

Rubik's cubes et groupe des rotations du cube

21 septembre 2020, Jean Mouric (jean.mouric@orange.fr)

1 Groupe des mouvements M d'une opération de groupe

1.1 Cas général

Soit G un groupe multiplicatif fini opérant à droite sur un ensemble fini I (opération $(i, g) \rightarrow i \cdot g$).

Soit S l'ensemble des permutations de I ($S = \mathcal{S}_I$).

Soit, pour toute application m de I dans G (i.e. $m \in G^I$), $s(m)$ l'application $i \rightarrow i \cdot m(i)$ de I dans I aussi notée plus loin s_m .

Soit M (M comme Mouvement) l'ensemble des applications m de I dans G telles que $s(m) \in S$

Pour tout élément g de G l'application $i \rightarrow g$ de I dans G est un élément de M qu'on notera c_g : on a $s(c_g)(i) = i \cdot g$

Sur G^I on définit la loi interne $*$ par

$$(m * m')(i) = m(i)m'(s_m(i))$$

On a alors, pour tout $(m, m') \in G^I \times G^I$ et tout $i \in I$,

$$s(m * m')(i) = i \cdot (m * m')(i) = i \cdot (m(i)m'(s_m(i))) = (i \cdot m(i)) \cdot m'(s_m(i)) = s_m(i) \cdot m'(s_m(i)) = s_{m'}(s_m(i)) = (s_{m'} \circ s_m)(i)$$

i.e. en posant pour tout $(s_1, s_2) \in I^I \times I^I$ $s_1 \bullet s_2 = s_2 \circ s_1$,

$$s(m * m') = s(m) \bullet s(m')$$

En particulier $*$ induit une loi interne sur M (qu'on notera aussi $*$) et s un morphisme de $(M, *)$ dans (S, \bullet) .

$(M, *)$ est un groupe car

— $*$ est associative :

$$\begin{aligned} ((m * m') * m'')(i) &= (m * m')(i) m''(s_{m * m'}(i)) = (m * m')(i) m''(s_m \bullet s_{m'}(i)) = (m * m')(i) m''(s_{m'}(s_m(i))) \\ &= m(i) m'(s_m(i)) m''(s_{m'}(s_m(i))) = m(i) (m' * m'')(s_m(i)) = (m * (m' * m''))(i) \quad \text{ceci pour tout } i \in I, \\ \text{donc } (m * m') * m'' &= m * (m' * m'') \quad \text{ceci pour tout } (m, m', m'') \in M \end{aligned}$$

— $*$ a pour élément neutre c_e , où e est l'élément neutre de G :

$$c_e \in M \text{ avec } s(c_e) = \text{id}_I$$

$$\text{et } (m * c_e)(i) = m(i)c_e(s_m(i)) = m(i)e = m(i) = em(i) = c_e(i)m(s_{c_e}(i)) = (c_e * m)(i) \text{ pour tout } i \in I \text{ et tout } m \in M$$

$$\text{i.e. } m * c_e = c_e * m = m \text{ pour tout } m \in M$$

— tout élément m de M a un inverse pour $*$, à savoir l'application $m' : i \rightarrow (m(s_m^{-1}(i)))^{-1}$ de I dans G .

En effet, pour tout $i \in I$ $(m * m')(i) = m(i)m'(s_m(i)) = m(i)m(i)^{-1} = e$ i.e. $m * m' = c_e$, donc $s_m \circ s_{m'} = \text{id}_I$, donc $m' \in M$, et donc aussi $m' * m = c_e$.

L'application $c : g \rightarrow c_g$ de G dans M est un morphisme injectif de groupes par lequel on peut identifier G à un sous-groupe de M .

On sait maintenant que $s : (M, *) \rightarrow (S, \bullet)$ est un morphisme de groupes.

Son noyau $K = \text{Ker}(s)$ est l'ensemble produit $\prod_{i \in I} \text{st}(i)$, où $\text{st}(i)$ est le stabilisateur de $i \in I$ pour l'action de G sur I , et sur ce noyau la loi $*$ de M induit la loi de groupe produit direct :

$$\forall (m, m') \in K \times K \quad \forall i \in I \quad (m * m')(i) = m(i)m'(i)$$

puisque $\forall m \in K \quad s_m(i) = i \quad (s_m = s(m) = \text{id}_I \text{ où } \text{id}_I \text{ est l'élément neutre de } S \text{ (permutation identité de } I))$.

1.2 Cas d'une opération transitive

1.2.1 Suite exacte scindée $0 \rightarrow K \xrightarrow{\iota} M \xrightarrow{s} S \rightarrow 0$

Dans ce cas le morphisme s est surjectif et la suite exacte $0 \rightarrow K \xrightarrow{\iota} M \xrightarrow{s} S \rightarrow 0$ ($\iota : K \rightarrow M$ injection canonique) est scindée, i.e. il existe un morphisme $\ell : S \rightarrow M$ tel que $s \circ \ell = \text{id}_S$. En effet, pour obtenir une application $\ell : S \rightarrow M$ telle que $\forall \sigma \in S \quad s(\ell(\sigma)) = \sigma$ i.e. telle que $\forall i \in I \quad i \cdot \ell(\sigma)(i) = \sigma(i)$, il suffit de choisir pour tout $(i, j) \in I \times I$ un élément g_{ij} de G tel que $i \cdot g_{ij} = j$ (c'est possible puisque l'action de G sur I est transitive) et de poser $\ell(\sigma)(i) = g_{i\sigma(i)}$. ℓ est alors un morphisme de groupes si et seulement si $\forall (\sigma, \sigma') \in S \times S \quad \ell(\sigma \bullet \sigma') = \ell(\sigma) * \ell(\sigma')$ i.e. si et seulement si $\forall (\sigma, \sigma') \in S \times S \quad \forall i \in I \quad \ell(\sigma \bullet \sigma')(i) = (\ell(\sigma) * \ell(\sigma'))(i) = \ell(\sigma)(i) \ell(\sigma')(s_{\ell(\sigma)}(i)) = \ell(\sigma)(i) \ell(\sigma')(\sigma(i))$ i.e. si et seulement si $\forall (\sigma, \sigma') \in S \times S \quad \forall i \in I \quad g_{i\sigma'(\sigma(i))} = g_{i\sigma(i)} g_{\sigma(i)\sigma'(\sigma(i))}$, et pour cela il suffit que les g_{ij} soient tels que $\forall (i, j, k) \in I \times I \times I \quad g_{ij} = g_{ik} g_{kj}$. De tels g_{ij} s'obtiennent, à partir de n'importe quel élément κ de I en choisissant arbitrairement les $g_{\kappa i}$ ($i \in I$) tels $\kappa \cdot g_{\kappa i} = i$ et $g_{\kappa \kappa} = e$ (c'est possible puisque l'action de G sur I est transitive) puis en généralisant par $g_{ij} = g_{\kappa i}^{-1} g_{\kappa j}$. On choisit aussi pour ce qui suit $h_\kappa \in \text{st}(\kappa)$ et on pose plus généralement pour tout $i \in I \quad h_i = g_{\kappa i}^{-1} h_\kappa g_{\kappa i}$. On vérifie que $\forall i \in I \quad h_i \in \text{st}(i)$ et que $\forall (i, j) \in I \times I \quad h_i g_{ij} = g_{ij} h_j$

Marques : A étant un ensemble sur lequel le groupe G opère à droite, supposons qu'on dispose d'une application $\mu : I \rightarrow A$ telle que

$$\forall (i, j) \in I \times I \quad \exists ! g \in G \quad i \cdot g = j \quad \text{et} \quad \mu(i) \cdot g = \mu(j)$$

On dira alors, pour tout $i \in I$, que i est marqué par $\mu(i)$.

Notons pour tout $(i, j) \in I \times I$, g_{ij} l'unique élément g de G tel que $i \cdot g = j$ et $\mu(i) \cdot g = \mu(j)$. On obtient, puisque G agit à droite sur I et sur A , que

$$\forall (i, j, k) \in I \times I \times I \quad g_{ij} = g_{ik} g_{kj}$$

Soit, pour tout $\sigma \in S$, $\ell(\sigma) : i \rightarrow g_{i\sigma(i)} (I \rightarrow G)$. On a, pour tout $i \in I$, $s(\ell(\sigma))(i) = i \cdot \ell(\sigma(i)) = i \cdot g_{i\sigma(i)} = \sigma(i)$, i.e. $s(\ell(\sigma)) = \sigma$, ceci pour tout $\sigma \in S$, i.e. $s \circ \ell = \text{id}_S$. De plus

$$\forall i \in I \quad \ell(\sigma \bullet \sigma')(i) = g_{i\sigma'(\sigma(i))} = g_{i\sigma(i)} g_{\sigma(i)\sigma'(\sigma(i))} = \ell(\sigma)(i) \ell(\sigma')(\sigma(i)) = (\ell(\sigma) * \ell(\sigma'))(i)$$

i.e. $\ell(\sigma \bullet \sigma') = \ell(\sigma) * \ell(\sigma')$. Ainsi ℓ est une section de la suite exacte $0 \rightarrow K \xrightarrow{\ell} M \xrightarrow{s} S \rightarrow 0$.

La démarche adoptée au début de 1.2.1 pour obtenir ℓ revient en fait, en faisant opérer $G = A$ à droite sur lui-même par $(g, a) \rightarrow ag$, à choisir $\kappa \in I$ et les $g_{\kappa i} \in G$ tels que $\kappa \cdot g_{\kappa i} = i$ et à marquer tout $i \in I$ par $\mu(i) = g_{\kappa i}$.

1.2.2 Produit semi-direct isomorphe à M dans le cas de stabilisateurs cycliques

Comme G opère transitivement sur I , les stabilisateurs $\text{st}(i)$ sont isomorphes entre eux. On les suppose dans toute la suite cycliques i.e. isomorphes à un même groupe $\mathbf{Z}/p\mathbf{Z}$. K est alors commutatif isomorphe au groupe additif $(\mathbf{Z}/p\mathbf{Z})^n$ où n est le cardinal de I . On peut dans ce cas faire en 1.2.1 en sorte que pour tout $i \in I$ h_i soit un générateur de $\text{st}(i)$ (en choisissant pour h_κ un générateur de $\text{st}(\kappa)$) puis évaluer l'action par automorphisme intérieur de S sur K associée à la section ℓ de la suite exacte $0 \rightarrow K \xrightarrow{\ell} M \xrightarrow{s} S \rightarrow 0$ de la façon suivante (où $\ell_\sigma = \ell(\sigma)$) :

Posons pour tout $k = (k_i)_{i \in I} \in K$ et tout $i \in I$ $k_i = h_i^{\alpha_k(i)}$, ce qui définit l'exposant $\alpha_k(i)$ modulo p . Alors si $k' = \ell_\sigma * k * \ell_\sigma^{(*-1)}$ on a

$$\forall i \in I \quad k'_i = \ell_\sigma(i) k(\sigma(i)) \ell_\sigma(i)^{-1} = \ell_\sigma(i) h_{\sigma(i)}^{\alpha_k(\sigma(i))} \ell_\sigma(i)^{-1} = (\ell_\sigma(i) h_{\sigma(i)} \ell_\sigma(i)^{-1})^{\alpha_k(\sigma(i))} = (g_{i\sigma(i)} h_{\sigma(i)} g_{i\sigma(i)}^{-1})^{\alpha_k(\sigma(i))} = h_i^{\alpha_k(\sigma(i))}$$

ce qui s'écrit aussi $\forall i \in I \quad \alpha_{k'}(i) \equiv \alpha_k(\sigma(i)) \pmod{p}$

En numérotant de 0 à $n-1$ les éléments de I , on obtient donc que le groupe $(M, *)$ est isomorphe au produit semi-direct $(\mathbf{Z}/p\mathbf{Z})^n \rtimes_\tau \mathcal{S}_n$ où (\mathcal{S}_n, \bullet) est le groupe des permutations de $E_n = \{0, 1, \dots, n-1\}$ et τ le morphisme de (\mathcal{S}_n, \bullet) dans le groupe des automorphismes de $(\mathbf{Z}/p\mathbf{Z})^n$ défini par :

$$\tau(\sigma) : \alpha = (\alpha_0, \alpha_1, \dots, \alpha_{n-1}) \rightarrow \alpha \circ \sigma = (\alpha_{\sigma(0)}, \alpha_{\sigma(1)}, \dots, \alpha_{\sigma(n-1)})$$

La loi interne \odot de ce produit semi-direct est :

$$((\alpha_0, \alpha_1, \dots, \alpha_{n-1}), \sigma) \odot ((\alpha'_0, \alpha'_1, \dots, \alpha'_{n-1}), \sigma') = ((\alpha_0 + \alpha'_{\sigma(0)}, \alpha_1 + \alpha'_{\sigma(1)}, \dots, \alpha_{n-1} + \alpha'_{\sigma(n-1)}), \sigma \bullet \sigma')$$

Cet isomorphisme dépend de ℓ , du choix des générateurs h_i des stabilisateurs $\text{st}(i)$, et de la numérotation des éléments de I . Ce produit semi-direct pourra éventuellement remplacer M .

Exposant total (ou « rotation totale ») :

Pour $k \in K$ posons $\phi_\ell(k) = \sum_{i \in I} \overline{\alpha_k(i)}$ où le surlignement d'un entier désigne sa classe modulo p élément de $\mathbf{Z}/p\mathbf{Z}$. ϕ_ℓ est un morphisme de groupes de K dans $\mathbf{Z}/p\mathbf{Z}$ et $\forall \sigma \in S \quad \phi_\ell(\ell_\sigma * k * \ell_\sigma^{(*-1)}) = \sum_{i \in I} \overline{\alpha_k(\sigma(i))} = \phi_\ell(k)$ puisque σ est une permutation de I . Plus généralement, tout $m \in M$ s'écrit de façon unique $m = k * l$ où $k \in K$ et $l \in \ell(S) : l = \ell_\sigma$ avec $\sigma = s(m)$. Posons $\phi_\ell(m) = \phi_\ell(k)$ (On prolonge ainsi la fonction ϕ_ℓ à M de telle sorte que $\forall m \in \ell(S) \quad \phi_\ell(m) = \bar{0}$). Si de même $m' = k' * l'$ avec $k' \in K$ et $l' \in \ell(S)$, il vient $m * m' = k * l * k' * l' = k * (l * k' * l^{(*-1)}) * l * l' = k'' * l''$ avec $k'' = k * (l * k' * l^{(*-1)}) = k * (\ell_\sigma * k' * \ell_\sigma^{(*-1)})$ et $l'' = l * l'$. Donc $\phi_\ell(m * m') = \phi_\ell(k'') = \phi_\ell(k) + \phi_\ell(\ell_\sigma * k' * \ell_\sigma^{(*-1)}) = \phi_\ell(k) + \phi_\ell(k') = \phi_\ell(m) + \phi_\ell(m')$. On obtient ainsi que ϕ_ℓ est un morphisme de groupes de $(M, *)$ dans $\mathbf{Z}/p\mathbf{Z}$ (d'ailleurs en évidence sur le produit semi-direct $(\mathbf{Z}/p\mathbf{Z})^n \rtimes_\tau \mathcal{S}_n$).

Mouvements particuliers :

Soient $\gamma \in G \setminus \text{st}(\kappa)$ et O_κ l'orbite de κ sous l'action du sous-groupe $\text{gr}(\gamma)$ de G engendré par γ . Écrivons $O_\kappa = \{i_0, i_1, \dots, i_{r-1}\}$ avec $i_0 = \kappa$, $i_\alpha \cdot \gamma = i_{\alpha+1}$ et $r = \text{card } O_\kappa$. On peut choisir la section ℓ (i.e. les h_i et les g_{ij}) tels que $g_{\kappa i_\alpha} = \gamma^\alpha$. Alors le mouvement m défini par $m(i) = i$ si $i \notin O_\kappa$ et $m(i) = \gamma$ si $i \in O_\kappa$ est tel que $\sigma = s(m)$ soit la permutation circulaire $(i_0 \rightarrow i_1 \rightarrow \dots \rightarrow i_{r-1} \rightarrow i_0)$, et on a $m = \ell(\sigma)$ donc $\phi_\ell(m) = \bar{0}$. On a alors aussi $\phi_\ell(m') = \bar{0}$ pour tout conjugué m' de m dans M , en particulier pour l'élément $m' = c(g) * m * c(g)^{(*-1)}$; cet élément $m' : i \rightarrow g m(i \cdot g) g^{-1}$ ($g \in G$) s'obtient à partir de $\gamma' = g \gamma g^{-1}$ comme m à partir de γ : orbite $O_{\kappa'} = \{i'_0 \rightarrow i'_1 \rightarrow \dots \rightarrow i'_{r-1} \rightarrow i'_0\}$ avec $\kappa' = \kappa \cdot g^{-1}$, $i'_\alpha = i_\alpha \cdot g^{-1}$, $m'(i') = \gamma'$ pour $i' \in O_{\kappa'}$ et $m'(i') = i'$ si $i' \notin O_{\kappa'}$. Les quarts de tour de Rubik décrits plus loin correspondent à cette description avec $r = 4$. Leurs rotations totales sont donc nulles.

1.2.3 Digression

Soit une extension de groupe $\mathcal{M} : 0 \rightarrow K \xrightarrow{\ell} M \xrightarrow{s} S \rightarrow 0$ a priori quelconque à ceci près qu'on suppose K commutatif comme c'était le cas précédemment. Alors S opère de manière naturelle par conjugaison sur K (opération τ) et pour toute section ℓ de la suite exacte \mathcal{M} l'opération par morphisme intérieur de S sur K associée à ℓ est τ (indépendamment de ℓ). Mais ℓ peut ne pas exister. En fait l'extension \mathcal{M} est scindée si et seulement si elle est isomorphe à l'extension scindée canonique $0 \rightarrow K \rightarrow K \times_\tau S \rightarrow S \rightarrow 0$, auquel cas les groupes M et $K \times_\tau S$ sont isomorphes.

1.3 Retour au cas général

Les considérations précédentes s'appliquent à chaque orbite de l'action de G sur I lorsque cette opération n'est pas transitive : il y a alors une suite exacte $0 \rightarrow K_O \xrightarrow{\ell_O} M \xrightarrow{s_O} S_O \rightarrow 0$ pour chaque orbite O , d'où résulte une suite exacte $0 \rightarrow K \xrightarrow{\ell} M \xrightarrow{s} S \rightarrow 0$ où K est isomorphe au produit direct des K_O et S au produit direct des S_O . Et, si on suppose les stabilisateurs cycliques, on obtient comme précédemment, après numérotation de chaque orbite, un produit semi-direct isomorphe à M comportant une composante n_O -uplet α_O pour chaque orbite O , où n_O est le cardinal de O , et pour lequel \mathcal{S}_n est remplacé par le produit des \mathcal{S}_{n_O} .

2 Application aux Rubik's cubes

Le Rubik's cube, dans son état *initial*, est rapporté au repère orthormal direct $(O; e_1, e_2, e_3)$ où O est le centre du cube et où les centres des faces orange, verte et blanche sont, pour les Rubik's cubes 2x2 et 3x3, respectivement les points $O + e_1$, $O + e_2$ et $O + e_3$, et pour le Rubik's cube 4x4 les points $O + 3e_1$, $O + 3e_2$ et $O + 3e_3$ (Repère **OVB**).

Les faces rouge, bleue et jaune sont respectivement opposées aux faces orange, verte et blanche comme dans le cube officiel.

G est le groupe des rotations conservant le cube. Les éléments g de G , assimilés à des rotations vectorielles puisqu'ils fixent O qui sera sous-entendu, sont représentés en base (e_1, e_2, e_3) par les 24 matrices 3-3 de déterminant 1 dont chaque élément vaut $-1, 0$, ou 1 avec un et un seul non nul par ligne et par colonne. On identifiera G à ce groupe de matrices.

On visualise le cube dans un second repère orthonormal direct $(O'; e'_1, e'_2, e'_3)$ déduit du précédent par une rotation (a priori quelconque) élément de G en convenant que e'_1 pointe vers l'avant, e'_2 pointe vers la droite et e'_3 pointe vers le haut (Repère **ADH**). Ce repère, utilisé pour les mouvements globaux du cube, facilite l'utilisation répétée de formules définissant des séquences de quarts de tours de Rubik.

Un point quelconque est représenté dans chaque repère par une matrice ligne à trois éléments, par exemple $X = [x_1, x_2, x_3]$ en repère **OVB** et $X' = [x'_1, x'_2, x'_3]$ en repère **ADH** avec $X = X'P$ où P est la matrice de passage de (e_1, e_2, e_3) à (e'_1, e'_2, e'_3) i.e. un élément quelconque de G . Si R et R' sont les matrices d'une même rotation respectivement en base (e_1, e_2, e_3) et (e'_1, e'_2, e'_3) transformant le point M représenté par les matrices lignes X et X' en le point N représenté par les matrices lignes Y et Y' , on a $XR = Y$ et $X'R' = Y'$ et $X = X'P$ et $Y = Y'P$, donc $PR^tP = R'$ où $^tP = P^{-1}$ (matrice orthogonale !) est la transposée de P .

Le plan de projection porté à l'écran est le plan passant par O orthogonal au vecteur $e'_1 + e'_2 + e'_3$ rapporté au repère orthonormal $(O; \frac{-e'_1+e'_2}{\sqrt{2}}, \frac{-e'_1-e'_2+2e'_3}{\sqrt{6}})$ avec un facteur d'échelle $c = \frac{\sqrt{6}}{2}$. Le point $O + e'_1 + e'_2 + e'_3$ est « en avant » visible, Les faces cachées du cube sont montrées dans des miroirs.

En théorie le Rubik's cube est divisé en minicubes mobiles sous l'action de G (il y en a n^3 pour le Rubik's cube $n \times n$). Mais seul ceux qui présentent une couleur sur les faces du Rubik's cube sont réellement pris en compte, indexés par les matrices de coordonnées de leurs centres dans l'état *initial* du cube par rapport au repère **OVB**, matrices formant l'ensemble I . Les mouvements (ou mélanges ou états) du Rubik's cube sont les mouvements de l'opération à droite de G (groupe de matrices g) sur I par produit matriciel : $(i, g) \rightarrow i \cdot g$ où $i = [i_1, i_2, i_3]$ est une matrice ligne et $g = [g_{\alpha\beta}]_{1 \leq \alpha, \beta \leq 3}$ (produit ligne par colonnes). Le mouvement m fait passer en le réorientant sous l'action de $m(i) \in G$ le minicube d'indice i à l'emplacement centré en $s(i) = i \cdot m(i)$.

2.1 Rubik's cube 2x2

I est l'ensemble C des « coins » i.e. des 8 triplets représentés en repère **OVB** par les matrices lignes $[x, y, z]$ où x, y, z valent ± 1 . L'opération de G sur I est transitive et les stabilisateurs des coins sont isomorphes à $\mathbf{Z}/3\mathbf{Z}$.

On peut *marquer* le cube en utilisant l'ensemble $A = \{(\pm 1, 0, 0), (0, \pm 1, 0), (0, 0, \pm 1)\}$ symbolisant les faces du cube et la fonction $\mu : [x, y, z] \rightarrow (0, 0, z)$. On peut alors conformément à **1.2** se servir du produit semi-direct M_2 en suivant lors des mouvements de Rubik du cube le décalage des marques inscrites sur les faces des minicubes par rapport à leurs emplacements sur le cube : ces décalages correspondent aux exposants des éléments générateurs choisis pour les stabilisateurs des éléments de I . On constate aussi que de cette façon les quarts de tour de Rubik m autour de $(0, 0, 1)$ sont leurs propres relèvements ($m = \ell(s(m))$) et ont donc une *rotation totale nulle* ainsi que les autres quarts de tour de Rubik puisque ces derniers leur sont conjugués.

Le groupe de Rubik R , sous-groupe de M engendré par les quarts de tour de Rubik, est donc inclus dans le noyau de la rotation totale des coins. En fait R est égal à ce noyau : en effet l'algorithme de résolution par niveaux (supérieur et inférieur) permet toujours (rotation totale des coins nulle ou pas) de remonter le niveau supérieur puis de remettre en place les coins inférieurs par un ou deux cycles d'ordre trois réalisables par séquences de Rubik (*après* s'être éventuellement par rotation d'un quart de tour du niveau inférieur ramené à une permutation paire des coins). Et enfin, si ce n'est pas fini (coins inférieurs mal orientés), comme la rotation totale des coins est nulle, on peut terminer par rotations simultanées en sens inverses (éventuellement répétées) de deux coins adjacents puisqu'on dispose de séquences de Rubik pour le faire.

M est isomorphe au produit semi-direct

$$M_2 = (\mathbf{Z}/3\mathbf{Z})^8 \times \mathfrak{S}_8$$

muni de la loi \odot suivante :

$$(\alpha_c, \sigma_c) \odot (\alpha'_c, \sigma'_c) = (\alpha''_c, \sigma''_c)$$

avec

$$\forall i \in \{0, 1, \dots, 7\} \quad \alpha''_c(i) = \alpha_c(i) + \alpha'_c(\sigma_c(i)) \quad \text{et} \quad \sigma''_c = \sigma_c \bullet \sigma'_c$$

R est isomorphe au sous-groupe défini par $\sum_{i=0}^7 \alpha_c(i) \equiv 0 \pmod{3}$

2.2 Rubik's cube 3x3

Ici $I = \{-1, 0, 1\}^3 \setminus \{[0, 0, 0]\}$. L'opération de G sur I comporte 3 orbites I_c, I_a, I_m formées respectivement de 8 « coins » (3 faces visibles), 12 « angles » (2 faces visibles) et 6 « milieux » (une seule face visible) :

Les 8 coins sont représentés par les matrices lignes $[x, y, z]$ où x, y, z valent ± 1 , les angles par les matrices lignes $[x, y, z]$ où un et un seul de x, y, z vaut 0 les deux autres valant ± 1 et les 6 « milieux » (ou « centres ») par les matrices lignes $[x, y, z]$ où deux parmi x, y, z valent 0 le troisième valant ± 1 .

Les stabilisateurs des angles sont isomorphes à $\mathbf{Z}/2\mathbf{Z}$, les stabilisateurs des coins à $\mathbf{Z}/3\mathbf{Z}$ et les stabilisateurs des milieux à $\mathbf{Z}/4\mathbf{Z}$.

On peut marquer le cube en utilisant l'ensemble $A = \{(\pm 1, 0, 0), (0, \pm 1, 0), (0, 0, \pm 1)\}$ et en posant pour les coins $\mu(x, y, z) = (0, 0, z)$, pour les angles $\mu(0, y, z) = (0, y, 0)$, $\mu(x, 0, z) = (0, 0, z)$ et $\mu(x, y, 0) = (x, 0, 0)$. De cette façon les quarts de tour de Rubik autour de $(0, 0, 1)$ sont, pour les orbites I_c et I_a , les mouvements m associés comme en 1.2.2 à $\gamma \in G \setminus \text{st}(\kappa)$, où γ est une rotation d'un quart de tour autour de $\kappa = (0, 0, 1)$; ils sont donc leurs propres relèvements ($m = \ell(s(m))$) et leurs rotations totales sont nulles pour ces deux orbites ; de même pour les autres quarts de tour de Rubik puisque ces derniers leur sont conjugués dans M .

À noter que les minicubes indexés par les milieux sont fixes sous l'action des quarts de tour de Rubik (ces derniers n'affectent pas les tranches centrales). Deux cas se présentent alors suivant qu'on décide de prendre en compte les mouvements de rotation par quarts de tour sur eux même des minicubes indexés par les milieux ou de les ignorer : ignorer ces mouvements revient à supprimer les milieux dans I , c'est l'attitude la plus courante. On peut dans tous les cas remplacer M par son sous-groupe M_1 de mouvements laissant fixe les milieux (mouvements m tels que, pour tout milieu i , $m(i) = i$).

Le groupe de Rubik R , sous-groupe de M (en fait de M_1) engendré par les quarts de tour de Rubik, est donc inclus dans les noyaux des rotations totales associées aux orbites I_c et I_a . De plus, comme aux opérations de Rubik sont associées des permutations de I_c et I_a impaires (cycles d'ordre 4), tout élément de R induit des permutations de I_c et I_a de même parité. Si on prend en compte la rotation des milieux, la signature commune aux permutations de I_c et I_a est $(-1)^r$ où r est la rotation totale des milieux.

L'algorithme de résolution par niveaux donne la réciproque : tout élément de M_1 qui appartient aux noyaux des rotations totales associées aux orbites I_c et I_a et induit des permutations de I_c et I_a de même parité (de signature $(-1)^r$ où r est la rotation totale des milieux si on les prend en compte) appartient à R .

En fait cet algorithme permet toujours de remonter les niveaux supérieur et médian avec annulation des rotations des minicubes centraux sur ces deux niveaux.

L'égalité des parités et la nullité des deux rotations totales (celle des angles et celle des coins), et éventuellement la relation entre ces parités et la rotation totale des milieux, permettent ensuite de remonter le niveau inférieur :

Observer pour cela que

- comme la rotation totale des angles est nulle, le nombre d'angles du niveau inférieur dont la face jaune est vers le bas est pair (0, 2 ou 4) et que dans les deux premiers cas on dispose d'une séquence de Rubik permettant de ramener ce nombre à 4 pour obtenir la « croix jaune ».
- quitte à effectuer une rotation d'un quart de tour de la face inférieure, on peut supposer que les permutations des angles et des coins sont paires. On peut alors par un ou deux cycles d'ordre 3 réalisables par séquences de Rubik conservant l'acquis ramener les angles à leur place, puis de la même façon ramener les coins à leur place.
- Comme la rotation totale des coins est nulle, on peut terminer par rotations simultanées en sens inverses (éventuellement répétées) de deux coins adjacents, puisqu'on dispose de séquences de Rubik pour le faire (voir les programmes Caml joints qui traitent aussi les rotations des centres).

Le groupe des mouvements avec prise en compte des rotations des centres est isomorphe au produit semi-direct

$$(\mathbf{Z}/4\mathbf{Z})^6 \times (\mathbf{Z}/2\mathbf{Z})^{12} \times \mathfrak{S}_{12} \times (\mathbf{Z}/3\mathbf{Z})^8 \times \mathfrak{S}_8$$

muni de la loi \odot suivante :

$$(\alpha_m, \alpha_a, \sigma_a, \alpha_c, \sigma_c) \odot (\alpha'_m, \alpha'_a, \sigma'_a, \alpha'_c, \sigma'_c) = (\alpha''_m, \alpha''_a, \sigma''_a, \alpha''_c, \sigma''_c)$$

$$\text{avec } \begin{cases} \forall i \in \{0, 1, \dots, 5\} & \alpha''_m(i) = \alpha_m(i) + \alpha'_m(i) \\ \forall i \in \{0, 1, \dots, 11\} & \alpha''_a(i) = \alpha_a(i) + \alpha'_a(\sigma_a(i)) \\ \forall i \in \{0, 1, \dots, 7\} & \alpha''_c(i) = \alpha_c(i) + \alpha'_c(\sigma_c(i)) \\ \sigma''_a = \sigma_a \bullet \sigma'_a & \sigma''_c = \sigma_c \bullet \sigma'_c \end{cases}$$

R correspond alors au sous-groupe défini par les conditions :

$$\text{sign}(\sigma_a) = \text{sign}(\sigma_c) = (-1)^{\sum_{i=0}^5 \alpha_m(i)} \quad \text{et} \quad \sum_{i=0}^{11} \alpha_a(i) = 0 \quad \text{et} \quad \sum_{i=0}^7 \alpha_c(i) = 0$$

(Omettre le facteur direct $(\mathbf{Z}/4\mathbf{Z})^6$ et les α_m si on ne considère pas les rotations des milieux des faces).

2.3 Rubik's cube 4x4

Ici $I = \{-3, -1, 1, 3\}^3 \setminus \{-1, 1\}^3$ dont les 56 éléments se répartissent sous l'action du groupe du cube G en 3 orbites :

- les coins $[x, y, z]$, tels que x, y, z valent ± 3
- les angles $[x, y, z]$, tels que deux parmi x, y, z valent ± 3 et le troisième ± 1
- les milieux $[x, y, z]$, tels que deux parmi x, y, z valent ± 1 et le troisième ± 3

Les stabilisateurs des coins sont ici encore isomorphes à $\mathbf{Z}/3\mathbf{Z}$

Comme les stabilisateurs des angles et des milieux sont triviaux, on obtient, par exemple en marquant les coins comme précédemment, que la suite $0 \rightarrow K \rightarrow M \rightarrow S \rightarrow 0$ est exacte et scindée : On dispose d'une section à laquelle est associé un morphisme de rotation totale des coins.

Comme précédemment la rotation totale des coins est nulle pour les quarts de tour des tranches externes donc pour tout élément du sous-groupe de Rubik R de M puisque les quarts de tour des tranches internes ne touchent pas aux coins. Les permutations des milieux et des coins associées aux quarts de tour des tranches externes étant impaires (cycles d'ordre 4) et les permutations des milieux et des coins associées aux quarts de tour des tranches internes étant paires, à tout élément de R sont associées des permutations des milieux et des coins de même parité.

On vérifie inversement que ces conditions suffisent à assurer l'appartenance à R d'un élément de M .

Cependant on est généralement plutôt intéressé par les états du cube pouvant être ramenés par quarts de tour de Rubik à un état où toutes les faces du cube sont monocolores. On vérifie que ces états sont ceux dont la rotation totale des coins est nulle.

La résolution du cube, i.e. le passage par quarts de tour de Rubik d'un état mélangé correct à l'état neutre (résolution complète) ou à un état où les faces sont monocolores (résolution partielle) peut se faire en plusieurs étapes en commençant par reconstituer un cube 3x3 dans le cube 4x4 :

1. Appariement des angles présentant les deux mêmes couleurs (pour former 2 par 2 les angles du cube 3x3)
2. Regroupement des milieux par couleurs (pour former 4 par 4 les milieux du cube 3x3)
3. (uniquement pour résolution complète) Permutation des 4 centres (de même couleur) dans chacune des 6 faces
4. Contrôles de parités, car le cube 3x3 obtenu peut être incorrect comme dans le cas où on réassemble au hasard un cube 3x3 éclaté.
5. Résolution complète (i.e. prenant en compte la rotation des centres) ou incomplète du cube 3x3 suivant qu'on vise une résolution complète ou incomplète du cube 4x4

On peut aussi regrouper les milieux avant d'apparier les angles. Les contrôles de parités peuvent être reportés dans la résolution par niveaux du cube 3x3 au début du traitement du troisième niveau.

Le groupe des mouvements M est isomorphe au produit semi-direct

$$\mathcal{S}_{24}^2 \times (\mathbf{Z}/3\mathbf{Z})^8 \times \mathcal{S}_8$$

muni de la loi \odot suivante :

$$(\sigma_m, \sigma_a, \alpha_c, \sigma_c) \odot ((\sigma'_m, \sigma'_a, \alpha'_c, \sigma'_c) = (\sigma''_m, \sigma''_a, \alpha''_c, \sigma''_c))$$

$$\text{avec } \begin{cases} \sigma''_m = \sigma_m \bullet \sigma'_m \\ \sigma''_a = \sigma_a \bullet \sigma'_a \\ \sigma''_c = \sigma_c \bullet \sigma'_c \end{cases} \quad \text{et} \quad \forall i \in \{0, 1, \dots, 7\} \quad \alpha''_c(i) = \alpha_c(i) + \alpha'_c(\sigma_c(i))$$

R est le sous-groupe défini par les conditions :

$$\text{sign}(\sigma_m) = \text{sign}(\sigma_c) \quad \text{et} \quad \sum_0^7 \alpha_c(i) \equiv 0 \quad [3]$$

M a $N = 24!^2 \cdot 3^8 \cdot 8!$ éléments, R en a $N/6$, et si on considère que les milieux ne peuvent être distingués que par leurs couleurs et qu'on ne peut distinguer deux états du cubes qui ne diffèrent que par une rotation globale, il ne reste que $N/(3 \cdot 4!^6 \cdot 4!)$ états discernables (la condition sur les signatures disparaît ici) i.e.

$$24!^2 \cdot 3^7 \cdot 8!/24^7 = 7\,401\,196\,841\,564\,901\,869\,874\,093\,974\,498\,574\,336\,000\,000\,000$$