

Groupe du Rubik's Cube

Cet article présente un modèle mathématique du **groupe** du **Rubik's Cube**.

Sommaire

Notations utilisées

Décomposition des mouvements du cube

Isomorphisme entre H et ""`UNIQ--postMath-00000019-QINU`""

Factorisation sommets-arêtes

Permutation des arêtes et des sommets

Orientation des arêtes et des sommets

Théorème fondamental : caractérisation des mouvements légaux

Démonstration de la partie directe

Démonstration de la réciproque

Calcul du cardinal du groupe des mouvements du Rubik's Cube

Générateurs et relations

Propriétés particulières

Présentation du problème

Première application : nombre minimum de mouvements

Générateurs et relations : présentation d'un groupe

Produit semi-direct

Recherche d'une présentation de ""`UNIQ--postMath-00000093-QINU`""

Liens externes

Bibliographie

Notes et références

Notations utilisées

- G est le groupe des mouvements légaux (sans démonter le cube !).
- H est le groupe élargi (ici on peut démonter le cube pour disposer ses éléments comme on le souhaite).
- $C_n = \mathbb{Z}/n\mathbb{Z}$ est l'ensemble des classes d'équivalence pour la congruence modulo n . Il est isomorphe au groupe des n -èmes de tour d'axe donné. On utilisera en particulier C_3 pour pivoter un coin du cube, et C_2 pour pivoter une arête. On note $C_k^n = (C_k)^n$ à savoir $\underbrace{C_k \times C_k \times \dots \times C_k}_{n \text{ fois}}$.
- \mathfrak{S}_n est le groupe symétrique d'ordre n . Ses éléments sont les permutations de n objets. Parmi ces permutations, celle de deux objets s'appelle transposition. On utilisera en

particulier \mathfrak{S}_8 pour permuter les coins du cube, et \mathfrak{S}_{12} pour permuter ses arêtes. La composition des permutations se lit de droite à gauche.

- ε désigne la signature d'une permutation de \mathfrak{S}_n .
- Pour toute permutation s élément de \mathfrak{S}_n , on note $P(s)$ l'automorphisme défini par :

$$P(s) : C_k^n \rightarrow C_k^n$$

$$(x_1, x_2, \dots, x_n) \mapsto (x_{s^{-1}(1)}, x_{s^{-1}(2)}, \dots, x_{s^{-1}(n)})$$

$$(x_1, x_2, \dots, x_n).$$
 s étant une bijection, on remarque que la somme des composantes est invariante : $\sum_{i=1}^n x_i = \sum_{i=1}^n x_{s^{-1}(i)}$. P est un morphisme du groupe \mathfrak{S}_n dans le groupe des automorphismes de C_k^n .
- \rtimes est le symbole d'un produit semi-direct interne, et \rtimes_P celui d'un produit semi-direct externe induit par P .
- Les rotations d'un quart de tour, dans le sens des aiguilles d'une montre (sens direct par rapport à un axe entrant dans le cube), sont appelées R, U, L, F, B, D pour les faces droite (right), haut (up), gauche (left), avant (front), arrière (back) et bas (down)^{1,2}.
- On identifie les sommets par 3 coordonnées et les arêtes par 2 ; par exemple FUL est le sommet de face en haut à gauche et BR est l'arête arrière droite¹.

Décomposition des mouvements du cube

Isomorphisme entre H et $(C_3^8 \rtimes_P \mathfrak{S}_8) \times (C_2^{12} \rtimes_P \mathfrak{S}_{12})$

Factorisation sommets-arêtes

Un élément de H se décompose naturellement entre son action sur les coins et son action sur les arêtes, ces deux actions étant indépendantes. On introduit les deux sous-groupes H_{co} et H_{ar} constitués respectivement des mouvements agissant sur les coins et laissant invariante chaque arête, et des mouvements agissant sur les arêtes et laissant invariant chaque coin. H est isomorphe au produit direct des groupes $H_{\text{co}} \times H_{\text{ar}}$ ³.

On va maintenant montrer que H_{co} est isomorphe au produit semi-direct $C_3^8 \rtimes_P \mathfrak{S}_8$ et H_{ar} au produit semi-direct $C_2^{12} \rtimes_P \mathfrak{S}_{12}$.

L'isomorphisme entre H_{co} et $C_3^8 \rtimes_P \mathfrak{S}_8$ exprime le fait qu'une action sur les coins se décompose en une permutation des 8 coins (élément de \mathfrak{S}_8), et pour chaque coin, d'une rotation possible de 0, 1 ou 2 tiers de tour (pour chaque coin, le groupe de ces rotations est isomorphe à C_3)⁴.

De même, l'isomorphisme entre H_{ar} et $C_2^{12} \rtimes_P \mathfrak{S}_{12}$ exprime le fait qu'une action sur les arêtes se décompose en une permutation des 12 arêtes, et pour chaque arête, d'une rotation possible de 0 ou 1 demi-tour.

Permutation des arêtes et des sommets

On numérote les sommets du Rubik's cube de 1 à 8 dans cet ordre : FUR, BUR, BUL, FUL, FDR, BDR, BDL, FDL. Les arêtes vont de 1 à 12 : UL, BL, DL, FL, FU, BU, BD, FD, UR, BR, DR, FR.

On définit alors deux morphismes surjectifs de groupes $\rho : H_{\text{co}} \rightarrow \mathfrak{S}_8$ et $\sigma : H_{\text{ar}} \rightarrow \mathfrak{S}_{12}$ qui extraient d'un élément de H les permutations des sommets et des arêtes correspondantes sans tenir compte de leur

à un élément de H les permutations des sommets et des arêtes correspondantes, sans tenir compte de leur orientation³.

Par exemple, en utilisant la notation des cycles, on a $\rho(F) = (1, 5, 8, 4)$ et $\rho(U) = (4, 3, 2, 1)$, d'où $\rho(U \circ F) = (1, 5, 8, 3, 2)$.

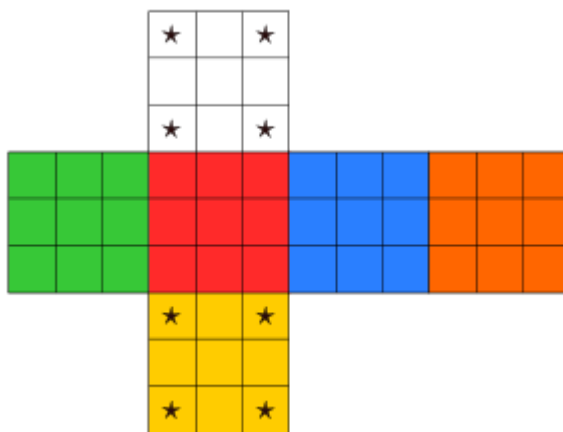
Orientation des arêtes et des sommets

Posons $\mathbf{Rot}_{co} = \ker(\rho)$ et $\mathbf{Rot}_{ar} = \ker(\sigma)$. Ce sont deux sous-groupes distingués de H . Leurs éléments sont les rotations des coins (identité ou tiers de tour, dans un sens ou dans l'autre) et des arêtes (identité ou demi-tour). Seule l'orientation des cubes change, pas leur position. Ces deux groupes vont permettre de décomposer H_{co} et H_{ar} en les produits semi-directs annoncés.

Changer un cube de position (par exemple mettre FUL en FUR) est une opération ambiguë : dans la position d'arrivée, il y a 3 orientations possibles pour les coins, 2 pour les arêtes. Parmi tous ces mouvements possibles, on en choisit formant deux sous-groupes, Perm_{co} et Perm_{ar} , complémentaires de \mathbf{Rot}_{co} et \mathbf{Rot}_{ar} .

Perm_{co} est le groupe des mouvements des coins à orientation constante, isomorphe à \mathfrak{S}_8 . En identifiant Perm_{co} à \mathfrak{S}_8 , on peut voir ρ comme un morphisme de H dans Perm_{co} . Pour tout g de H_{co} , $g\rho(g)^{-1}$ est alors un élément de H qui laisse en place chaque coin, mais en les pivotant sur place. C'est donc un élément $v(g)$ de \mathbf{Rot}_{co} . On a donc la décomposition $g = v(g)\rho(g)$. Cette décomposition est unique du fait que $\mathbf{Rot}_{co} \cap \text{Perm}_{co} = \{\text{Id}\}$. $\rho(g)$ indique où les coins sont déplacés, et $v(g)$ comment ils sont pivotés. La rotation de chaque sommet est donnée par un élément de C_3 indiquant de combien de tiers de tour le sommet est pivoté, de sorte que \mathbf{Rot}_{co} est isomorphe à C_3^8 . On peut représenter $v(g)$ par un élément $(v_j)_{1 \leq j \leq 8}$ de C_3^8 , la j -ème composante indiquant la rotation que subira le sommet qui arrivera en j par le déplacement dû à g .

On peut dessiner le choix de Perm_{co} en plaçant un marqueur ★ sur chaque coin du Rubik's cube. Un mouvement d'orientation constante est celui qui amène la face marquée de la position de départ sur la face marquée de la position d'arrivée⁴. On peut prendre par exemple le marquage suivant :



pour lequel un mouvement élément de Perm_{co} laisse la réunion des faces blanc-jaune globalement invariante. On note ci-dessous par les valeurs 0, 1 ou 2 la valeur à attribuer à la rotation d'un coin en fonction de la place qu'occuperait sa face marquée par une étoile :

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | 0 | | | 0 | | | | |
| | | | | U | | | | | | |
| | | | 0 | | | 0 | | | | |
| 1 | | 2 | 1 | | 2 | 1 | | 2 | 1 | 2 |
| | L | | | F | | | R | | | B |
| 2 | | 1 | 2 | | 1 | 2 | | 1 | 2 | 1 |
| | | | 0 | | 0 | | | | | |
| | | | | D | | | | | | |
| | | | 0 | | 0 | | | | | |

Si g et h sont éléments de H_{co} avec :

$$\begin{aligned} g &= v(g) \circ \rho(g) \\ h &= v(h) \circ \rho(h) \end{aligned}$$

alors, on a :

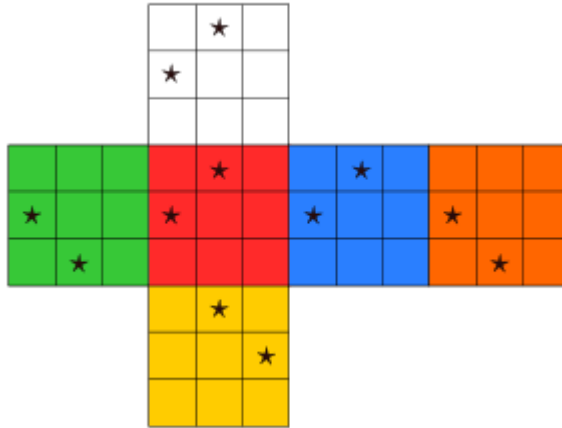
$$hg = v(h)\rho(h)v(g)\rho(g) = v(h)\rho(h)v(g)\rho(h)^{-1}\rho(h)\rho(g)$$

$\rho(h)\rho(g) = \rho(hg)$ est élément de \mathbf{Perm}_{co} et $v(h)\rho(h)v(g)\rho(h)^{-1} = v(hg)$ est élément de \mathbf{Rot}_{co} . On n'a pas en général $v(hg) = v(h)v(g)$; v n'est donc pas un morphisme de groupe, ce qui empêche d'avoir un produit direct entre \mathbf{Rot}_{co} et \mathbf{Perm}_{co} . Mais la relation $v(hg) = v(h)\rho(h)v(g)\rho(h)^{-1}$ est caractéristique d'un produit semi-direct. Ainsi, $H_{co} = \mathbf{Rot}_{co} \rtimes \mathbf{Perm}_{co}$.

Si $v(g)$ a pour composantes $(v_j)_{1 \leq j \leq 8}$, alors $\rho(h)v(g)\rho(h)^{-1}$ a pour composantes $(v_{\rho(h)^{-1}(j)})_{1 \leq j \leq 8} = P(\rho(h))((v_j)_{1 \leq j \leq 8})$. Le remplacement de \mathbf{Rot}_{co} par son groupe isomorphe C_3^8 transfère le produit semi-direct interne $\mathbf{Rot}_{co} \rtimes \mathbf{Perm}_{co}$ en le produit semi-direct externe $C_3^8 \rtimes_P \mathfrak{S}_8$.

On remarque par ailleurs que la somme des composantes de $v(g)$ est égale à celle de $\rho(h)v(g)\rho(h)^{-1}$. Il en résulte que la somme des composantes de $v(hg)$ est égale à la somme de celles de $v(h)$ et de celles de $v(g)$. Ainsi, v n'est pas un morphisme, mais la somme des composantes (appelée rotation totale des coins) en est un, à valeurs dans C_3^4 .

On opère de même sur les arêtes en choisissant un marquage privilégié de chacune d'elles, ce qui permet de définir leur orientation $w : H \rightarrow C_2^{12}$ par le nombre de rotations de 180° permettant de rétablir l'orientation initiale. On peut prendre par exemple :



Comme pour v , w n'est pas un morphisme de groupe, et on a seulement une structure de produit semi-direct $H_{\text{ar}} = \text{Rot}_{\text{ar}} \rtimes \text{Perm}_{\text{ar}} \simeq C_2^{12} \rtimes_P \mathfrak{S}_{12}$, mais la somme de des composantes de w (appelée rotation totale des arêtes) est un morphisme, à valeurs dans C_2 .

Théorème fondamental : caractérisation des mouvements légaux

On rappelle que H est le groupe des actions sur le cube de Rubik démontable, et G le groupe des actions sur le cube non démontable (en effectuant des mouvements des faces selon les règles). Pour tout g élément de H , soit $vrws$ la décomposition de g en le produit d'un élément v de C_3^8 (pivotements des coins), r élément de \mathfrak{S}_8 (permutation des coins), w élément de C_2^{12} (pivotements des arêtes), s élément de \mathfrak{S}_{12} (permutation des arêtes). Alors^{5,6} :

$$g \in G \iff \begin{cases} a) & \varepsilon(r)\varepsilon(s) = 1 \\ b) & \sum_{i=1}^8 v_i \equiv 0 \pmod{3} \\ c) & \sum_{i=1}^{12} w_i \equiv 0 \pmod{2} \end{cases}$$

Autrement dit, G est le noyau du morphisme Φ de H dans $\{\pm 1\} \times C_3 \times C_2$, qui, à tout g de H associe le triplet $\Phi(g) = (\varepsilon(r)\varepsilon(s), \sum_{i=1}^8 v_i, \sum_{i=1}^{12} w_i)$.

Le a) exprime par exemple que, selon les règles du jeu, il est impossible de transposer seulement deux sommets, ou bien seulement deux arêtes. Selon le b), il est impossible de pivoter un coin seul. Deux coins seuls peuvent être pivotés mais en sens inverse l'un de l'autre. Il dit aussi que l'orientation d'un coin est défini de manière unique par l'orientation des 7 autres coins. Le c) exprime qu'il est impossible de pivoter une arête seule. Le pivotement des arêtes s'opère nécessairement par paire. L'orientation d'une arête est définie de manière unique par l'orientation des 11 autres.

Le sens direct de la démonstration consiste à montrer que tout mouvement selon les règles vérifient ces conditions. Le sens réciproque consiste à prouver que, si on se donne une configuration du Rubik's cube vérifiant ces conditions, alors il existe une suite de mouvements selon les règles qui conduit à cette configuration (ou inversement, qui fait passer de cette configuration à la configuration initiale). C'est la description d'un algorithme de résolution du Rubik's cube⁷.

Démonstration de la partie directe

Il s'agit de montrer que G est inclus dans $\ker(\Phi)$. Pour cela, Φ étant un morphisme, il suffit de le prouver pour un système générateur de G , à savoir les six rotations de chacune des faces⁷.

En ce qui concerne $\varepsilon(\rho(g))\varepsilon(\sigma(g))$, une rotation d'une face est constitué d'un 4-cycle sur les coins et d'un 4-cycle sur les arêtes. Chaque cycle a pour signature -1 et leur produit fait bien 1.

En ce qui concerne $\sum_{i=1}^8 v_i \bmod 3$, observons comment chaque rotation de face fait pivoter chacun des coins, (en utilisant le codage 0, 1 et 2 des trois faces de chaque coin donné dans le paragraphe précédent) :

| g | $v(g)$ |
|-----|-------------------|
| F | (2,0,0,1,1,0,0,2) |
| U | (0,0,0,0,0,0,0,0) |
| D | (0,0,0,0,0,0,0,0) |
| B | (0,1,2,0,0,2,1,0) |
| R | (1,2,0,0,2,1,0,0) |
| L | (0,0,1,2,0,0,2,1) |

On constate bien que, pour chaque face, la somme des composantes de $v(g)$ est nulle modulo 3.

On peut opérer une vérification analogue sur les arêtes pour montrer que $\sum_{i=1}^{12} w_i$ est nulle modulo 2. Mais il

est plus rapide de remarquer que la rotation d'une face induit sur les $2 \times 12 = 24$ facettes carrées des 12 arêtes une permutation qui est le produit de deux 4-cycles (l'un des 4-cycles permute circulairement 4 facettes, l'autre 4-cycle permute circulairement 4 autres facettes, adjacentes aux 4 premières). Il en résulte que la signature de la permutation des 24 facettes vaut 1, et qu'il en est de même par composition pour un mouvement quelconque du Rubik's cube. Or cette signature n'est autre que $(-1)^{\sum w_i}$. Il en résulte que

$\sum_{i=1}^{12} w_i$ est nulle modulo 2⁷.

Démonstration de la réciproque

Il s'agit de montrer que $\ker(\Phi)$ est inclus dans G . Pour cela, partant d'une configuration g appartenant à $\ker(\Phi)$, on lui applique une suite S de rotations des faces appartenant à G de façon que $S \circ g = \text{Id}$. Cela prouve que g est le symétrique de S , donc est élément de G ⁸.

Les mouvements des faces à effectuer seront donnés ici par une suite de lettres : majuscules F, R, L, B, U, D pour une rotation dans le sens des aiguilles d'une montre, minuscules f, r, l, b, u, d pour le sens inverse. La composition des mouvements se fera dans ce paragraphe dans le sens de la lecture du mot ainsi formé, i.e. de gauche à droite. Ainsi, le mouvement "FUL" est constitué d'une rotation dans le sens des aiguilles d'une montre de la face F, suivie de la face U, et on termine par une rotation en sens inverse de la face L. La suite S est construite en mettant d'abord en place les arêtes, puis les coins, puis en pivotant convenablement les arêtes, puis les coins.

Mise en place des arêtes : pour tout couple d'arêtes, il existe un élément de G qui transpose ces deux arêtes, en laissant les autres arêtes en place (à pivotement près)⁸. Par exemple "uFUU.uUf" transpose deux

arêtes, en faisant des arêtes arêtes en place (à pivotement près). Par exemple, la permutation des arêtes de la face U⁹. Comme les transpositions engendrent le groupe symétrique, cela prouve qu'il existe un élément de G qui dispose les arêtes à leur place.

Mise en place des coins : Compte tenu de la condition de parité a) sur la signature des permutations des arêtes et des coins, si les arêtes sont en place, cela signifie que les coins sont permutés par une permutation paire. Or ces permutations sont engendrées par les 3-cycles (permutation circulaire de trois coins). Pour mettre les coins en place par un mouvement élément de G , il suffit donc de montrer que, pour tout triplet de coins, il existe un élément de G qui permute ces trois coins tout en laissant les autres coins et les arêtes à leur place. C'est effectivement le cas. Par exemple, le mouvement "LurUluRU" permute trois coins de la face U tout en laissant tous les autres cubes à leur place, sans modifier aucun autre cube¹⁰.

Pivotement des arêtes : Compte tenu de la condition c) sur le pivotement des arêtes, on peut pivoter convenablement les arêtes en opérant successivement sur deux arêtes à la fois. Pour tout couple d'arêtes, il existe un élément de G qui se borne à pivoter deux arêtes⁸. Par exemple, le mouvement "BddbdbBDBddflbLF" pivote deux arêtes adjacentes de la face D sans modifier aucun autre cube¹¹.

Pivotement des coins : Compte tenu de la condition b) sur le pivotement des coins, on peut pivoter convenablement les coins en opérant successivement sur deux coins à la fois, les rotations étant de sens opposé sur ces deux coins. Pour tout couple de coins, il existe un élément de G satisfaisant ces conditions¹². Par exemple, le mouvement "uBULBIFLbUf" pivote en sens inverse deux coins de la face U¹³.

Une fois ces opérations terminées, le cube est remis en place et on a prouvé que la configuration initiale g est bien élément de G .

Calcul du cardinal du groupe des mouvements du Rubik's Cube

On rappelle qu'on a introduit un morphisme Φ de H dans $\{\pm 1\} \times C_3 \times C_2$, qui, à une configuration g du cube démontable associe le triplet constitué du produit des signatures des permutations sur les coins et les arêtes, la rotation totale des coins et la rotation totale des arêtes. Le noyau de Φ est le groupe G des mouvements du Rubik's cube.

Ce morphisme est surjectif car, pour tout élément de $\{\pm 1\} \times C_3 \times C_2$, on peut trouver une configuration g de H antécédent par Φ de cet élément. Il suffit pour cela de pivoter un coin et une arête de façon adéquate et éventuellement de permuter deux coins (on rappelle que, dans H , tous les mouvements sont possibles). Comme $\{\pm 1\} \times C_3 \times C_2$ est de cardinal 12, il en résulte que G est un sous-groupe de H d'indice 12, les classes de G étant les gG avec g parcourant dans H un sous-ensemble de 12 représentants d'antécédents par Φ des 12 éléments de $\{\pm 1\} \times C_3 \times C_2$.

Par conséquent, le cardinal de G est le douzième de celui de H ³. (C'est une variante du théorème de Lagrange ou de la formule des indices). Or le cardinal de H est $|H| = 8! \times 3^8 \times 12! \times 2^{12}$ (produit du nombre de permutations des coins par le nombre de pivotement des coins par le nombre des permutations des arêtes par le nombre de pivotement des arêtes), donc celui de G est :

$$|G| = \frac{|H|}{12} = 2^{27} \times 3^{14} \times 5^3 \times 7^2 \times 11 = 43\,252\,003\,274\,489\,856\,000 \approx 43 \times 10^{18}$$

soit environ 43 milliards de milliards de combinaisons.

On peut aussi dire qu'il y a 2^{11} pivotements d'arêtes possibles (l'orientation de la dernière arête étant alors imposée par la condition c)), 3^7 pivotements de coins possibles (l'orientation du dernier coin étant imposé par la condition b)), $8!$ placements possibles des huit sommets, mais seulement $\frac{12!}{2}$ placements possibles des douze arêtes en raison de la condition de parité donnée par la condition a). Le total $2^{11} \times 3^7 \times 8! \times \frac{12!}{2}$ redonne le résultat précédent^{14,15}.

Générateurs et relations

Propriétés particulières

Comme précédemment, on donne les mouvements des faces à effectuer par une suite de lettres, la composition s'effectuant ici de gauche à droite : majuscules F, R, L, B, U, D pour une rotation dans le sens des aiguilles d'une montre, minuscules f, r, l, b, u, d pour le sens inverse.

- On peut engendrer le groupe G en autorisant seulement les rotations de cinq faces données. En effet, le mouvement "rLffbbRldrLffbbR", dû à David Benson, permet de tourner la face supérieure en utilisant uniquement les autres faces¹⁶.
- L'ordre maximal d'un élément de G est 1260. Il est obtenu par exemple par le mouvement "rbbDuD"¹⁷.
- Le groupe G peut être engendré par deux mouvements seulement, par exemple "lbrDL" et "ufruRUF"¹⁸.

Présentation du problème

D'après les notations utilisées pour étudier le Cube, le problème peut se présenter sous deux formes. On peut le traiter en utilisant des notations totalement mathématiques ou alors le traiter sous forme de mots puisque chacune des lettres R,U etc. correspond à une permutation (voir numérotation du Cube). Il existe donc une fonction surjective de l'ensemble des mots sur $X = \{R,L,U,D,F,B\}$ vers l'ensemble des permutations du Cube. Pour une permutation, la longueur est définie comme étant, en partant du Cube résolu, le nombre minimum de mouvement (= générateurs considérés) à effectuer pour obtenir la permutation.

Première application : nombre minimum de mouvements

À partir de ces mouvements, on peut construire un arbre où chaque nœud représente une position du cube (la permutation appliquée au cube résolu). En partant de l'identité, on peut construire une suite (S_n) qui à chaque étape est égal au nombre de position possible du cube réalisable avec n mouvements de base. On a $S_0 = 1, S_1 = 18, S_2 = 18 * 18 + 27$ et ensuite pour tout n , on a $S_n = 12S_{n-1} - 18S_{n-2}$. En effet, pour plus de précision dans le calcul, il ne faut pas compter toutes les permutations qui permettraient de revenir à une position déjà atteinte. Pour cela, il faut donc fixer des conditions (on compte ici les mouvements de la tranche du milieu) : on ne compte pas les positions obtenues par deux mouvements consécutifs sur une même face ni trois mouvements autour du même axe. Dans une situation donnée, il ne reste plus que 12 dans une position de S_{n-1} mouvements possible plus les 18 que l'on peut effectuer sur S_{n-2} qui correspond aux positions où l'on n'a pas répété les mouvements (ou encore les positions où l'on a répété les mouvements pour revenir à une identité). On peut ensuite calculer le terme général de la suite

(S_n) puis l'égaliser à N , le nombre de positions totales possibles du cube afin de déterminer n . On trouve alors $n = 17.3$ ce qui montre qu'il existe une position du cube qui ne peut pas être atteinte en moins de 18 mouvements. Il a même été prouvé qu'une position (le centre du cube) nécessite 20 mouvements. (Voir [Optimal solutions for Rubik's Cube](#))

Générateurs et relations : présentation d'un groupe

Soit X un ensemble fini avec $n = \text{card } X$. Le groupe libre sur les générateurs éléments de X , noté F_n est le groupe des mots réduits de X .

Soit Y un groupe de mots réduits sur X . Soit R le plus petit sous groupe normal de F_n contenant Y . R constitue l'ensemble des relations de F_n . Le quotient F_n/R est un groupe ; c'est le plus grand groupe qui satisfait ces relations. On dit qu'il a pour générateurs l'ensemble X et pour relations l'ensemble Y . Un ensemble de générateurs et de relations est appelé une présentation.

En termes de notation, un élément r de R est noté sous forme d'une équation de la forme $r = 1$.

Exemple : le groupe cyclique d'ordre n possède un générateur x et une relation $x^n = 1$ donc on a $X = \{x\}$ et $R = \{(x^n)^k | k \in \mathbb{Z}\} \subset F_1 = x^k | k \in \mathbb{Z}$. C_n admet donc comme présentation : $C_n = \{x | x^n = 1\}$ Le groupe diédral d'ordre n a pour présentation $D_n = \{a, b | a^n = 1, b^2 = 1, aba = b\}$

Produit semi-direct

Recherche d'une présentation de $C_m^n \rtimes S_{n+1}$

Il faut d'abord chercher les représentations des groupes symétriques et des groupes cycliques. Pour le groupe symétrique d'ordre $n+1$, on a : $S_{n+1} = \langle a_1, \dots, a_n | (a_i a_j)^{m_{i,j}} = 1, 1 \leq i, j \leq n \rangle$ avec

$$m_{i,j} = \begin{cases} 3 & \text{si } j = i \pm 1 \\ 2 & \text{si } |i - j| > 1 \\ 1 & \text{si } i = j \end{cases} \text{ Dans le cas où } n=4, \text{ la matrice est : } \begin{pmatrix} 1 & 3 & 2 & 2 \\ 3 & 1 & 3 & 2 \\ 2 & 3 & 1 & 3 \\ 2 & 2 & 3 & 1 \end{pmatrix}$$

Pour le produit cartésien du groupe cyclique d'ordre m , on a : $C_m^n = \langle h_1, \dots, h_n | h_i^m = 1, h_i * h_j = h_j * h_i, 1 \leq i, j \leq n \rangle$

Pour le groupe symétrique, on peut associer à chaque transposition (de deux indices consécutifs) a_i une

$$\text{matrice de permutation de taille } (n+1) \times (n+1) \quad s_i = \begin{pmatrix} 1 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\ \vdots & \ddots & & & & & & \vdots \\ \vdots & & 1 & & & & & \vdots \\ \vdots & & & 0 & 1 & & & \vdots \\ \vdots & & & 1 & 0 & & & \vdots \\ \vdots & & & & & 1 & & \vdots \\ \vdots & & & & & & \ddots & \vdots \\ 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 1 \end{pmatrix}$$

autrement dit $s_i = I - E_{ii} - E_{i+1,i+1} + E_{i,i+1} + E_{i+1,i}$

On peut aussi identifier C_m^n avec le produit cartésien $\{(h_1(x_1), \dots, h_n(x_n)) | x_i \in C_m\}$ où $h_i(t) = I - E_{ii} - E_{i+1,i+1} + tE_{ii} + t^{-1}E_{i+1,i+1}$

$$s_i h_j(t) s_i^{-1} = h_j(t), |i - j| > 1$$

On a alors les relations suivantes entre les s_i et les $h_j(t)$ $s_i h_i(t) s_i^{-1} = h_i(t)^{-1}, i = j$

$$s_{j\pm 1} h_j(t) s_{j\pm 1}^{-1} = h_i(t) h_{j\pm 1}, i = j \pm 1$$

On peut alors démontrer la propriété suivante :

$$(C_m^n \rtimes_P \mathfrak{S}_{n+1}) = \left\langle a_1, \dots, a_n, h_1, \dots, h_n \mid \begin{cases} (a_i a_j)^{m_{ij}} = 1 \\ h_i^m = 1, h_i h_j = h_j h_i \\ a_i h_j a_i^{-1} = h_j, |i - j| > 1 \\ a_i h_i a_i^{-1} = h_i^{-1} \\ a_{j\pm 1} h_j a_{j\pm 1} = h_i h_{j\pm 1} \end{cases} \right\rangle$$

Démonstration : si on appelle P la représentation présentée ci-dessus. Le but de la démonstration est bien sûr de montrer $(C_m^n \rtimes_P \mathfrak{S}_{n+1}) \cong P$. Pour cela on considère le morphisme $F : P \mapsto (C_m^n \rtimes_P \mathfrak{S}_{n+1})$ qui associe les générateurs de P avec les générateurs de $(C_m^n \rtimes_P \mathfrak{S}_{n+1})$. Par définition de l'application, F est surjective. Pour prouver l'injectivité, on note $K = \ker(F)$. En notant $\text{card}(G) = |G|$, on a d'après le théorème de Lagrange : $|P| = |P/K| |K| \geq |P/K| = |(C_m^n \rtimes_P \mathfrak{S}_{n+1})| = m^n (n+1)!$.

En considérant maintenant $H = \{h_1, \dots, h_n | h_i^m = 1, h_i h_j = h_j h_i\} \subset P$, H est un sous groupe normal à P . En effet, chaque a_i renvoie un générateur de H sur un produit de générateurs de H ou sur son inverse. Comme H est un groupe, on obtient que $\{a_i h_j a_i^{-1} | 1 \leq i, j \leq n\} = H$. On a donc $H \cong C_m^n$. Si $w = W(a_1, \dots, a_n, h_1, \dots, h_n) = 1$ est une relation de P , le mot w écrit dans le groupe quotient P/H devient un mot qui ne contiendra plus que des relations du type $(a_i a_j)^{m_{ij}} = 1$. On peut montrer ainsi que $P/H \cong S_{n+1}$ (cette partie de la démonstration sera précisée).

Ainsi, on a $|P/H| |H| = |C_m^n| |S_{n+1}|$ ce qui montre $|P| = m^n (n+1)!$ et ainsi $|K| = 1$ d'où $K = 1$. F est donc injectif donc bijectif.

■ : fin de la démonstration

Liens externes

- Pierre Colmez, « Le Rubik's Cube, groupe de poche » (<https://webusers.imj-prg.fr/~pierre.colmez/rubik.pdf>)
- W. D. Joyner, « Mathematics of the Rubik's cube » (http://www.logicalpoetry.com/rubik/math_joyner.pdf), 1996
- Matthieu Barreau, « Une analyse du Cube Hongrois » (http://ronan.terpereau.perso.math.cnrs.fr/Projet-L3/analyse_cube_hongrois.pdf), 2011

Bibliographie

- David Singmaster, *Notes on Rubik's cube*, Enslow Publishers, 1981
- Edward C. Turner et Karen F. Gold, « Rubik's Groups », *The American Mathematical Monthly*, vol. 92, n° 9, 1985, p. 617-629
(DOI 10.1080/00029890.1985.11971700 (<https://dx.doi.org/10.1080/00029890.1985.11971700>), lire en ligne (<https://maa.tandfonline.com/doi/abs/10.1080/00029890.1985.11971700>))
- André Warusfel, *Réussir le Rubik's cube*, Denoël, 1981

Notes et références

- (Singmaster, p. 4)
- (Warusfel, p. 33)
- (Colmez, p. 2)
- (Colmez, p. 3)
- (Colmez, p. 4)
- (Warusfel, p. 152-160)
- (Colmez, p. 5)
- (Colmez, p. 6)
- (Warusfel, p. 186)
- (Warusfel, p. 182)
- (Warusfel, p. 146). Ce mouvement a été découvert par Morwen Thistlethwaite (en)
- (Colmez, p. 7)
- (Warusfel, p. 184)
- http://ronan.terpereau.perso.math.cnrs.fr/Projet-L3/analyse_cube_hongrois.pdf, Proposition 3
- (Warusfel, p. 161)
- (Warusfel, p. 142)
- (Warusfel, p. 145)
- (Warusfel, p. 144)

Ce document provient de « https://fr.wikipedia.org/w/index.php?title=Groupe_du_Rubik%27s_Cube&oldid=189503529 ».

La dernière modification de cette page a été faite le 3 janvier 2022 à 01:12.

Droit d'auteur : les textes sont disponibles sous licence Creative Commons attribution, partage dans les mêmes conditions ; d'autres conditions peuvent s'appliquer. Voyez les conditions d'utilisation pour plus de détails, ainsi que les crédits graphiques. En cas de réutilisation des textes de cette page, voyez comment citer les auteurs et

mentionner la licence.

Wikipedia® est une marque déposée de la Wikimedia Foundation, Inc., organisation de bienfaisance régie par le paragraphe 501(c)(3) du code fiscal des États-Unis.

Politique de confidentialité

À propos de Wikipédia

Avertissements

Contact

Développeurs

Statistiques

Déclaration sur les témoins (cookies)