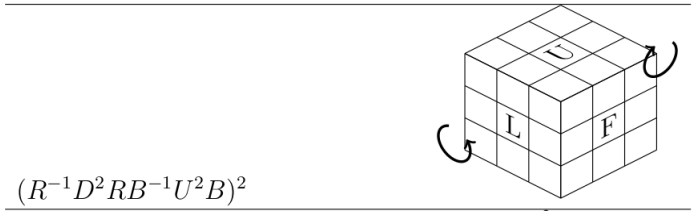
□

4.2 Pivotement des coins

Supposons que σ_A, σ_C sont toutes les deux l'identité et $\rho_A = (w_1, \ldots, w_{12}) = (0, \ldots, 0)$. Le mouvement

$$\gamma = (R^{-1}D^2RB^{-1}U^2B)^2 \text{ ([Dan14], } p.18)$$

tourne le coin $x_{U,F,R}$ d'un tiers de tour, tourne le coin $x_{B,D,L}$ de deux tiers de tour et conserve la position et l'orientation des autres coins (cf figure 4.2).



Le mouvement pivotant les coins $x_{U,F,R}$ et $y_{B,D,L}$

De la même manière que pour l'orientation des arêtes, pour tout couple x_1, x_2 de coins, il existe $g \in Rub$ qui envoie x_1 sur $x_{U,F,R}$ et x_2 sur $x_{B,D,L}$. Il s'en suit que $g\gamma g^{-1}$ réoriente x_1 et x_2 sans déranger les autres coins.

On note Rot_C^0 les éléments de Rot_C de rotation totale nulle. De manière analogue, on obtient :

Lemme. *$\pi_C : Rub \cap Ker(\sigma_C \circ \pi_C) \to Rot_C^0$ est surjective.*

Autrement dit, toute réorientation des coins peut être réalisée légalement.

Démonstration. Par un raisonnement analogue que dans le lemme 4.1, les éléments de $\pi_C(Rub \cap \mathrm{Ker}(\sigma_C \circ \pi_C))$ engendrent Rot_C^0. □

4.3 Permutation des coins et des arêtes

On suppose désormais que $\rho_A = (w_1, \ldots, w_{12}) = (0, \ldots, 0)$ et $\rho_C = (v_1, \ldots, v_8) = (0, \ldots, 0)$.

4.3.1 Permutation des arêtes

Montrons que pour deux arêtes quelconques, il existe un élément de *Rub* qui les transpose. Le mouvement

$$U^{-1}FULU^{-1}L^{-1}F^{-1} \text{ ([War81], } p.186) \tag{4.2}$$

a pour vertu de permuter deux arêtes de la face U sans déranger les autres arêtes du Rubik's cube. De la même manière, par conjugaison convenable de 4.2, on peut ainsi transposer deux arêtes quelconques. Or les transpositions engendrent le groupe symétrique $\mathfrak{S}_A$. Cela prouve qu'il existe un mouvement de *Rub* qui envoie les arêtes à leurs places respectives.

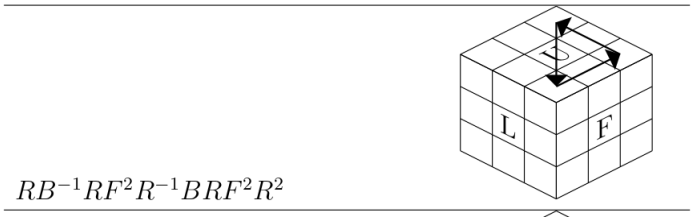
4.3.2 Permutation des coins

Une fois les arêtes mises en place, en vertu de la condition 3.1 du théorème fondamental, la permutation opérant sur les coins doit être paire, donc elle doit être dans le groupe alterné $\mathfrak{A}_8$. Or le groupe alterné de l'ensemble des coins est engendré par les 3-cycles. Ainsi, pour montrer que l'on peut mettre en place les coins par permutation paire, il suffit de prouver qu'il existe bien un 3-cycle agissant sur un triplet de coins quelconque et laissant invariant les autres coins.

Par exemple, le mouvement

$$\mu = RB^{-1}RF^2R^{-1}BRF^2R^2 \text{ ([Dan14], } p.18) \tag{4.3}$$

est un 3-cycle agissant sur les positions des coins $x_{U,F,L}, x_{U,F,R}$ et $x_{U,B,R}$ et laissant invariantes les positions des autres coins (cf figure 4.3).



Le mouvement induisant un 3-cycle sur les coins $x_{U,F,L}, x_{U,F,R}, x_{U,B,R}$

Pour tout triplet $(x_1, x_2, x_3) \in C \setminus \{x_{U,F,L}, x_{U,F,R}, x_{U,B,R}\}$, il existe $g \in Rub$ qui envoie x_1, x_2, x_3 sur les positions de $x, x', x'' \in \{x_{U,F,L}, x_{U,F,R}, x_{U,B,R}\}$. Ainsi le mouvement $g\mu g^{-1}$ induit un 3-cycle sur (x_1, x_2, x_3). Ainsi on peut construire un 3-cycle pour n'importe quel triplet de coins (x_i, x_j, x_k).

4.3.3 Résolution

Partant d'une configuration $c_0 \in \mathrm{Ker}(rt)$, on lui applique une suite de mouvements g composée d'éléments exposés ci-dessus (donc composée de mouvements élémentaires) pour aboutir à $g \circ c_0 = 1_{Rub}$, l'élément neutre de *Rub*. On a donc prouvé que c_0 est le symétrique de g, mais comme *Rub* est un groupe, cela sous-entend que c_0 est bien dans *Rub*. Ainsi $\mathrm{Ker}(rt) \subset Rub$. On a donc prouvé l'égalité de ces deux ensembles.

4.4 Conséquences du théorème fondamental du Rubik's cube

Le raisonnement dans cette section s'inspire en grande partie de [Joy97], p. 194-195, "Some consequences" et de [Dan14], p. 20-21, "Applications of the Legal Rubik's Cube Group".

Supposons que les conditions du théorème 2 soient satisfaites. On définit alors

$$G_0 = \{(\sigma_A, \rho_A, \sigma_C, \rho_C), \sigma_A \in \mathfrak{S}_{12}, \sigma_C \in \mathfrak{S}_8, \tag{4.4}$$

$$\rho_A = (m_1, \ldots, m_{12}), \rho_C = (n_1, \ldots, n_8) \text{ tels que} \tag{4.5}$$

$$\sum_{i=1}^{12} m_i = 0 \ [2] \text{ et } \sum_{i=1}^{8} n_i = 0 \ [3] \ \} \tag{4.6}$$

On définit l'opération binaire $*$ sur G_0 de la manière suivante : si $g = (\sigma_A, \rho_A = (m_y)_{y\in A}, \sigma_C, \rho_C = (n_x)_{x\in C}), g' = (\sigma'_A, \rho'_A = (m'_y)_{y\in A}, \sigma'_C, \rho'_C = (n'_x)_{x\in C})$, alors $g * g' = g'' = (\sigma''_A, \rho''_A, \sigma''_C, \rho''_C)$, où

$$\begin{aligned}\sigma''_A = \sigma_A \circ \sigma'_A, \sigma''_C = \sigma_C \circ \sigma'_C,\\ \rho''_A = (m''_y)_{y\in A} = (m_y + m_{\sigma_A(y)})_{y\in A},\\ \rho''_C = (n''_x)_{x\in C} = (n_x + n_{\sigma_C(x)})_{x\in C}.\end{aligned}$$

Le groupe G_0 muni de la loi $*$ est un groupe.

Théorème 3. *Le groupe G_0 est isomorphe au produit direct de $((\mathbb{Z}/3\mathbb{Z})^7 \rtimes \mathfrak{S}_8) \times ((\mathbb{Z}/2\mathbb{Z})^{11} \rtimes \mathfrak{S}_{12})$, autrement dit*

$$G_0 \simeq ((\mathbb{Z}/3\mathbb{Z})^7 \rtimes \mathfrak{S}_8) \times ((\mathbb{Z}/2\mathbb{Z})^{11} \rtimes \mathfrak{S}_{12}).$$

Corollaire. *En particulier,*

$$\mid G_0 \mid = \mid \mathfrak{S}_8 \mid\mid (\mathbb{Z}/3\mathbb{Z})^7 \mid\mid \mathfrak{S}_{12} \mid\mid (\mathbb{Z}/2\mathbb{Z})^{11} \mid = 8! \cdot 3^7 \cdot 12! \cdot 2^{11}.$$

Démonstration. Par le théorème 2, on détermine les positions des coins et des arêtes. Une fois que l'on a placé 7 coins, l'orientation du dernier coin est déterminée par la condition 3.2 et de ce fait, on réduit $(\mathbb{Z}/3\mathbb{Z})^8$ d'un facteur. De la même manière, une fois les 11 arêtes placées, l'orientation de la dernière arête est donnée par la condition 3.3 et on réduit $(\mathbb{Z}/12\mathbb{Z})^{12}$ d'un facteur . On obtient ainsi le groupe G. □

Défini ainsi, le groupe G_0 n'est pas encore égal à *Rub*. Le résultat suivant établira un lien entre G_0 et *Rub*.

Théorème 1. *Soit le morphisme $\psi : G_0 \to \{\pm 1\}$ défini de la manière suivante :*

$$\text{Pour } g = (\sigma_A, \rho_A, \sigma_C, \rho_C), \psi(g) = \varepsilon(\sigma_A)\varepsilon(\sigma_C).$$

Alors Rub est le noyau du morphisme ψ, autrement dit

$$Rub = \{g = \sigma_C\rho_C\sigma_A\rho_A \in G_0, \varepsilon(\sigma_C)\varepsilon(\sigma_A) = 1\}.$$

Corollaire. *En particulier, le groupe du Rubik's cube Rub est un sous-groupe distingué dans G_0 d'indice 2 et son ordre est*

$$\mid Rub \mid = 2^{10} \cdot 3^7 \cdot 8! \cdot 12!$$

Démonstration. Soit $g \in Rub, g = \sigma_C\rho_C\sigma_A\rho_A$. Par le théorème fondamental 2, $g \in Rub$ si et seulement si g satisfait

$$E(g) = 1 \tag{4.7}$$
$$n_1 + \cdots + n_8 = 0 \ [3] \tag{4.8}$$
$$m_1 + \cdots + m_{12} = 0 \ [2] \tag{4.9}$$

si et seulement si $g \in \mathrm{Ker}(\psi)$ (condition 4.7) et $g \in G_0$ (condition 4.8 et 4.9).

De plus, par le premier théorème d'isomorphisme, $G_0/\mathrm{Ker}(\psi) \simeq \mathrm{Im}(\psi) = \{-1, 1\}$. Comme G_0 est fini, on peut écrire que $[G_0 : \mathrm{Ker}(\psi)] = \frac{|G_0|}{\mathrm{Ker}(\psi)} = 2$. Donc

$$\mid Rub \mid = \frac{\mid G_0 \mid}{2}.$$

□

Chapitre 5

Quelques sous-groupes remarquables du groupe du Rubik's cube

5.1 Le groupe carré (*square group*)

Les résultats de cette section sont tirés de [Ban82], p. 52-53.

Notons le groupe $S = \langle U^2, F^2, L^2, R^2, D^2, B^2 \rangle$ le groupe engendré par les "carrés" de mouvements élémentaires. Nous allons démontrer un résultat remarquable concernant ce groupe carré.

Théorème 4. *Le groupe carré S est d'ordre $2^{13}3^4$.*

Démonstration. Le groupe S agit sur l'ensemble des coins et l'ensemble des arêtes séparement (on peut toujours trouver un mouvement d'arêtes (respectivement de coins) qui n'agit pas sur les coins (respectivement les arêtes)).

On note φ_A l'action de S sur l'ensemble A des arêtes. Cette action de groupes n'est pas transitive et admet trois orbites qui sont (cf [Joy97], p. 218) :

$$\mathrm{Orb}(y_{UF}) = \{y_{UF}, y_{UB}, y_{DB}, y_{DF}\} \tag{5.1}$$
$$\mathrm{Orb}(y_{UL}) = \{y_{UL}, y_{UR}, y_{DR}, y_{DL}\} \tag{5.2}$$
$$\mathrm{Orb}(y_{FL}) = \{y_{FL}, y_{FR}, y_{BR}, y_{BL}\} \tag{5.3}$$

En effet, pour démontrer que l'orbite de l'arête y_{UF} est bien 5.1, on applique les mouvements élémentaires suivants (en fait, ici on montre que les quatre arêtes sont bien dans l'orbite) :

$$y_{UF} \xrightarrow{U^2} y_{UB}$$
$$y_{UF} \xrightarrow{F^2} y_{DF}$$
$$y_{UF} \xrightarrow{U^2B^2} y_{DB}.$$

Montrons que les mouvements élémentaires de S font correspondre les éléments de $\mathrm{Orb}(y_{UF})$ aux éléments de $\mathrm{Orb}(y_{UF})$ (on montre qu'aucune autre arête n'est dans cette orbite).

1. Le mouvement U^2 échange l'arête y_{UF} et y_{UB} ;
2. Le mouvement F^2 échange y_{UF} et y_{DF} ;
3. Le mouvement B^2 échange y_{UB} et y_{DB} ;
4. Le mouvement D^2 échange y_{DF} et y_{DB} ;
5. Les mouvements L^2 et R^2 laissent les 4 arêtes de cette orbite en place.

Comme ces résultats sont valables pour les mouvements élémentaires qui engendrent S, ils le seront aussi pour des mouvements composés.

La démonstration pour les orbites 5.2 et 5.3 est identique.

De manière analogue, on note φ_C l'action de S sur les coins. Cette action n'est pas transitive et admet exactement deux orbites qui sont :

$$\mathrm{Orb}(x_{UFL}) = \{x_{UFL}, x_{UBR}, x_{DFR}, x_{DBL}\} \tag{5.4}$$
$$\mathrm{Orb}(x_{UFR}) = \{x_{UFR}, x_{ULB}, x_{DRB}, x_{DLF}\}. \tag{5.5}$$

On peut monter de la même manière que pour l'orbite $\mathrm{Orb}(y_{UF})$ (5.1) la stabilité de $\mathrm{Orb}(x_{UFL})$ et de $\mathrm{Orb}(x_{UFR})$ par les mouvements élémentaires.

Par conséquent, on peut placer les arêtes de $(4!)^3$ façons différentes. On constate par ailleurs que chaque mouvement $s \in S$ induit une transposition de deux éléments d'une orbite d'arêtes. Cependant, par le théorème fondamental du Rubik's cube 2 condition 3.1, la permutation des coins ainsi que la permutation des arêtes doit être paire. De ce fait, il reste seulement $\frac{(4!)^3}{2} = 2^8 3^3$ emplacements possibles pour les arêtes. De plus, par le théorème fondamental condition 3.2, une fois que l'on a placé 4 coins, il reste seulement 4 positions possibles pour les coins restants du fait que l'on doit conserver l'orientation totale nulle. Donc on a $4! \cdot 4$ façons de placer les coins et finalement,

$$\mid S \mid = \frac{(4!)^3}{2} \cdot 4! \cdot 4 = 2^8 \cdot 3^3 \cdot 2^5 \cdot 3 = 2^{13} \cdot 3^4.$$

□

5.2 Le groupe des quaternions

5.2.1 Lien entre le groupe des quaternions et le Rubik's cube

Le groupe des quaternions $\mathcal{Q}$ muni de la multiplication est formé de la manière suivante :

$$\mathcal{Q} = \langle i, j, k \mid i^2 = j^2 = k^2 = ijk = -1 \rangle.$$

La table de Cayley de $\mathcal{Q}$ sera donnée en annexes.

Remarque.

1. *Les éléments i, j, k sont tous d'ordre 4 dans $\mathcal{Q}$.*
2. *Par le calcul on vérifie que $i^{-1} = -i, j^{-1} = -j, k^{-1} = -k$.*

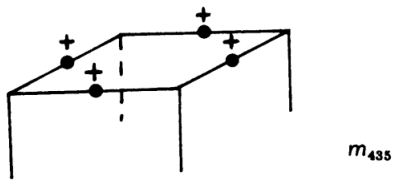
Démonstration.

1. On vérifie que $i^4 = i^2 \times i^2 = 1$, donc l'ordre de i divise 4. Or $i^1 = i \neq 1$ et $i^2 = -1 \neq 1$, donc $ord(i) = 4$. On fait le même raisonnement pour j et pour k.
2. On a $(-i) \times i = 1$, donc $i^{-1} = -i$ par l'unicité de l'inverse.

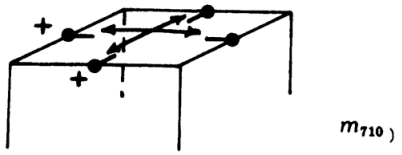
□

Si l'on considère les manoeuvres du Rubik's cube suivantes agissant sur les arêtes $y \in A$ (cf [Ban82], p. 54) :

1. $1 := id$;
2. $-1 := m_{435}$ qui pivote les arêtes y_{UF}, y_{UL}, y_{UB}, y_{UR} d'une demie de tour dans le sens des aiguilles d'une montre (cf 5.1) ;
3. $i = m_{706}$ qui transpose y_{UR} et y_{UF} en pivotant y_{UR} d'une demie de tour et qui transpose y_{UL} et y_{UB} en pivotant y_{UL} d'une demie de tour ;
4. $j = m_{707}$ qui transpose y_{UL} et y_{UF} en pivotant y_{UL} d'une demie de tour et qui transpose y_{UB} et y_{UR} en pivotant y_{UB} d'une demie de tour ;
5. $k = m_{710}$ qui transpose y_{UF} et y_{UB} en pivotant y_{UF} d'une demie de tour et qui transpose y_{UL} et y_{UR} en pivotant y_{UL} d'une demie de tour (cf 5.2).



La manoeuvre m_{435}



La manoeuvre m_{710}

Les mouvements du Rubik's cube permettant de réaliser ces opérations sur les arêtes seront explicités en annexes.

Notons $\mathcal{R}$ le groupe engendré par $-1 = m_{435}, i = m_{706}, j = m_{707}, k = m_{710}$. L'ensemble $\mathcal{R}$ muni de $\circ$ est un groupe dont les éléments vérifient les propriétés suivantes :

$$i^2 = j^2 = k^2 = ijk = -1, \tag{5.6}$$

$$ij = -ji = k, jk = -kj = i, ki = -ik = j. \tag{5.7}$$

Dans ce cas, on a un isomorphisme de groupes $\varphi : \mathcal{Q} \to \mathcal{R}$.

Démonstration. La démonstration de ce résultat est purement calculatoire. On ne va pas l'expliciter ici pour ne pas encombrer le texte. Néanmoins, on constate que, par exemple :

1. Lorsque l'on compose le mouvement m_{435} avec lui-même, on réoriente chaque arête deux fois de suite, ce qui revient à lui appliquer le mouvement identité. On a bien $m_{435}^2 = (-1)^2 = 1$.
2. Voyons ce qu'il se passe lorsque l'on réalise l'opération m_{706} deux fois. Quand on applique m_{706} une première fois, on transpose y_{UR} et y_{UF} en pivotant y_{UR} d'une demie de tour. Lorsque l'on applique m_{706} une fois de plus, y_{UR} et y_{UF} reviennent à leurs sites respectifs, et comme y_{UF} était à l'emplacement de y_{UR}, on lui induit une rotation d'une demie de tour. Finalement, y_{UF} et y_{UR} sont à leurs places de départ et ont subi une rotation d'une demie de tour. Le résultat est identique pour le couple d'arêtes y_{UL} et y_{UB}.

   Faire l'opération m_{706} deux fois revient à réaliser le mouvement m_{435}, donc $i^2 = 1$.

On peut s'amuser à vérifier que les mouvements définis ci-dessus satisfont les relations du groupe quaternionien. On définit par la suite un isomorphisme de groupes entre $\mathcal{R}$ et $\mathcal{Q}$.

□

5.2.2 Propriétés du groupe de quaternions

Dans cette section nous allons montrer que $\mathcal{Q}$ est un groupe d'ordre 8 dont les sous-groupes propres sont cycliques et distingués dans $\mathcal{Q}$. Les résultats s'inspirent de ceux de [Wal17], p. 1-4.

En donnant une liste exhaustive de tous les éléments de $\mathcal{Q} = \{1, -1, i, -i, j, -j, k, -k\}$, on détermine facilement que $| \mathcal{Q} | = 8$.

Le groupe $\mathcal{Q}$ n'est clairement pas commutatif car $ij \neq ji$ d'après 5.7. Le centre $Z(\mathcal{Q})$ se réduit à deux éléments qui sont 1 et -1.

Par le théorème de Lagrange, si $\mathcal{Q}$ possède des sous-groupes propres, alors leur ordre divise nécessairement 8. Donc si les sous-groupes propres de $\mathcal{Q}$ existent, ils sont d'ordre 2 ou 4.

1. Le seul sous-groupe d'ordre 2 de $\mathcal{Q}$ est $\langle -1 \rangle$. En effet, s'il existait un sous-groupe d'ordre 2 contenant i, j ou k, il devrait contenir $-i$ ou $-j$ ou $-k$ et il aurait trois éléments, ce qui contredit le fait qu'il est d'ordre 2.
2. Les sous-groupes d'ordre 4 sont $\langle i \rangle$, $\langle j \rangle$, $\langle k \rangle$. Si on voulait construire un sous-groupe d'ordre 4 avec 2 éléments, par exemple avec i et j, alors il contiendrait nécessairement $1, i, j, -i, -j$, ce qui contredirait le fait qu'il est d'ordre 4.

On va montrer maintenant la propriété suivante :

Proposition 5.2.1. *Tous les sous-groupes de $\mathcal{Q}$ sont distingués dans $\mathcal{Q}$.*

Démonstration.

1. Le centre de $\mathcal{Q}$, $\langle -1 \rangle$, est distingué dans $\mathcal{Q}$, car il est abélien.
2. Montrons que $\langle i \rangle$ est distingué. On a

$$jij^{-1} = ji(-j) = -jij = ijj = i(-1) = -i,$$
$$kik^{-1} = ki(-k) = k(-ik) = kki = -i.$$

Les calculs sont similaires pour $-j$ et $-k$. Donc $\langle i \rangle$ est bien stable par conjugaison. Donc $\langle i \rangle$ est distingué.
Le raisonnement pour montrer que $\langle j \rangle$ et $\langle k \rangle$ sont distingués est analogue.

□

Remarque. *Le groupe des quaternions peut être décrit matriciellement en posant*

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, I = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, J = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, K = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},$$

où I, J, K sont à coefficients dans $\mathbb{C}$.

Chapitre 6

Approfondissement de la notion du produit semi-direct

Le concept central qui nous a aidés à décomposer le groupe du Rubik's cube est le produit semi-direct. En théorie des groupes, il est souvent utile de déconstruire un groupe G en un produit de groupes N et K plus connus. C'est plus simple lorsque G est isomorphe au produit direct de N et de K, mais cette situation est relativement rare. C'est là où on a besoin d'une généralisation du produit direct, le produit semi-direct.

Le contenu de ce chapitre s'inspire principalement de [Del01] (Actions de groupes – Groupes de Sylow, "Produit semi-direct").

6.1 Suite exacte

Commençons par introduire une notion fondamentale au concept du produit direct.

Définition 6.1.1 (Suite exacte)**.** *Soit $G_i, i \in \mathbb{N}$ des groupes et $f_i, i \in \mathbb{N}$ des morphismes de groupes tels que $f_{i+1} \circ f_i$ existe pour tout i. On écrira alors :*

$$\dots \xrightarrow{f_{n-2}} G_{n-1} \xrightarrow{f_{n-1}} G_n \xrightarrow{f_n} G_{n+1} \xrightarrow{f_{n+1}} \dots$$

On dira que cette suite est exacte si pour tout $n \in \mathbb{N}$, $\mathrm{Im}(f_n) = \mathrm{Ker}(f_{n+1})$.

Définition 6.1.2 (Suite exacte courte)**.** *Une suite exacte de type*

$$e \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow e \tag{6.1}$$

est dite suite exacte courte*. Elle est aussi appelée* extension de groupe*. Cette suite est exacte en A, B et C.*

Remarque. *Par abus, on note e ou 1 le groupe réduit à l'élément neutre.*

Remarque. *Dans le cas d'une suite exacte courtre, le morphisme f est injectif et g est surjectif.*

Démonstration. Montrons que f est injectif. Le seul morphisme de groupes allant de $\{e\}$ dans A est l'identité id. Comme la suite courte est exacte en A, on a $\mathrm{Im}(id) = e = \mathrm{Ker}(f)$, ce qui prouve que f est injectif.

Montrons que g est surjectif. Le morphisme allant de C dans e est le morphisme constant qui vaut e. Notons ce morphisme h. Le noyau de h est C tout entier car pour tout élément $c \in C, h(c) = e$. Comme la suite courte est exacte en C, on a $\mathrm{Ker}(h) = \mathrm{Im}(g) = C$, donc g est surjectif. □

Remarque. *Pour cette même suite exacte courte 6.1, $f(A)$ est distingué dans B et $B/f(A) \simeq C$.*

Démonstration. Comme la suite est exacte en B, on a $\mathrm{Im}(f) = f(A) = \mathrm{Ker}(g)$, or $\mathrm{Ker}(g)$ est distingué dans B étant le noyau d'un morphisme de groupes.

Par le premier théorème d'isomorphisme, $B/\mathrm{Ker}(g) \simeq \mathrm{Im}(g)$. Or $\mathrm{Ker}(g) = f(A)$ et $\mathrm{Im}(g) = C$ étant donné que g est surjectif par la remarque précédente. On a donc $B/f(A) \simeq C$. □

Exemple Soit G un groupe et H un sous-groupe distingué de G. On a alors

$$e \longrightarrow H \xrightarrow{i} G \xrightarrow{\pi} G/H \longrightarrow e,$$

où i est l'injection de H dans G et π est la projection canonique.

Démonstration. Cette suite est exacte, car, par la remarque 6.1, i l'injection de H dans G est injective par définition et la projection canonique π de G sur G/H est surjective. □

Exemple On définit $i : A \to A \times B$ par $\forall a \in A, i(a) = i(a, e_B)$ où e_B est l'élément neutre de B. On définit également pour tout couple $(a, b) \in A \times B$, l'application $p : A \times B \to B$ telle que $p((a, b)) = b$. Les morphismes i et p sont respectivement injectif et surjectif et la suite

$$e \longrightarrow A \xrightarrow{i} A \times B \xrightarrow{p} B \longrightarrow e$$

est exacte. Notons que les rôles de A et de B dans ce cas peuvent être échangés.

6.2 Produit semi-direct

Plaçons-nous dans un cadre plus général. Soient G, N, K des groupes et $\varphi : K \to Aut(N)$ un morphisme de groupes.

Proposition 6.2.1. *Le morphisme φ défini comme suit*

$$\varphi : \begin{array}{lll} K \times N & \longrightarrow & N \\ (k, n) & \longmapsto k \cdot n = \varphi(k)(n) & \end{array}$$

est une action de K sur N.

Démonstration.

1. Soit $x \in N$. On a $e \cdot x = \varphi(e)(x) = id(x) = x$.
2. Soient $k, k' \in K$ et $x \in N$. Alors

$$k \cdot (k' \cdot x) = k \cdot (\varphi(k')(n)) = \varphi(k)\varphi(k')(n) = \varphi(kk')(n) = (kk') \cdot n.$$

Cela confirme que c'est bien une action de groupes. □

Le groupe G est le produit ensembliste de N par K et on munit G de la loi $*$ telle que pour $(n, k), (n', k') \in N \times K$:

$$(n, k) * (n', k') = (n\varphi(k)(n'), kk') = (n(k \cdot n'), kk').$$

Définition 6.2.1 (Produit semi-direct)**.** *On appellera G muni de la loi $*$ le **produit semi-direct** de N par K et on notera*

$$G = N \rtimes_\varphi K.$$

Proposition 6.2.2. *L'ensemble G est bien un groupe.*

Démonstration.

1. *Stabilité par $*$:* Soient (n, k) et (n', k'). Naturellement kk' est dans K. D'autre part, $\varphi(k)$ est un automorphisme de N. Ainsi $\varphi(k)(n)$ est bien un élément de N, donc $n\varphi(k)(n)$ est dans N.

2. *Associativité de $*$:* Soient $(n_1,k_1),(n_2,k_2),(n_3,k_3) \in N \times K$. Alors on a d'une part :

$$\begin{aligned}((n_1,k_1)*(n_2,k_2))*(n_3,k_3) &= (n_1\varphi(k_1)(n_2),k_1k_2)*(n_3,k_3)\\ &= (n_1\varphi(k_1)(n_2)\varphi(k_1k_2)(n_3),k_1k_2k_3)\\ &= (n_1(k_1\cdot n_2)(k_1\cdot(k_2\cdot n_3)),k_1k_2k_3)\end{aligned}$$

et d'autre part :

$$\begin{aligned}(n_1,k_1)*((n_2,k_2)*(n_3,k_3)) &= (n_1,k_1)*(n_2\varphi(k_2)(n_3),k_2k_3)\\ &= (n_1\varphi(k_1)(n_2\varphi(k_2)(n_3)),k_1k_2k_3)\\ &= (n_1(k_1\cdot n_2)(k_1\cdot(k_2\cdot n_3)),k_1k_2k_3)\end{aligned}$$

Donc $*$ est bien associative.

3. *Element neutre :* (e_N,e_K) est l'élément neutre de G. En effet, pour tout $(n,k)\in G$, on a

$$(e_N,e_K)*(n,k) = (e_N\varphi(e_K)(n),e_Kk) = (e_Nn,e_Kk) = (n,k).$$

4. *Existence d'un inverse :* Soit $(n,k)\in N\times K$. Alors on a :

$$\begin{aligned}(n,k)*(\varphi(k^{-1})(n^{-1}),k^{-1}) &= (n\varphi(k)(\varphi(k^{-1})(n^{-1}))),kk^{-1})\\ &= (n\varphi(kk^{-1}(n^{-1}),e_K) = (nn^{-1},e_K) = (e_N,e_K).\end{aligned}$$

Donc il existe bien un inverse de (n,k) qui est $(n,k)^{-1} = (\varphi(k^{-1})(n^{-1}),k^{-1})$.

□

Proposition 6.2.3. *Avec les notations de la définition 6.2.1, la suite*

$$1 \longrightarrow N \xrightarrow{i} G = N\rtimes_\varphi K \xrightarrow{p} K \longrightarrow 1,$$

où $i(n) = (n,e_K)$ et $p(n,k) = k$, est une suite exacte.

Démonstration. Montrons que i et p sont bien des morphismes de groupe.

On a

$$i(nn') = (nn',e_K) = (n\varphi(e_K)(n'),e_Ke_K) = (n,e_K)*(n',e_K) = i(n)*i(n'),$$

et

$$p((n,k)*(n',k')) = p(n\varphi(k)(n'),kk') = kk'.$$

Donc i et p sont bien des morphismes de groupe.

On a de plus

$$\mathrm{Ker}(p) = \{(n,k)\in G, p(n,k) = e_K\} = \{(n,e_K), n\in N\} = \mathrm{Im}(i),$$

ce qui montre bien que la suite est exacte. □

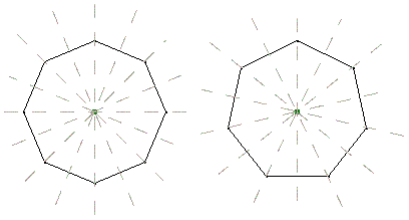
Remarque. *Lorsque $\varphi(k) = id$ pour tout $k\in K$, alors la loi $*$ est celle d'un produit direct.*

Pour introduire un premier exemple, on aura besoin de la définition suivante ([SM70], p. 100) :

Définition 6.2.2 (Groupe diédral)**.** *Le groupe diédral d'ordre n, noté D_{2n}, est le groupe des isométries du plan laissant fixe un polygone régulier P_n de n côtés et de centre O. Il contient $2n$ éléments qui sont :*

— *n rotations du polygone dans son plan d'angle $\frac{2k\pi}{n}, 0\le k<n$;*

— *n réflexions (cf figure 6.1) :*



Les réflexions dans le cas où n est pair (P_n est un octogone) et dans le cas où n est impair (P_n est heptagone).

1. *Si n est impair, alors les réflexions passent par O et par les sommets ;*
2. *Si n est pair, alors les réflexions passent par O et par les milieux des côtés.*

Une représentation par générateurs et relations du groupe diédral est alors la suivante :

$$\langle \sigma, \rho \mid \sigma^2 = 1, \rho^n = 1, \sigma\rho\sigma^{-1} = \rho^{-1} \rangle.$$

Remarque. *De ce fait, pour tout $k \in \{0, \dots, n-1\}$, $\sigma\rho^k\sigma^{-1} = \rho^{-k}$.*

Exemple On montre que le groupe diédral D_{2n} est le produit semi-direct de $\mathbb{Z}/n\mathbb{Z}$ par $\mathbb{Z}/2\mathbb{Z}$.

Démonstration. La démonstration s'inspire de l'exercice 3.3.4 de [Del01] (p. 86).

On sait que $Aut(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^*$, autrement dit tous les automorphismes de $\mathbb{Z}/n\mathbb{Z}$ sont de la forme $x \mapsto \kappa x$, où $(\kappa, n) = 1$.

D'après [Gem09] (p. 1), il existe une action (différente de l'identité dès que $n \geq 3$) de $\mathbb{Z}/2\mathbb{Z}$ sur $\mathbb{Z}/n\mathbb{Z}$. Pour $\delta \in \mathbb{Z}/2\mathbb{Z}$ et $k \in \mathbb{Z}/n\mathbb{Z}$, on pose

$$\delta \cdot k = (-1)^\delta k.$$

Ainsi pour l'élément $\delta = 1$ de $\mathbb{Z}/2\mathbb{Z}$, l'action de $\mathbb{Z}/2\mathbb{Z}$ sur $\mathbb{Z}/n\mathbb{Z}$ (on notera cette action φ par la suite) est différente de l'identité.

On considère le produit semi-direct suivant

$$G = \mathbb{Z}/n\mathbb{Z} \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}.$$

Notons ρ un générateur de $\mathbb{Z}/n\mathbb{Z}$ et σ un générateur de $\mathbb{Z}/2\mathbb{Z}$(on verra dans la démonstration du théorème 5 que l'on peut identifier ρ^k avec le couple $(\rho^k, 1)$ et σ avec $(1, \sigma)$).

D'une part, on a

$$\rho^k\sigma = (\rho^k, 1)(1, \sigma) = (\rho^k, \sigma),$$

et d'autre part, on a :

$$\sigma\rho^{-k} = (1, \sigma)(\rho, 1)^{-1} = (\varphi(\sigma)(\rho^{-k}), \sigma) = (\rho^k, \sigma),$$

autrement dit la relation $\sigma\rho^k\sigma^{-1} = \rho^{-k}$ est satisfaite. Donc le groupe diédral est bien isomorphe à G.

□

On donne une autre caractérisation du produit semi-direct : il s'agit de savoir si un groupe est produit semi-direct de deux de ses sous-groupes.

Théorème 5 (Critère du produit semi-direct de deux sous-groupes d'un groupe G)**.** *Soient G un groupe et H, K des sous-groupes de G. Alors G est le produit semi-direct de H par K si et seulement si :*

1. $H \cap K = \{e_G\}$;
2. $G = HK = \{hk, h \in H, k \in K\}$;
3. H *est distingué dans* G.

Démonstration. La démonstration s'inspire de l'exercice 3.3.5 de [Del01] (p. 86).

Soit $G = H \rtimes_\varphi K$ un produit semi-direct.

On considère la suite exacte suivante :

$$1 \longrightarrow H \xrightarrow{i} G \xrightarrow{p} K \longrightarrow 1. \tag{6.2}$$

On note $\mathcal{H} = \mathrm{Im}(i) = \{(h, 1), h \in H\}$, $\mathcal{K} = \{(1, k), k \in K\}$.

Montrons que $\mathcal{H}$ est distingué dans G, que $\mathcal{H} \cap \mathcal{K} = \{1\}$ et que $G = \mathcal{H}\mathcal{K}$.

Montrons que $\mathcal{H}$ est stable par conjugaison. Le groupe $\mathcal{H}$ est l'image de i, mais comme la suite 6.2 est exacte, $\mathcal{H}$ est aussi le noyau de p. Donc $\mathcal{H}$ est distingué dans G.

Montrons que $\mathcal{H} \cap \mathcal{K} = \{1\}$. Soit $g \in \mathcal{H} \cap \mathcal{K}$. Alors il existe $h \in H$ tel que $g = (h, 1)$ et il existe $k \in K$ tel que $g = (1, k)$. Donc g est bien l'élément neutre de G.

Montrons maintenant que $G = \mathcal{H}\mathcal{K}$. Soit $g = (h, k) \in G$. Alors on peut écrire

$$(h, k) = (h\varphi(1)(1), k) = (h, 1) * (1, k).$$

Par la suite, comme H et $\mathcal{H}$ sont isomorphes, on pourra identifier H et $\mathcal{H}$ (de même pour K et $\mathcal{K}$).

On montre que l'action de K sur H se traduit par une action par automorphismes intérieurs et ensuite on prouvera que si H et K remplissent les conditions énoncées dans 5, alors $G \simeq H \rtimes_\varphi K$, où $\varphi_k(h) = khk^{-1}$.

Par la loi interne de G, on a la relation suivante, pour $h \in H, k \in K$:

$$(1, k)(h, 1)(1, k^{-1}) = (\varphi(k)(h), k)(1, k^{-1}) = (\varphi(k)(h), 1).$$

Si l'on identifie h avec $(h, 1)$, k et k^{-1} avec $(1, k)$ et $(1, k^{-1})$, alors on a :

$$\varphi(k)(h) = khk^{-1}.$$

On suppose maintenant que H et K sont deux sous-groupes de G qui satisfont les conditions de 5. Alors l'application $f : H \rtimes_\varphi K \to G$ définie par

$$\forall (h, k) \in H \rtimes_\varphi K, f((h, k)) = hk$$

est un isomorphisme de groupes.

En effet,

$$\begin{aligned} f((h, k) * (h', k')) &= f((hkh'k^{-1}, kk')) \\ = hkh'k^{-1}kk' &= hkh'k' = f((h, k))f((h', k')). \end{aligned}$$

Donc f est bien un morphisme de groupes. Le morphisme f est injectif, car

$$\mathrm{Ker}(f) = \{h \in H, k \in K \mid hk = 1\},$$

ce qui implique que $n = k^{-1}$. Comme $H \cap K = \{1\}$, $n = k = 1$. Le morphisme f est surjectif, car, par la condition 2 do théorème 5, $G = HK$. Donc f est bien bijectif.

On a ainsi prouvé le théorème. □

Remarque. *Grâce à ce critère, on peut montrer plus aisément que* D_{2n} *est produit semi-direct de* $\mathbb{Z}/n\mathbb{Z}$ *par* $\mathbb{Z}/2\mathbb{Z}$ *en identifiant le sous-groupe des rotations avec* $\mathbb{Z}/n\mathbb{Z}$ *et le sous-groupe engendré par la réflexion avec* $\mathbb{Z}/2\mathbb{Z}$.

Exemple Soit $G = \mathfrak{A}_4$, le groupe alterné de degré 4 et $V = \{e, a, b, c\}$ le sous-groupe contenant les doubles transpositions où

$$a = (1,2)(3,4)$$
$$b = (1,3)(2,4)$$
$$c = (1,4)(2,3)$$

et soit $K = \langle (1,2,3) \rangle$. Alors V et K satisfont le critère du produit semi-direct et on a

$$\mathfrak{A}_4 \simeq (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes_\varphi \mathbb{Z}/3\mathbb{Z}.$$

Démonstration.

1. Explicitons K. On a

   $$K = \langle (1,2,3) \rangle = \{id, (1,2,3), (1,3,2)\}.$$

   Le groupe K ne contient aucune permutation de type (2,2) ce qui implique que $K \cap V = \{1\}$.
2. Montrons que V est distingué dans $\mathfrak{A}_4$. Montrons qu'il est stable par conjugaison. Dans $\mathfrak{S}_n$, deux permutations sont conjuguées si et seulement si elles sont du même type. Donc tous les conjugués des permutations de type (2,2) sont aussi de type (2,2). Or dans $\mathfrak{A}_4$, les seules permutations de type $(2, 2)$ sont celles contenues dans V. Donc V est stable par conjugaison.
3. Dans $\mathfrak{S}_4$, les éléments de signature paire sont soit des cycles de longueur impaire (donc l'identité et les 3-cycles), soit des permutations de type (2,2). Donc si $w \in \mathfrak{A}_4$, alors w est nécessairement produit d'un élément de V et d'un élément de K.

Donc $\mathfrak{A}_4 \simeq V \rtimes_\varphi K$.

Le groupe V est d'ordre 4. Il est soit isomorphe à $\mathbb{Z}/4\mathbb{Z}$, soit isomorphe au groupe de Klein. Or un élément de V différent de l'identité est produit de deux éléments d'ordre 2 distinctes, donc son ordre est le ppcm des ordres de ses facteurs, à savoir 2. Le groupe V ne contient aucun élément d'ordre 4, donc il ne peut être isomorphe à $\mathbb{Z}/4\mathbb{Z}$, donc V est isomorphe au groupe de Klein.

De plus, K étant d'ordre 3, et 3 étant premier, il est isomorphe à $\mathbb{Z}/3\mathbb{Z}$. On en déduit que

$$\mathfrak{A}_4 \simeq (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes_\varphi \mathbb{Z}/3\mathbb{Z}.$$

□

6.3 Section

Considérons la suite exacte

$$1 \longrightarrow N \xrightarrow{i} G \xrightarrow{p} K \longrightarrow 1. \tag{6.3}$$

Proposition 6.3.1. *Le groupe G est le produit semi-direct de N et de K si et seulement si il existe un morphisme $s : K \to G$ tel que*

$$p \circ s = id.$$

Dans ce cas, on dira que s est une ***section****.*

Démonstration.

1. *Sens direct :* Supposons que G est le produit semi-direct de N et de K. Alors i est le morphisme injection et p est le morphisme projection définis dans la proposition 6.2.3.
   Considérons une application $s : K \to G$ telle que

   $$\forall k \in K, s(k) = (1, k).$$

   On vérifie aisément que s est un morphisme de groupes. De plus, on a, pour tout $k \in K$:

$$p \circ s(k) = p((1,k)) = k,$$

ce qui signifie que $p \circ s = id$.

2. *Sens réciproque :* Supposons qu'il existe un morphisme $s : K \to G$ tel que $p \circ s = id$. On rappelle que

$$\mathrm{Im}(i) = \{(n,1), n \in N\};$$
$$\mathrm{Im}(s) = \{(1,k), k \in K\}.$$

Ce sont tous les deux des sous-groupes de G. On peut utiliser le critère 5 afin de vérifier que $G \simeq N \rtimes K$.

(a) Comme la suite 6.3 est exacte, $\mathrm{Im}(i) = \mathrm{Ker}(p)$, ce qui implique que $\mathrm{Im}(i)$ est distingué dans G.

(b) On a $\mathrm{Im}(s) \cap \mathrm{Im}(i) = \{(1,k), k \in K\} \cap \{(n,1), n \in N\} = \{(1,1)\}$.

(c) Tout élément (n,k) de G s'écrit de manière unique comme produit de $(n,1) \in \mathrm{Im}(i)$ et de $(1,k) \in \mathrm{Im}(s)$.

On a vu dans la démonstration du critère 5 que l'on peut identifier N et $\mathrm{Im}(i) = i(N)$. On peut également identifier $\mathrm{Im}(s) = s(K)$ et K, car s est un monomorphisme de groupes par hypothèse. Donc on a prouvé que G est le produit semi-direct de N et de K.

□

Proposition 6.3.2. *On considère la suite exacte 6.3.*

Il existe une section $s : K \to G$ si et seulement si G admet un sous-groupe isomorphe à K dont les éléments sont dans des classes différentes modulo N. On dira que ce sous-groupe est un ***relèvement*** *de K.*

Démonstration.

1. *Sens direct :* On suppose que $s : K \to G$ est une section. Montrons que $\mathrm{Im}(s) = s(K)$ est un relèvement de K. Montrons que deux éléments k_1, k_2 de $s(K)$ congrus modulo $N \simeq p(N)$ sont égaux. En effet,

$$k_1 = k_2 \mod p(N) \iff p(k_1) = p(k_2) \iff p((1,k_1)) = p((1,k_2)) \iff k_1 = k_2.$$

2. *Sens réciproque :* Soit $\mathcal{K}$ un relèvement de K. Montrons que la restriction de p à $\mathcal{K}$ est bijective. Une fois que l'on aura montré cela, une section $s : K \to G$ sera la bijection réciproque de $p_{|\mathcal{K}}$. La projection $p : G \to K$ est surjective par définition. Montrons que $p_{|\mathcal{K}}$ est injective. Soient k, k' deux éléments de K tels que $p_{|\mathcal{K}}(k_1) = p_{|\mathcal{K}}(k_2)$. Donc $k_1 = k_2 \mod p(N)$. Comme $\mathcal{K}$ est un relèvement de K, donc ses éléments sont dans des classes différentes modulo N. Donc $k_1 = k_2$. On a prouvé que $p_{|\mathcal{K}}$ est bijective.

□

Exemple Examinons la suite exacte

$$e \longrightarrow \mathfrak{A}_n \xrightarrow{i} \mathfrak{S}_n \xrightarrow{\varepsilon} \{1,-1\} \longrightarrow e.$$

Un relèvement de $\{1,-1\}$ dans $\mathfrak{S}_n$ est un sous-groupe de $\mathfrak{S}_n$ contenant deux éléments, donc c'est un sous-groupe engendré par une permutation τ d'ordre 2. Pour tous $\sigma, \sigma' \in \langle\tau\rangle$, on doit avoir

$$\sigma = \sigma' \mod \mathfrak{A}_n \iff \sigma = \sigma'.$$

On a $\sigma = \sigma' \mod \mathfrak{A}_n$ si et seulement si $\varepsilon(\sigma) = \varepsilon(\sigma')$. Pour que $\sigma = \sigma'$, il faut que τ soit une permutation impaire. De ce fait, τ ne peut être qu'une transposition.

Ainsi

$$\mathfrak{S}_n \simeq \mathfrak{A}_n \rtimes_\varphi \langle\tau\rangle,$$

avec $\varphi(\tau)(\sigma) = \tau \circ \sigma \circ \tau$.

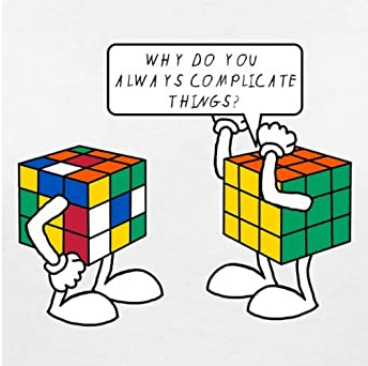
Conclusion

Ce mémoire était une occasion de constater que derrière un casse-tête aussi connu
on a vu que

l'on peut décomposer G, le groupe élargi du Rubik's cube en produit direct de $(\mathbb{Z}/3\mathbb{Z})^8 \rtimes \mathfrak{S}_8$ et de $(\mathbb{Z}/2\mathbb{Z})^{12} \rtimes \mathfrak{S}_{12}$. Pour qu'une opération g de G soit un mouvement autorisé par le mécanisme du Rubik's cube, il doit satisfaire le théorème fondamental du Rubik's cube. Ce théorème nous a permis de calculer le nombre de toutes les opérations que l'on peut effectuer par rotation des six tranches du Rubik's cube, à savoir environ 43 milliards de milliards. Donc lorsque l'on a ce puzzle à la main, on ne peut le résoudre en se fiant au hasard.

Le groupe *Rub* contient des sous-groupes aux structures et propriétés remarquables, comme le groupe isomorphe à $\mathcal{Q}$, le groupe des quaternions. C'est un groupe non-abélien dont les sous-groupes sont tous distingués.

On s'est restreint à l'étude du Rubik's cube de taille 3×3. On pourrait réaliser une étude similaire pour le Rubik's cube de taille 2×2, 4×4 ou 5×5 ou encore pour d'autres puzzles comme le Pyraminx (équivalent tétraédrique du Rubik's cube) ou le Skewb (un équivalent du Rubik's cube dont les axes de rotation passent par les sommets).



Bibliographie

[Ban82] Christoph Bandelow. *Inside Rubik's cube and beyond.* BIRKHAUSER, 1982.

[Col10] Pierre Colmez. Le rubik's cube, groupe de poche. *https ://webusers.imj-prg.fr/ pierre.colmez/rubik.pdf*, 2010.

[Dan14] Lindsey Daniels. Group theory and the rubik's cube. *http ://math.fon.rs/files/DanielsProject58.pdf*, 2014.

[Del01] Jean Delcourt. *Théorie des groupes, rappels de cours, exercices et problèmes corrigés.* Dunod, 2001.

[Gem09] Jérôme Gemoni. Agrégation de mathématiques : Algèbre & géométrie, présentation de groupes. *http ://math.univ-lyon1.fr/ germoni/agreg/presentation.pdf*, 2008-2009.

[Joy97] W. D. Joyner. Mathematics of the rubik's cube. *https ://www.fuw.edu.pl/ konieczn/RubikCube.pdf*, 1996-1997.

[Rio] Ivan Riou. Le rubik's cube et son petit frère, le taquin à retournement, du point de vue de la théorie des groupes. *https ://culturemath.ens.fr/thematiques/superieur/les-maths-derriere-le-rubik-s-cube-et-son-petit-frere-le-taquin-a.*

[Sin81] David Singmaster. *Notes on Rubik's magic cube.* Enslow Publishers, 1981.

[SM70] G. Birkhoff S. Maclane. *Algèbre, Structures fondamentales.* Imprimerie Gauthier-Villars, 1970.

[Wal17] Samuel Wallon. Examen de 2ème session. *https ://pperso.ijclab.in2p3.fr/page_-perso//Wallon/problemes-M1-symetries/examen-session2-2017-corrige.pdf*, 2017.

[War81] André Warusfel. *Réussir le Rubik's cube.* Denoël, 1981.

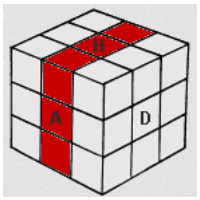
Annexe A

Table de Cayley du groupe quaternionien

Elément	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

Annexe B

Certaines manoeuvres du Rubik's cube



On note MR la rotation de la tranche du milieu (celle qui coupe verticalement les faces F et U) d'un quart de tour dans le sens des aiguilles d'une montre lorsqu'on a la face D devant soi. Alors

$$m_{435} = F^2(MR)^{-1}F^2(MR)^{-1}U^{-1}(MR)^2F^2(MR)F^2U,$$
$$m_{706} = F^2(MR)U^{-1}(MR)^{-1}U^{-1}(MR)U(MR)^{-1}UF^2,$$
$$m_{707} = B^{-1}F^2R^{-1}U^{-1}(MR)^{-1}URU(MR)^{-1}U^{-1}F^2B,$$
$$m_{710} = FU^2F^{-1}U^{-1}L^{-1}B^{-1}U^2BUL.$$