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

Armand Perrin

June 6, 2024

Part I
Produits semi-direct

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 $\varphi : \begin{cases} H \times K & \to & G \\ (h,k) & \mapsto & hk \end{cases}$ 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 :

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

On le note $H \triangleleft G$.
Remarque : On peut montrer facilement que le noyeau d'un morphisme de groupe est un sous groupe normal.

Produit semi-direct interne

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 $\cdot : \begin{cases} (H \times K)^2 & \to & H \times K \\ (h,k),(h',k') & \mapsto & (hkh'k^{-1}, kk') \end{cases}$
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 $\varphi : \begin{cases} H \rtimes K & \to & G \\ (h,k) & \mapsto & hk \end{cases}$ est un isomorphisme de groupes. On écrira $G \cong H \rtimes K$ pour signifier qu'ils sont isomorphes.

Produit semi-direct externe

Dans cette partie on considère H et K deux groupes quelconques et $f : K \to \mathrm{Aut}(H), k \mapsto f_k$ un morphisme de K dans $\mathrm{Aut}(H)$, le groupe des automorphismes de H. On va chercher à construire un groupe G a l'aide de f, tel que l'on puisse identifier H et K à des sous-groupes H_G et K_G de G vérifiant $G \cong H_G \rtimes K_G$.

Définition 4 : (Loi du produit semi-direct externe) On défini la loi de composition interne $\cdot_f$ sur $H \times K$ par $\cdot_f : \begin{cases} (H \times K)^2 & \to & H \times K \\ (h,k),(h',k') & \mapsto & (hf_k(h'), kk') \end{cases}$ on appelle produit semi-direct externe relatif à f et on note $H \rtimes_f K$ le couple $(H \times K, \cdot_f)$.

Proposition 3 : Comme annoncé plus haut, $G := H \rtimes_f K$ 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 $f : \begin{cases} K & \to & \mathrm{Aut}(H) \\ k & \mapsto & \left(h \mapsto khk^{-1}\right) \end{cases}$
Alors f est un morphisme de groupes et $G \cong H \rtimes_f K$.
f est appelé "morphisme de conjuguaison 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 :

$$\varphi : H \to H'$$
$$\psi : K \to K'$$

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

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

Alors $\tilde{f}$ est un morphisme et

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

Part II
Le Groupe du Rubik's cube

Notations:
- S_n est le groupe symétrique d'ordre n
- C_n le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$
- "$A \cong B$" signifie que les groupes A et B sont isomorphes.
- 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).

Decrivons G : chaque mouvement correspond exactement à un état du cube (l' état dans lequel se trouve le cube après application de ce mouvement depuis l'état final) et chaque état du cube est déterminé par les positions et rotations de chaque pièce. 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 et les sommets. Les centres sont toujours fixes (une rotation de l'espace n'est pas un mouvement).

On observe premièrement que tout mouvement est constitué d'un mouvement sur les arêtes et d'un mouvement sur les sommets. Formellement, tout mouvement $g \in G$ s'écrit de manière unique : $g = g_a g_s$, où g_a est un élément du sous groupe G_a de G constitué des éléments laissant fixes tous les sommets et g_s un élément du sous groupe G_s constitué des éléments de G laissant fixes toutes les arêtes. De plus, il est facile de voir que $g_a g_s = g_s g_a$. On en déduit la proposition suivante :

Proposition 6 : $G \cong G_a \times G_s$.

Preuve : On montre que l'application : $\varphi : \left\{ \begin{array}{ccc} G_a \times G_s & \longrightarrow & G \\ (g_a, g_s) & \longmapsto & g_a g_s \end{array} \right.$ est un isomorphime 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 :

$$\forall((g_a, g_s), (g'_a, g'_s)) \in (G_a \times G_s)^2 \quad \varphi((g_a, g_s)(g'_a, g'_s)) = \varphi((g_a g'_a, g_s g'_s)) = g_a g'_a g_s g'_s$$
$$= (g_a g_s)(g'_a g'_s) = \varphi(g_a, g_s)\varphi(g_a, g'_s) \ \square$$

Il y a 12 arêtes qui peuvent toutes prendre chaqune un des 12 emplacements d'arête et 8 sommets qui peuvent tous prendre un des 8 emplacements de sommet. Toutes les pièces étant 2 à 2 distinctes, les états du cube correspondants sont également distincts.

Proposition 7 : On dispose donc de deux morphismes de groupe surjectifs $\sigma_a : G_a \to S_{12}$ et $\sigma_s : G_s \to S_8$ représentants respectivement les positions des arêtes et des sommets.

Preuve : On s'occupe ici des sommets, la preuve est similaire pour les arêtes. On numérote de 1 à 8 les emplacements de sommets ainsi que les sommets, de telle sorte que dans l'état final, pour $i = 1, \ldots, 8$ le sommet i soit en position i. On pose alors $\sigma_s : g \mapsto s_g$ où $s_g \in S_8$ est l'unique permutation telle que pour $i = 1, \ldots, 8$ le sommet $s_g(i)$ soit en position i apres le mouvement g appliqué depuis l'état final. On observe que cela ne dépend pas de l'état de départ : si l'emplacement i contient le sommet a_i alors apres le mouvement g l'emplacement i contient le sommet $s_g(a_i)$. σ_s est bien surjective dans S_8 (car on considère les mouvement avec démontage du cube) et c'est un morphisme car après le mouvement g' appliqué à l'état final, l'emplacement i contient le sommet $s_{g'}(i)$, si on applique ensuite le mouvement g l'emplacement i contient alors le sommet $s_g(s_{g'}(i))$. Finalement $s_{gg'} = s_g \circ s_{g'}$.□

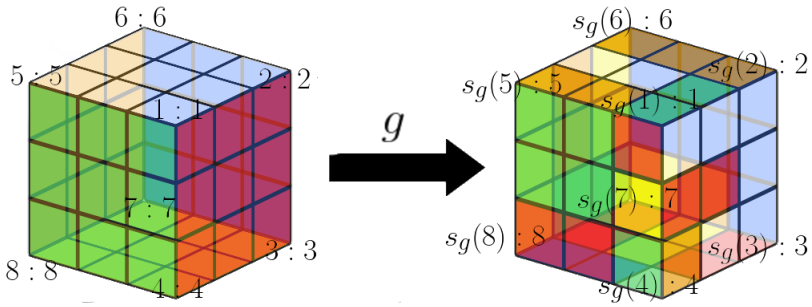


Figure 1: Permutation des sommets

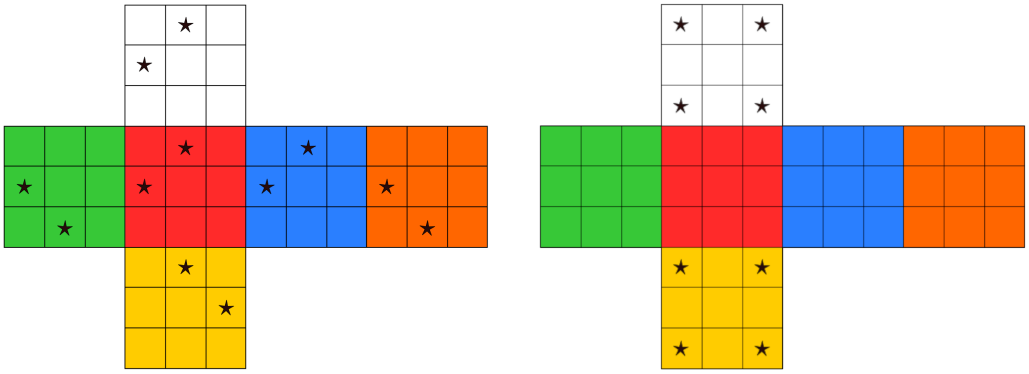
Notons $R_a = Ker(\sigma_a)$ et $R_s = Ker(\sigma_s)$. Il s'agit des sous groupes de G des mouvements de rotation des arêtes et des sommets respectivement.

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.

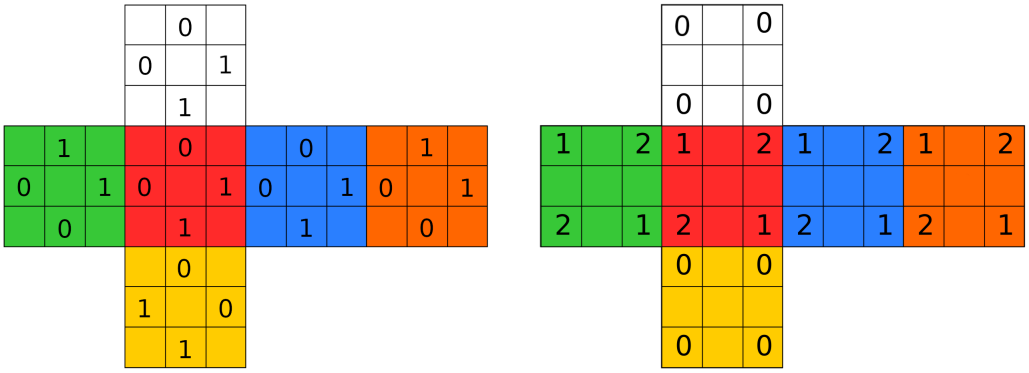
Définition 5 : Soit $g \in G_a$ Pour les arêtes, marquons d'une étoile l'une des deux faces de chaque arête, que l'on choisis arbitrairement. On dit qu'une arête à pour orientation 0 si après le mouvement g, sa face marquée coincide avec celle de l'arête qui se trouve à sa place dans l'état final et 1 sinon. L'orientation est donc un élément de C_2. Et l'orientation de toutes les arêtes un élément de C_2^{12} que l'on note $\rho_a(g) = (c_1, \ldots, c_{12})$ tel que c_i soit l'orientation de l'arête qui se trouve en position i après le mouvement g.

On procède de même pour les sommets : on marque cette fois ci 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 coincider sa face marquée avec l'étoile de l'état final. Ce qui permet définir pour $g \in G_s$ l'orientation des sommets comme $\rho_s(g) = (d_1, \ldots, d_8) \in C_3^8$ tel que d_i soit l'orientation du sommet i en position i après le mouvement g.

Figure 2: 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 :



Pour $n, m \in \mathbb{N}^*$ notons $F_{n,m}$ le morphisme : $\left\{ \begin{array}{ccc} S_n & \longrightarrow & \mathrm{Aut}(C_m^n) \\ s & \longmapsto & \Big((x_1, \ldots, x_n) \mapsto (x_{s^{-1}(1)}, \ldots, x_{s^{-1}(n)}) \Big) \end{array} \right.$

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

Lemme 1 : Les applications $\rho_a : G_a \to C_2^{12}$ et $\rho_s : G_s \to C_3^8$ 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 : On traite le cas des sommets, la preuve est similaire pour les arêtes. Soient $g, h \in G_s$, notons :

$$\rho_s(h) =: (h_1, \ldots, h_8) \in C_3^8$$

$$\rho_s(g) =: (g_1, \ldots, g_8) \in C_3^8$$

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

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

Notons $\rho_s(u) =: (u_1, \ldots, u_8)$ 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 :

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

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 : $\rho_a : G_a \to C_2^{12}$ et $\rho_s : G_s \to C_3^8$ sont surjectives, et $P_a := Ker(\rho_a)$ et $P_s := Ker(\rho_s)$ 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 :
  $\rho_a(gh) = \rho_a(g) + \alpha(\sigma_a(g))(\rho_a(h))$
  $= 0 + \alpha(\sigma_a(g))(0) = 0$ donc $gh \in P_a$.
- 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 $g \in R_a = Ker(\sigma_a)$ donc g

laisse les positions des arêtes invariantes et $g \in P_a = Ker(\rho_a)$ donc g laisse les orientations des arêtes invariantes. On observe qu'un mouvement de G_a est entierement 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

$$\sigma_{s|P_s} : P_s \to S_8$$
$$\rho_{s|R_s} : R_s \to C_3^8$$
$$\sigma_{a|P_a} : P_a \to S_{12}$$
$$\rho_{a|R_a} : R_a \to C_2^{12}$$

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 $g \in Ker(\sigma_{s|P_s})$ on a $Ker(\sigma_{s|P_s}) = Ker(\sigma_s) \cap P_s = R_s \cap P_s$ Or d'après la propostition 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 $g \in Ker(\rho_{s|R_s})$ on a $Ker(\rho_{s|R_s}) = Ker(\rho_s) \cap R_s = P_s \cap R_s = \{id\}$ donc $g = id$.
Surjectivité : Soit $c \in C_3^8$, 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.

Théorème 1 : On a :

$$G \cong (C_3^8 \rtimes_\alpha S_8) \times (C_2^{12} \rtimes_\beta S_{12})$$

.

Preuve : Montrons que $G_s \cong C_3^8 \rtimes_\alpha S_8$.
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 noyeau 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 conjuguaison 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 $R_s \cong C_3^8$ 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, $G_s \cong C_3^8 \rtimes_{\tilde{f}} S_8$.

Il ne reste qu'a vérifier que $\tilde{f} = \alpha$. En effet, soient $s \in S_8, h \in C_3^8$, 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 $G_a \cong C_2^{12} \rtimes_\beta S_{12}$. D'après la proposition 6, il en découle que

$$G \cong (C_3^8 \rtimes_\alpha S_8) \times (C_2^{12} \rtimes_\beta S_{12}).$$