

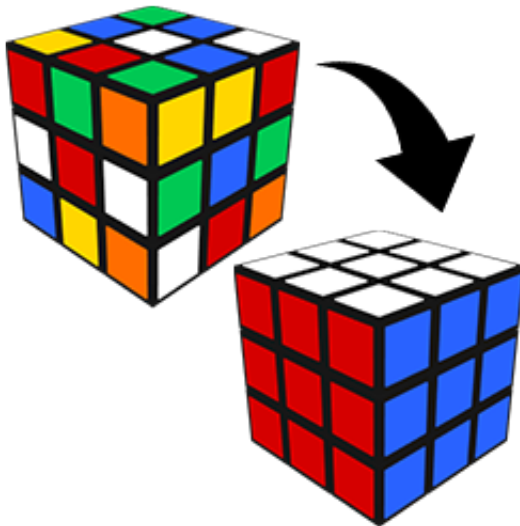
TIPE : Groupe du Rubik's Cube et produit semi-direct

Armand Perrin

10854

June 7, 2024

Le Rubik's Cube



Mouvements légaux



Problématique :

Comment décrire le groupe du Rubik's Cube à l'aide de groupes connus ?

1 Outils sur les groupes

- Groupes compléments
- Produit semi-direct interne
- Produit semi-direct externe

2 Le Groupe du Rubik's cube

- Description du groupe du Rubik's cube
- Positionnement des pièces
- Orientation des pièces

1 Outils sur les groupes

- Groupes compléments
- Produit semi-direct interne
- Produit semi-direct externe

2 Le Groupe du Rubik's cube

- Description du groupe du Rubik's cube
- Positionnement des pièces
- Orientation des pièces

Définition 1 : (Compléments)

Soit G un groupe de neutre 1 et H, K deux sous-groupes de G . On dit que K est un complément de H dans G si $G = HK$ et $H \cap K = \{1\}$.

Proposition 1 :

Dans ce contexte, K est un complément de H dans G si et seulement si l'application $\varphi : \begin{cases} H \times K & \rightarrow G \\ (h, k) & \mapsto hk \end{cases}$ est bijective.

Définition 2 : (Sous-groupe normal)

Un sous-groupe H d'un groupe G est dit normal, ou distingué dans G si il est stable par conjugaison par les éléments de G , i.e :

$$\forall g \in G \quad \forall h \in H \quad ghg^{-1} \in H$$

On le note $H \triangleleft G$.

Remarque : On peut montrer facilement que le noyau d'un morphisme de groupe est un sous groupe normal.

Dans cette partie on fixe G un groupe, H et K des sous groupes de G .

Définition 3 : (Loi du produit semi-direct interne)

On définit la loi de composition interne \cdot sur $H \times K$ par

$$\cdot : \begin{cases} (H \times K)^2 & \rightarrow & H \times K \\ (h, k), (h', k') & \mapsto & (hkh'k^{-1}, kk') \end{cases} \quad \text{Elle est bien définie si } H \triangleleft G,$$

on appelle alors produit semi-direct interne et on note $H \rtimes K$ le couple $(H \times K, \cdot)$.

Proposition 2 :

Si $H \triangleleft G$ et si K est un complément de H dans G , alors $H \rtimes K$ est un groupe et $\varphi : \begin{cases} H \rtimes K & \rightarrow G \\ (h, k) & \mapsto hk \end{cases}$ est un isomorphisme de groupes.

Produit semi-direct externe

Dans cette partie on considère H et K deux groupes quelconques et $f : K \rightarrow \text{Aut}(H), k \mapsto f_k$ un morphisme de K dans $\text{Aut}(H)$.

Définition 4 : (Loi du produit semi-direct externe)

On définit la loi de composition interne \cdot_f sur $H \times K$ par

$$\cdot_f : \begin{cases} (H \times K)^2 & \rightarrow & H \times K \\ (h, k), (h', k') & \mapsto & (hf_k(h'), kk') \end{cases} \quad \text{on appelle produit semi-direct externe relatif à } f \text{ et on note } H \rtimes_f K \text{ le couple } (H \times K, \cdot_f).$$

Proposition 3 :

$G := H \rtimes_f K$ est un groupe de neutre $(1, 1)$ avec $(h, k)^{-1} = (f_{k^{-1}}(h^{-1}), k^{-1})$ et si on pose les sous groupes de G : $H_G := H \times \{1\}$, $K_G := \{1\} \times K$ ils sont respectivement isomorphes à H et K , de plus H_G est normal dans G , K_G est un complément de H_G dans G et $G \cong H_G \rtimes K_G$.

Proposition 4 : (Passage du produit interne au produit externe)

Soient G un groupe, H et K des sous groupes de G avec $H \triangleleft G$ et K complément de H dans G tels que $G \cong H \rtimes K$, notons

$$f : \begin{cases} K & \rightarrow \text{Aut}(H) \\ k & \mapsto (h \mapsto khk^{-1}) \end{cases}$$

Alors f est un morphisme de groupes et $G \cong H \rtimes_f K$.
 f est appelé "morphisme de conjugaison de H par K ".

Proposition 5 : (Isomorphismes de produits semi-direct)

Soient H, H', K, K' des groupes tels que l'on ait des isomorphismes :

$$\varphi : H \rightarrow H'$$

$$\psi : K \rightarrow K'$$

Soit $f : K \rightarrow \text{Aut}(H), k \mapsto f_k$ un morphisme, et

$$\tilde{f} : \begin{cases} K' & \rightarrow & \text{Aut}(H') \\ k & \mapsto & \varphi \circ f_{\psi^{-1}(k)} \circ \varphi^{-1} \end{cases}$$

Alors \tilde{f} est un morphisme et

$$H \rtimes_f K \cong H' \rtimes_{\tilde{f}} K'$$

1 Outils sur les groupes

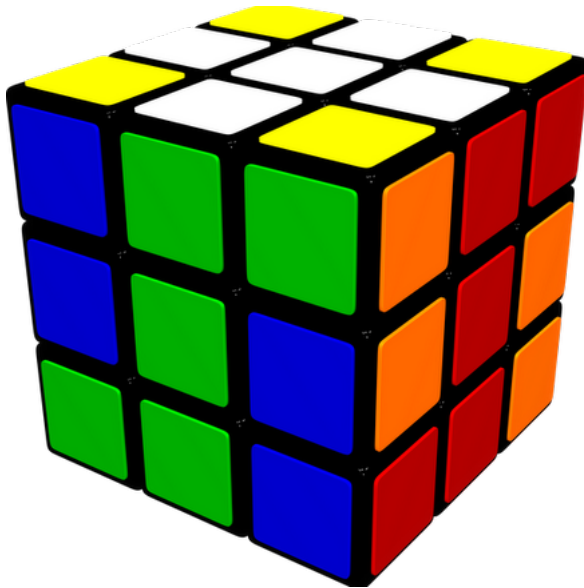
- Groupes compléments
- Produit semi-direct interne
- Produit semi-direct externe

2 Le Groupe du Rubik's cube

- Description du groupe du Rubik's cube
- Positionnement des pièces
- Orientation des pièces

- S_n est le groupe symétrique d'ordre n
- \mathbb{Z}_n le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$
- G le groupe du rubik's cube constitué de tous les mouvements possibles en démontant et remontant le cube.
- id le neutre de G laissant invariant le cube.
- "l'état final" désigne le cube complété (chaque face n'affiche qu'une couleur).

Le Rubik's Cube



Chaque mouvement correspond exactement à un état du cube La loi de composition que l'on note multiplicativement sur G envoie (g, g') sur gg' , le mouvement qui applique successivement g' puis g au cube. On distingue 3 types de pieces du Rubik's cube :

- les centres
- les arêtes
- les sommets

On observe premièrement que tout mouvement est constitué d'un mouvement sur les arêtes et d'un mouvement sur les sommets.

Définition 5 :

G_a : groupe des mouvements sur les arêtes (laissant fixes les sommets)

G_s : groupe des mouvements sur les sommets (laissant fixes les arêtes)

Proposition 6 :

$$G \cong G_a \times G_s.$$

Preuve : On montre que l'application : $\varphi : \begin{cases} G_a \times G_s & \longrightarrow G \\ (g_a, g_s) & \longmapsto g_a g_s \end{cases}$ est un isomorphisme de groupes. Le fait que φ soit bijective traduit notre précédente observation. C'est un morphisme car par commutativité des éléments de G_a avec ceux de G_s

$$\forall ((g_a, g_s), (g'_a, g'_s)) \in (G_a \times G_s)^2 :$$

$$\begin{aligned} \varphi((g_a, g_s)(g'_a, g'_s)) &= \varphi((g_a g'_a, g_s g'_s)) = g_a g'_a g_s g'_s \\ &= (g_a g_s)(g'_a g'_s) = \varphi(g_a, g_s) \varphi(g'_a, g'_s) \quad \square \end{aligned}$$

Positionnement des pièces

Il y a 12 arêtes qui peuvent toutes prendre chacune un des 12 emplacements d'arête et 8 sommets qui peuvent tous prendre un des 8 emplacements de sommet.

Définition 6 :

On définit deux applications $\sigma_a : G_a \rightarrow S_{12}$ et $\sigma_s : G_s \rightarrow S_8$ représentant respectivement les positions des arêtes et des sommets de la manière suivante :

On numérote de 1 à 8 les emplacements de sommets ainsi que les sommets, de telle sorte que dans l'état final, pour $i = 1, \dots, 8$ le sommet i soit en position i . On pose alors $\sigma_s(g) \in S_8$ l'unique permutation telle que pour $i = 1, \dots, 8$ le sommet $\sigma_s(g)(i)$ soit en position i après le mouvement g appliqué depuis l'état final. σ_a est définie de manière similaire avec les arêtes.

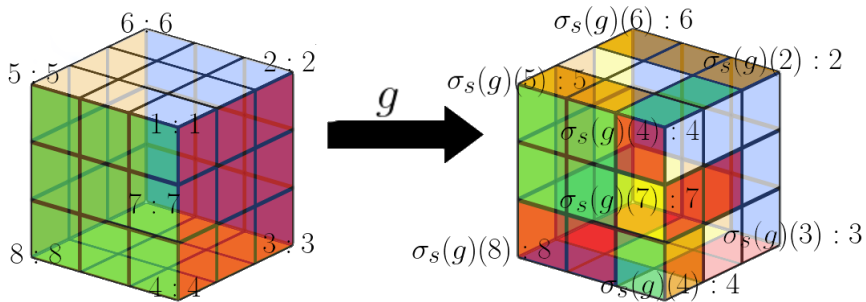


Figure: Permutation des sommets

Proposition 7 :

$\sigma_a : G_a \rightarrow S_{12}$ et $\sigma_s : G_s \rightarrow S_8$ sont deux morphismes de groupe surjectifs.

Preuve : On s'occupe ici des sommets, la preuve est similaire pour les arêtes. σ_s est bien surjective dans S_8 (car on considère les mouvement avec démontage du cube). On observe que quelque soit l'état de départ : si l'emplacement i contient le sommet a_i alors après le mouvement g l'emplacement i contient le sommet $\sigma_s(g)(a_i)$. σ_s est donc un morphisme car après le mouvement g' appliqué à l'état final, l'emplacement i contient le sommet $\sigma_s(g')(i)$, si on applique ensuite le mouvement g l'emplacement i contient alors le sommet $\sigma_s(g)(\sigma_s(g')(i))$. Finalement $\sigma_s(gg') = \sigma_s(g) \circ \sigma_s(g')$. \square

Définition 7 :

On note $R_a = \text{Ker}(\sigma_a)$ et $R_s = \text{Ker}(\sigma_s)$.

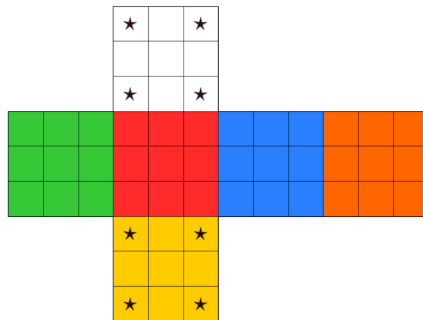
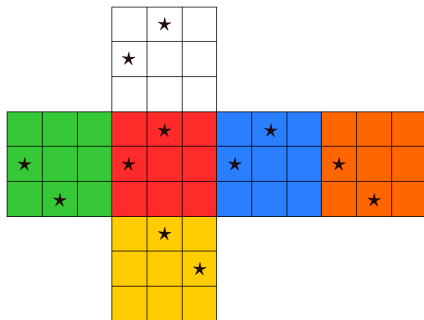
Il s'agit des sous groupes de G des mouvements de rotation des arêtes et des sommets respectivement.

Formalisons maintenant l'orientation des pièces, chaque emplacement d'arête peut contenir une même arête dans 2 orientation possibles et chaque emplacement de sommet peut contenir un même sommet dans 3 orientations possibles.

Définition 8 :

On marque une des trois faces de chaque sommet par une étoile et on dit que l'orientation d'un sommet est le nombre de tiers de tours à effectuer (dans le sens trigonométrique) pour faire coïncider sa face marquée avec l'étoile de l'état final. Ce qui permet définir pour $g \in G_s$ l'orientation des sommets comme $\rho_s(g) = (d_1, \dots, d_8) \in \mathbb{Z}_3^8$ tel que d_i soit l'orientation du sommet i en position i après le mouvement g . On définit de même ρ_a avec les arêtes.

Marquages des arêtes et des sommets



On peut représenter ces marquage en indiquant les rotations des sommets et arêtes en fonction de la place occupée par la face marquée d'une étoile :

			0							
			0		1					
			1							
	1		0		0		1			
0		1	0	1	0	1	0	1		
	0		1		1		0			
			0							
			1		0					
			1							

[illegible]

Pour $n, m \in \mathbb{N}^*$ notons $F_{n,m}$ le morphisme :

$$\left\{ \begin{array}{ll} S_n & \longrightarrow \text{Aut}(\mathbb{Z}_m^n) \\ s & \longmapsto \left((x_1, \dots, x_n) \mapsto (x_{s^{-1}(1)}, \dots, x_{s^{-1}(n)}) \right) \end{array} \right.$$

On s'intéressera en particulier à $\alpha := F_{8,3}$ et $\beta := F_{12,2}$.

Lemme 1 :

Les applications $\rho_a : G_a \rightarrow \mathbb{Z}_2^{12}$ et $\rho_s : G_s \rightarrow \mathbb{Z}_3^8$ vérifient :

$$\forall g, h \in G_s \quad \rho_s(gh) = \rho_s(g) + \alpha(\sigma_s(g))(\rho_s(h))$$

$$\forall g, h \in G_a \quad \rho_a(gh) = \rho_a(g) + \beta(\sigma_a(g))(\rho_a(h))$$

Preuve du lemme

Preuve : On traite le cas des sommets, la preuve est similaire pour les arêtes. Soient $g, h \in G_s$, notons :

$$\rho_s(h) =: (h_1, \dots, h_8) \in \mathbb{Z}_3^8$$

$$\rho_s(g) =: (g_1, \dots, g_8) \in \mathbb{Z}_3^8$$

On observe que tout mouvement de G_s peut être réalisé en positionnant d'abord les sommets puis en les orientant. Donc il existe $u, v \in G_s$ tels que $\rho_s(v) = 0$, $u \in R_s = \text{Ker}(\sigma_s)$ et $g = uv$. Comme v ne fait que permuter les sommets à orientation fixe, selon la permutation $\sigma_s(v)$, on a :

$$\rho_s(vh) = (h_{\sigma_s(v)^{-1}(1)}, \dots, h_{\sigma_s(v)^{-1}(8)}).$$

Notons $\rho_s(u) =: (u_1, \dots, u_8)$ on constate que l'orientation du sommet i après v est nulle et vaut u_i après uv donc $\rho_s(g) = \rho_s(uv) = \rho_s(u)$.

Or puisque u laisse en place tous les sommets, et que les rotations des sommets sont cycliques :

$$\rho_s(uvh) = (u_1 + h_{\sigma_s(v)^{-1}(1)}, \dots, u_8 + h_{\sigma_s(v)^{-1}(8)}) = \rho_s(u) + \alpha(\sigma_s(v))(\rho_s(h))$$

or

$$\sigma_s(g) = \sigma_s(uv) = \sigma_s(u)\sigma_s(v) = \sigma_s(v)$$

donc

$$\rho_s(gh) = \rho_s(g) + \alpha(\sigma_s(g))(\rho_s(h)) \quad \square$$

Proposition 8 :

$\rho_a : G_a \rightarrow \mathbb{Z}_2^{12}$ et $\rho_s : G_s \rightarrow \mathbb{Z}_3^8$ sont surjectives, et $P_a := \text{Ker}(\rho_a)$ et $P_s := \text{Ker}(\rho_s)$ sont des sous groupes respectivement compléments de R_a et R_s dans G_a et dans G_s .

Preuve : La surjectivité est claire puisque l'on peut orienter chaque arête et chaque sommet indépendamment.

P_a est un sous groupe de G_a :

- $id \in P_a$
- Soient $g, h \in P_a$ on a d'après le lemme 1 :
$$\begin{aligned}\rho_a(gh) &= \rho_a(g) + \alpha(\sigma_a(g))(\rho_a(h)) \\ &= 0 + \alpha(\sigma_a(g))(0) = 0 \text{ donc } gh \in P_a.\end{aligned}$$
- Soit $g \in P_a$ $0 = \rho_a(g^{-1}g) = \rho_a(g^{-1}) + \alpha(\sigma_a(g^{-1}))(\rho(g))$
d'où $\rho_a(g^{-1}) = 0$.

On démontre ensuite que P_a est complément de R_a dans G_a : Soit $g \in R_a \cap P_a$ puisque $g \in G_a$, g n'agit que sur les arêtes or $g \in R_a = \text{Ker}(\sigma_a)$ donc g laisse les positions des arêtes invariantes et $g \in P_a = \text{Ker}(\rho_a)$ donc g laisse les orientations des arêtes invariantes. On observe qu'un mouvement de G_a est entièrement déterminé par son action sur les orientations et les positions des arêtes, donc nécessairement $g = id$. Donc $R_a \cap P_a = \{id\}$. On observe de plus (comme dans le lemme 1) que tout mouvement $g \in G_a$ s'écrit comme uv , la composition d'un mouvement $v \in P_a$ agissant uniquement sur les positions par un mouvement $u \in R_a$ agissant uniquement sur les orientations. Finalement P_a est bien complément de R_a dans G_a . On traite de même le cas des sommets.

Proposition 9 :

Les applications restreintes

$$\sigma_{s|P_s} : P_s \rightarrow S_8$$

$$\rho_{s|R_s} : R_s \rightarrow \mathbb{Z}_3^8$$

$$\sigma_{a|P_a} : P_a \rightarrow S_{12}$$

$$\rho_{a|R_a} : R_a \rightarrow \mathbb{Z}_2^{12}$$

sont des isomorphismes de groupe.

Preuve : $\sigma_s|_{P_s}$ est un morphisme de groupe car c'est la restriction de σ_s au sous groupe P_s .

Injectivité : Soit $g \in \text{Ker}(\sigma_s|_{P_s})$ on a

$\text{Ker}(\sigma_s|_{P_s}) = \text{Ker}(\sigma_s) \cap P_s = R_s \cap P_s$ Or d'après la proposition 8 P_s est complément de R_s , donc $g = id$.

Surjectivité : Soit $\gamma \in S_8$, σ_s est surjective dans S_8 d'après la proposition 7, donc il existe $g \in G_s$ tel que $\sigma_s(g) = \gamma$. Or puisque P_s est complément de R_s dans G_s , $\exists u \in R_s, v \in P_s$ tel que $g = uv$. Alors :

$$\sigma_s|_{P_s}(v) = id \circ \sigma_s(v) = \sigma_s(u) \circ \sigma_s(v) = \sigma_s(uv) = \gamma.$$

$\sigma_s|_{P_s}$ est bien un isomorphisme.

Montrons maintenant que $\rho_s|_{R_s}$ est un isomorphisme : Soient $g, h \in R_s$,

$$\rho_s(gh) = \rho_s(g) + \alpha(\sigma_s(g))(\rho_s(h)) = \rho_s(g) + \alpha(id)(\rho_s(h)) = \rho_s(r) + \rho_s(g).$$

$\rho_s|_{P_s}$ est bien un morphisme.

Injectivité : Soit $g \in \text{Ker}(\rho_s|_{R_s})$ on a

$$\text{Ker}(\rho_s|_{R_s}) = \text{Ker}(\rho_s) \cap R_s = P_s \cap R_s = \{id\} \text{ donc } g = id.$$

Surjectivité : Soit $c \in \mathbb{Z}_3^8$, la surjectivité de ρ_s donne l'existence de $g \in G_s$ tel que $\rho_s(g) = c$. On décompose à nouveau g : $\exists u \in R_s, v \in P_s$ tel que $g = uv$. Puis $\rho_s|_{P_s}(u) = \rho_s(u) + 0 = \rho_s(u) + \rho_s(v) = \rho_s(uv) = c$. On traite de même le cas des arêtes. \square

Théorème 1 :

On a :

$$G \cong (\mathbb{Z}_3^8 \rtimes_{\alpha} S_8) \times (\mathbb{Z}_2^{12} \rtimes_{\beta} S_{12})$$

.

Preuve : Montrons que $G_s \cong \mathbb{Z}_3^8 \rtimes_{\alpha} S_8$.

D'après la proposition 8, P_s est un complément de R_s dans G_s , de plus R_s est normal dans G_s car c'est le noyau de σ_s qui est un morphisme partant de G_s . Donc d'après la proposition 2, $G_s \cong R_s \rtimes P_s$. De plus, si on note $f : k \mapsto f_k$ le morphisme de conjugaison de R_s par P_s , alors d'après la proposition 4, $G_s \cong R_s \rtimes_f P_s$, or d'après la proposition 9 $R_s \cong \mathbb{Z}_3^8$ et $P_s \cong S_8$, on note φ et ψ les isomorphismes respectifs $\rho_s|_{R_s}$ et $\sigma_s|_{P_s}$ ainsi que $\tilde{f} : s \mapsto \varphi \circ f_{\psi^{-1}(s)} \circ \varphi^{-1}$. On a alors d'après la proposition 5, $G_s \cong \mathbb{Z}_3^8 \rtimes_{\tilde{f}} S_8$.

Il ne reste qu'à vérifier que $\tilde{f} = \alpha$. En effet, soient $s \in S_8, h \in \mathbb{Z}_3^8$, on a avec le lemme 1 :

$$\begin{aligned}
 \tilde{f}(s)(h) &= \varphi(\psi^{-1}(s)\varphi^{-1}(h)\psi^{-1}(s)^{-1}) \\
 &= \varphi(\psi^{-1}(s)\varphi^{-1}(h)\psi^{-1}(s^{-1})) \\
 &= \varphi(\psi^{-1}(s)\varphi^{-1}(h)) + \alpha(\psi(\psi^{-1}(s)\varphi^{-1}(h)))(\varphi(\psi^{-1}(s^{-1}))) \\
 &= \varphi(\psi^{-1}(s)\varphi^{-1}(h)) + \alpha(\varphi^{-1}(h))(0) \\
 &= \varphi(\psi^{-1}(s)\varphi^{-1}(h)) \\
 &= \varphi(\psi^{-1}(s)) + \alpha(\psi(\psi^{-1}(s)))(h) \\
 &= \alpha(s)(h)
 \end{aligned}$$

On procède de même pour montrer que $G_a \cong \mathbb{Z}_2^{12} \rtimes_{\beta} S_{12}$. D'après la proposition 6, il en découle que

$$G \cong (\mathbb{Z}_3^8 \rtimes_{\alpha} S_8) \times (\mathbb{Z}_2^{12} \rtimes_{\beta} S_{12}).$$