

---

# LE RUBIK'S CUBE, GROUPE DE POCHE

*par*

Pierre COLMEZ

---

## Introduction

Le Rubik's cube se compose de  $27 = 3^3$  petits cubes dont 7 sont fixes (le cube central et ceux se trouvant au centre des faces) et 20 sont mobiles (les 8 coins et les 12 bords; on note  $X$  et  $Y$  respectivement les ensembles des coins et des bords). Un ingénieux système permet à chacune des tranches extérieures de tourner, et donc de mélanger les cubes mobiles, ce qui se voit physiquement puisque les faces extérieures des cubes mobiles sont colorées (une face extérieure reste à l'extérieur au cours de ces mouvements). *Résoudre le Rubik's cube* signifie le ramener dans l'état, dit *initial*, où chacune des faces est monocolore. Nous allons expliquer pourquoi, *si on démonte un Rubik's cube et qu'on le remonte au hasard, on a une chance sur 12 de pouvoir le résoudre*. Ceci va demander de transformer le Rubik's cube en un groupe<sup>(1)</sup>.

## 1. Le groupe de Rubik

On note  $E$  l'ensemble des états possibles du cube. Cet ensemble est le produit de l'ensemble  $E_X$  des états des coins par celui  $E_Y$  des états des bords. Comme il y a 8 coins que l'on peut permuter comme on veut, et que chaque coin peut être mis, une fois sa place choisie, dans 3 positions différentes (il faut que les faces extérieures soient apparentes), on a  $|E_X| = 8! \cdot 3^8$ . De même, les 12 bords peuvent être permutés comme on veut et chacun peut être retourné, une fois son emplacement choisi; on a donc  $|E_Y| = 12! \cdot 2^{12}$ , et  $|E| = 12! \cdot 8! \cdot 3^8 \cdot 2^{12} = 2^{29} \cdot 3^{15} \cdot 5^3 \cdot 7^2 \cdot 11$ .

Maintenant, il y a un groupe  $G$  qui agit naturellement sur  $E$ ; c'est le *groupe des mélanges du Rubik's cube*, décrit plus explicitement ci-dessous (on se permet de démonter le Rubik's cube et de le reconstruire, faces colorées à l'extérieur). Il y a une bijection naturelle de  $G$  sur  $E$ , qui

---

<sup>(1)</sup>C'est un des rares groupes avec lequel on peut se promener dans la rue; on peut en faire de même avec le groupe des tresses d'Artin, mais il a tendance à s'emmêler facilement.

consiste à faire agir  $g \in G$  sur l'état initial du Rubik's cube<sup>(2)</sup>, mais il est important de faire la distinction<sup>(3)</sup> entre  $G$  et  $E$  pour comprendre en quel sens le Rubik's cube est un groupe.

On note  $\text{Rub}$  le *groupe de Rubik* qui est le sous-groupe de  $G$  engendré par les 6 rotations des tranches (c'est donc le sous-groupe des mélanges du cube que l'on peut obtenir sans casser le cube). L'énoncé que l'on cherche à démontrer se traduit alors par l'énoncé suivant, qui est un pur énoncé de théorie des groupes.

**Théorème 1.** — *Le sous-groupe  $\text{Rub}$  est d'indice 12 dans  $G$ .*

Ce résultat est une conséquence d'une description (cf. th. 5) plus précise de  $\text{Rub}$  comme sous-groupe de  $G$ . Comme on connaît le cardinal de  $G$ , on peut en déduire celui de  $\text{Rub}$  qui n'est autre que le nombre d'états du cube que l'on peut atteindre par une suite de rotations des tranches (vu la taille de ce nombre, il est difficile d'espérer pouvoir résoudre le Rubik's cube en s'en remettant au pur hasard).

**Corollaire 2.** —  $|\text{Rub}| = \frac{1}{12} \cdot 12! \cdot 8! \cdot 2^{12} \cdot 3^8 = 43\,252\,003\,274\,489\,856\,000$ .

## 2. Dévissage du groupe des mélanges

- *Séparation des bords et des coins.*— Comme on ne peut pas échanger un coin et un bord, et qu'on peut mélanger les coins et les bords totalement indépendamment, le groupe  $G$  est le produit direct  $G_X \times G_Y$  du groupe  $G_X$  des mélanges des coins et du groupe  $G_Y$  des mélanges des bords. On peut donc écrire tout élément  $g$  de  $G$  sous la forme  $g = (\pi_X(g), \pi_Y(g))$ , où  $\pi_X(g) \in G_X$  et  $\pi_Y(g) \in G_Y$ ; de plus  $\pi_X : G \rightarrow G_X$  et  $\pi_Y : G \rightarrow G_Y$  sont des morphismes de groupes. Les groupes  $G_X$  et  $G_Y$  sont les sous-groupes de  $G$  laissant fixes  $Y$  et  $X$  respectivement; ce sont aussi les noyaux respectifs de  $\pi_Y$  et  $\pi_X$ .

- *Le groupe des mélanges de coins.*— Ne regarder que les emplacements des coins sans tenir compte de leurs orientations fournit un morphisme naturel de groupes  $g \mapsto \sigma_X(g)$  de  $G_X$  dans le groupe des permutations  $\text{Perm}_X$  de l'ensemble  $X$  des coins. Ce morphisme est surjectif car tous les coins sont physiquement identiques; le noyau de ce morphisme est le groupe  $\text{Rot}_X$  des

<sup>(2)</sup>En fait, on aurait pu partir de n'importe quel état  $e$ , et obtenir une bijection  $g \mapsto g \cdot e$  de  $G$  sur  $E$ ; en résumé, on peut passer de n'importe quel état du cube à n'importe quel autre en faisant agir  $G$ , et ceci par l'action d'un unique élément de  $G$ ; on dit que  $E$  est un *espace principal homogène* sous l'action de  $G$ . Une situation analogue est celle où  $E$  est un espace affine et  $G$  est l'espace vectoriel associé : le choix d'une origine  $O$  dans  $E$  définit une bijection  $\vec{v} \mapsto O + \vec{v}$  de  $G$  sur  $E$ , et on peut passer de n'importe quel point de  $E$  à n'importe quel autre point en translatant par un vecteur de  $G$ , et ceci de manière unique. De même, l'ensemble des bases d'un espace vectoriel de dimension  $n$  sur un corps  $K$  est un espace principal homogène sous l'action du groupe  $\text{GL}_n(K)$ .

<sup>(3)</sup>Ceci revient à faire la distinction entre les morceaux qui composent le cube et leurs positions : le groupe des mélanges agit sur les positions et  $g \in G$  envoie le morceau  $x$  se trouvant dans la position  $p$  sur la position  $g(p)$ , indépendamment de la position de  $x$  dans l'état initial du cube.

rotations des coins, qui est isomorphe<sup>(4)</sup> à  $(\mathbf{Z}/3\mathbf{Z})^X = \prod_{x \in X} (\mathbf{Z}/3\mathbf{Z})$ . On peut aussi voir  $\text{Perm}_X$  comme un sous-groupe de  $G_X$  en privilégiant une des faces visibles de  $x$ , pour tout  $x \in X$  : si  $\sigma \in \text{Perm}_X$ , alors  $\sigma$  envoie le cube se trouvant dans le coin  $x$  sur le cube  $x' = \sigma(x)$ , la face privilégiée de  $x$  étant apposée sur la face privilégiée de  $x'$ . On peut alors écrire tout élément  $g$  de  $G_X$ , de manière unique, sous la forme  $g = \rho\sigma$ , où  $\rho \in \text{Rot}_X$  et  $\sigma \in \text{Perm}_X$ , ce qui traduit le fait qu'un mélange des coins peut se décomposer en une permutation des coins (envoyant les faces privilégiées sur les faces privilégiées), suivi d'une rotation des coins.

On fera attention que les groupes  $\text{Rot}_X$  et  $\text{Perm}_X$  ne commutent pas : si  $\rho = (n_x)_{x \in X}$  et si  $\sigma \in \text{Perm}_X$ , alors  $\sigma\rho\sigma^{-1}$  est la rotation  $(n'_x)_{x \in X}$ , avec  $n'_x = n_{\sigma(x)}$ . Le groupe  $G_X$  n'est donc pas le produit direct<sup>(5)</sup> des groupes  $\text{Rot}_X$  et  $\text{Perm}_X$ .

Si  $g = \rho\sigma$ , où  $\rho = (n_x)_{x \in X} \in \text{Rot}_X$  et  $\sigma \in \text{Perm}_X$ , on définit la *rotation totale*  $\text{rt}_X(g)$  de  $g$  par la formule  $\text{rt}_X(g) = \sum_{x \in X} n_x$  ; c'est un élément de  $\mathbf{Z}/3\mathbf{Z}$ .

**Lemme 3.** —  $\text{rt}_X : G_X \rightarrow \mathbf{Z}/3\mathbf{Z}$  est un morphisme de groupes<sup>(6)</sup>.

*Démonstration.* — Si  $g = \rho\sigma$  et  $g' = \rho'\sigma'$ , avec  $\rho = (n_x)_{x \in X}$  et  $\rho' = (n'_x)_{x \in X}$ , alors  $gg' = \rho''\sigma''$ , où  $\rho'' = \rho\sigma\rho'\sigma^{-1}$  et  $\sigma'' = \sigma\sigma'$ . Or  $\sigma\rho'\sigma^{-1} = (m_x)_{x \in X}$ , avec  $m_x = n'_{\sigma(x)}$ , et donc, si  $\rho'' = (n''_x)_{x \in X}$ , on a  $n''_x = n_x + n'_{\sigma(x)}$ . Il s'ensuit que  $\text{rt}_X(gg') = \sum_{x \in X} (n_x + n'_{\sigma(x)})$ , et comme  $\sum_{x \in X} n'_{\sigma(x)} = \sum_{x \in X} n'_x$ , puisque  $x \mapsto \sigma(x)$  est une bijection de  $X$ , on obtient finalement  $\text{rt}_X(gg') = \sum_{x \in X} n_x + \sum_{x \in X} n'_x = \text{rt}_X(g) + \text{rt}_X(g')$ , ce qui permet de conclure.

• *Le groupe des mélanges des bords.* — On peut faire la même discussion avec les bords : on dispose d'un morphisme naturel de groupes  $g \mapsto \sigma_Y(g)$  de  $G_Y$  dans le groupe des permutations  $\text{Perm}_Y$  de l'ensemble  $Y$  des bords. Ce morphisme est surjectif et son noyau est le groupe  $\text{Rot}_Y$  des retournements des bords, qui est isomorphe à  $(\mathbf{Z}/2\mathbf{Z})^Y$ . On peut encore voir  $\text{Perm}_Y$  comme un sous-groupe de  $G_Y$  en privilégiant une des faces visibles de  $m$ , pour tout  $y \in Y$ , ce qui permet d'écrire tout élément  $g$  de  $G_Y$ , de manière unique, sous la forme  $g = \rho\sigma$ , où  $\rho \in \text{Rot}_Y$  et  $\sigma \in \text{Perm}_Y$ . On définit la *rotation totale*  $\text{rt}_Y(g)$  de  $g \in G_Y$  par  $\text{rt}_Y(g) = \sum_{y \in Y} n_y$ , si  $g = \rho\sigma$ ,

<sup>(4)</sup>Si  $(n_x)_{x \in X}$  est un élément de  $(\mathbf{Z}/3\mathbf{Z})^X$ , la rotation qui lui correspond fait tourner le coin  $x$  de  $n_x$  tiers de tour (dans le sens des aiguilles d'une montre) autour de l'axe partant du centre du Rubik's cube et passant par le coin du Rubik's cube correspondant à  $x$ .

<sup>(5)</sup>C'est le *produit semi-direct* de  $\text{Rot}_X$  et  $\text{Perm}_X$  (cette situation est assez rare : en général, si  $\varphi : G \rightarrow H$  est un morphisme surjectif de groupes, il est impossible de trouver un sous-groupe de  $G$ , isomorphe à  $H$ , s'envoyant bijectivement sur  $H$  par  $\varphi$ ).

<sup>(6)</sup>On peut se demander en quoi les constructions précédentes dépendent du choix des faces privilégiées. Soient donc  $(f_x)_{x \in X}$  et  $(f'_x)_{x \in X}$  deux choix de faces, et notons  $\iota$  et  $\iota'$  les injections de  $\text{Perm}_X$  dans  $G_X$  déterminées par ces deux choix. Il existe un unique  $r \in \text{Rot}_X$  envoyant  $f_x$  sur  $f'_x$ , pour tout  $x \in X$ , et on a  $\iota'(\sigma) = r\iota(\sigma)r^{-1}$  pour tout  $\sigma \in \text{Perm}_X$ . En effet, par définition  $\iota'(\sigma)$  envoie la face  $f'_x$  du coin  $x$  sur la face  $f'_{\sigma(x)}$  du coin  $\sigma(x)$ , ce qui est aussi le cas de  $r\iota(\sigma)r^{-1}$  puisque  $r^{-1}(f'_x) = f_x$ ,  $\iota(\sigma)(f_x) = f_{\sigma(x)}$  et  $r(f_{\sigma(x)}) = f'_{\sigma(x)}$ .

Il s'ensuit que si  $g$  se décompose sous la forme  $g = \rho\sigma$ , où  $\rho = (n_x)_{x \in X}$ , avec le choix  $(f_x)_{x \in X}$  et sous la forme  $g = \rho'\sigma'$ , où  $\rho' = (n'_x)_{x \in X}$ , avec le choix  $(f'_x)_{x \in X}$ , alors  $\sigma' = \sigma$  et  $\rho' = \rho r^{-1}\iota'(\sigma)r\iota(\sigma)^{-1}$ . Maintenant, si  $r = (m_x)_{x \in X}$ , alors  $\iota'(\sigma)r\iota(\sigma)^{-1} = (m'_x)_{x \in X}$ , avec  $m'_x = m_{\sigma(x)}$ , et donc  $n'_x = n_x + m_x - m_{\sigma(x)}$ . On en déduit que  $\sum_{x \in X} n'_x = \sum_{x \in X} n_x$ , ce qui prouve que  $\text{rt}_X$  est indépendant du choix des faces privilégiées.

avec  $\rho = (n_y)_{y \in Y} \in \text{Rot}_Y$  et  $\sigma \in \text{Perm}_Y$ . On obtient, comme ci-dessus, un morphisme de groupes  $\text{rt}_Y : G_Y \rightarrow \mathbf{Z}/2\mathbf{Z}$ .

On peut décrire le morphisme  $\text{rt}_Y$  de manière un peu plus directe : on note  $F$  l'ensemble des faces visibles des bords (comme chaque bord a deux faces visibles, on a  $|F| = 2|Y| = 24$ ). Le groupe  $G_Y$  permute les éléments de  $F$ , d'où un morphisme de groupe  $\sigma_F : G_Y \rightarrow \text{Perm}_F$ .

**Proposition 4.** — *Si  $g \in G_Y$ , alors  $(-1)^{\text{rt}_Y(g)}$  est la signature de la permutation  $\sigma_F(g)$ .*

*Démonstration.* — Il s'agit de vérifier que les deux morphismes de groupes  $g \mapsto \text{sign}(\sigma_F(g))$  et  $g \mapsto (-1)^{\text{rt}_Y(g)}$  coïncident et, pour ce faire, il suffit de le vérifier pour  $g \in \text{Perm}_Y$  et pour  $g \in \text{Rot}_Y$  retournant un seul bord : en effet, ces retournements engendrent  $\text{Rot}_Y$ , et  $G_Y$  est engendré par  $\text{Rot}_Y$  et  $\text{Perm}_Y$ .

- Si  $g \in \text{Rot}_Y$  retourne un seul bord, alors  $\text{rt}_Y(g) = 1$ , et donc  $(-1)^{\text{rt}_Y(g)} = -1$ . Par ailleurs,  $\sigma_Y(g)$  est la transposition échangeant les deux faces du bord que l'on retourne et donc  $\text{sign}(\sigma_F(g))$  est aussi égal à  $-1$ .

- Si  $g \in \text{Perm}_Y$ , alors  $\text{rt}_Y(g) = 0$ , et donc  $(-1)^{\text{rt}_Y(g)} = 1$ . Maintenant, si on note  $f_y$  la face privilégiée de  $y \in Y$  et  $f'_y$  l'autre, alors  $\sigma_F(g)$  permute les  $f_y$  et les  $f'_y$  de la même manière. Il en résulte que chaque longueur de cycle apparaît un nombre pair de fois dans la décomposition en cycles de  $\sigma_F(g)$ , et donc que  $\text{sign}(\sigma_F(g))$  est aussi égal à 1.

Ceci permet de conclure.

- *Un invariant global.*— On note  $\varepsilon$  le morphisme de  $G$  dans  $\{\pm 1\}$  envoyant  $g \in G$  sur la signature de la permutation  $\sigma_{X \cup Y}(g)$  induite sur les emplacements  $X \cup Y$  du Rubik's cube, en oubliant les orientations. Le groupe des permutations de  $X \cup Y$  contient le produit de  $\text{Perm}_X$  et  $\text{Perm}_Y$ , et  $\sigma_{X \cup Y}(g)$  correspond à l'élément  $(\sigma_X \circ \pi_X(g), \sigma_Y \circ \pi_Y(g))$  de ce produit ; on a donc aussi

$$\varepsilon(g) = \text{sign}(\sigma_X \circ \pi_X(g)) \text{sign}(\sigma_Y \circ \pi_Y(g)).$$

### 3. Le groupe de Rubik comme sous-groupe du groupe des mélanges

En combinant les trois morphismes de groupes définis ci-dessus, on obtient un morphisme de groupes

$$\text{rt} : G \rightarrow (\mathbf{Z}/3\mathbf{Z}) \times (\mathbf{Z}/2\mathbf{Z}) \times \{\pm 1\}, \quad \text{avec } \text{rt}(g) = (\text{rt}_X \circ \pi_X(g), \text{rt}_Y \circ \pi_Y(g), \varepsilon(g)).$$

Ce morphisme est surjectif de manière évidente ; son noyau  $H$  est donc d'indice 12 dans  $G$ , et le th. 1 est donc une conséquence du résultat suivant.

**Théorème 5.** — *On a  $\text{Rub} = H$ . Autrement dit, un élément  $g$  de  $G$  appartient à  $\text{Rub}$  si et seulement si  $\pi_X(g)$  et  $\pi_Y(g)$  sont de rotation totale nulle, et si  $g$  induit une permutation paire sur les emplacements du cube.*

*Démonstration.* — La démonstration de ce résultat comporte deux parties : la première (prop. 6), assez plaisante, consiste à vérifier que tout élément de  $\text{Rub}$  vérifie les conditions ci-dessus, et la seconde (prop. 12), un peu plus pénible, demande de montrer que tout élément de  $G$  vérifiant les

conditions du théorème peut s'écrire comme un produit de rotations de tranches du cube ; cela revient à décrire un algorithme de résolution<sup>(7)</sup> du Rubik's cube.

**Proposition 6.** — *Le groupe Rub est un sous-groupe de H.*

*Démonstration.* — Comme H est l'intersection des noyaux de  $rt_X \circ \pi_X$ ,  $rt_Y \circ \pi_Y$  et  $\varepsilon$ , et comme Rub est engendré par les rotations de tranche, il suffit, pour démontrer que  $\text{Rub} \subset H$ , de prouver que ces rotations de tranche appartiennent à ces noyaux. Soit donc  $g$  une rotation de tranche.

- D'après la prop. 4, le noyau de  $rt_Y$  est aussi l'ensemble des éléments de  $G_Y$  induisant une permutation de signature 1 sur l'ensemble F des faces des bords. Or  $g$  induit un produit de deux 4-cycles sur ces 24 faces, et donc est de signature 1. On en déduit l'appartenance de  $g$  au noyau de  $rt_Y \circ \pi_Y$ .

- On peut décider que les faces privilégiées sont celles du dessus et du dessous du cube ; alors les rotations d'une tranche horizontale sont nulles en chaque coin, et donc la rotation totale est nulle. Si on fait tourner une tranche verticale, les quatre coins qui ne sont pas sur cette tranche ont une rotation nulle, et les quatre autres ont pour rotations 1, 2, 1 et 2, dont la somme est effectivement nulle dans  $\mathbf{Z}/3\mathbf{Z}$ . On en déduit, dans tous les cas, l'appartenance de  $g$  au noyau de  $rt_X \circ \pi_X$ .

- $g$  induit un 4-cycle sur les coins et un 4-cycle sur les bords ; on a donc  $\varepsilon(g) = 1$ , ce qui prouve que  $g$  est dans le noyau de  $\varepsilon$ .

Ceci termine la démonstration de l'inclusion  $\text{Rub} \subset H$ .

#### 4. Résolution du Rubik's cube

L'algorithme décrit ci-dessous<sup>(8)</sup> consiste à :

- mettre les bords à leur place,
- les retourner 2 par 2 pour les orienter correctement,
- mettre les coins à leur place sans toucher aux bords,
- les retourner 2 par 2 pour les orienter correctement.

En réfléchissant un peu, on peut combiner les deux premières étapes et les deux dernières.

- *Notations.*— On note  $a, b, c, d, e$  et  $f$  les faces du Rubik's cube. Si  $r$  est une face, on note encore  $r$  la rotation d'un quart de tour de la tranche du cube correspondant à la face  $r$  (dans le sens des aiguilles d'une montre, l'axe étant orienté du centre du Rubik's cube vers le centre de la face  $r$ ). Par définition, Rub est le sous-groupe de G engendré par  $a, b, c, d, e, f$ , et si  $r$  est une

<sup>(7)</sup>L'algorithme qui en résulte n'est pas très efficace : on a vérifié, avec l'aide d'un ordinateur, qu'il est toujours possible de résoudre le Rubik's cube en moins de 25 rotations de tranche. Son intérêt est plus théorique ; il permet d'illustrer l'effet de la conjugaison sur l'action d'un groupe sur un ensemble.

<sup>(8)</sup>Il est plus facile à suivre avec un Rubik's cube en main, mais avec un peu de courage, un papier et crayon peuvent suffire (c'est quand même dommage de se priver de l'existence d'une version physique du groupe de Rubik).

face, alors  $r^{-1}$  est la rotation d'un quart de tour dans le sens trigonométrique de la tranche du cube correspondant à la face  $r$ .

Si  $r$  et  $s$  sont deux faces ayant un bord commun, on note ce bord  $y_{rs}$  (ou  $y_{sr}$ ), et si  $r, s, t$  sont trois faces ayant un coin en commun, on note ce coin  $x_{rst}$  (ou  $x_{str} \dots$ ).

On indexe les faces de telle sorte que  $(a, f)$ ,  $(b, e)$  et  $(c, d)$  forment des couples de faces opposées et que  $a$  envoie  $y_{ab}$  sur  $y_{ac}$ , et donc  $y_{ac}$  sur  $y_{ae}$ ,  $y_{ae}$  sur  $y_{ad}$  et  $y_{ad}$  sur  $y_{ab}$ . Les 8 coins sont alors  $x_{abc}$ ,  $x_{ace}$ ,  $x_{aed}$ ,  $x_{adb}$ ,  $x_{fcb}$ ,  $x_{fec}$ ,  $x_{fde}$  et  $x_{fdb}$ .

• *Mise en place des bords.*— La mise en place des bords utilise l'élément  $(a^2b)^5$  de Rub et ses conjugués. Cet élément a pour vertu d'échanger  $y_{ac}$  et  $y_{ad}$  en échangeant les faces  $a$ , et de laisser fixes les autres bords<sup>(9)</sup>. En particulier, son image dans  $\text{Perm}_Y$  par  $\sigma_Y \circ \pi_Y$  est la transposition des bords  $y_{ac}$  et  $y_{ad}$ .

Par ailleurs, on vérifie facilement que si  $y$  et  $y'$  sont deux éléments distincts de  $Y$ , alors il existe  $g \in \text{Rub}$  envoyant  $y_{ac}$  sur  $y$  et  $y_{ad}$  sur  $y'$ . L'image de  $g(a^2b)^5g^{-1}$  par  $\sigma_Y \circ \pi_Y$  est alors la transposition échangeant  $y$  et  $y'$ . Il en résulte que  $\sigma_Y \circ \pi_Y(\text{Rub})$  contient toutes les transpositions, et comme celles-ci engendrent  $\text{Perm}_Y$ , cela démontre le résultat suivant.

**Lemme 7.** — *La composée  $\sigma_Y \circ \pi_Y$  induit une surjection de Rub sur  $\text{Perm}_Y$ .*

• *Orientation des bords.*— La manipulation  $d^2fbd^{-1}$  retourne  $y_{ad}$  et laisse fixe  $y_{ac}$ ; donc

$$h = (a^2b)^5(d^2fbd^{-1})^{-1}(a^2b)^5(d^2fbd^{-1})$$

retourne  $y_{ac}$  et  $y_{ad}$  sans toucher aux autres bords. Si  $y$  et  $y'$  sont deux éléments distincts de  $Y$ , et si  $g \in \text{Rub}$  envoie  $y_{ac}$  sur  $y$  et  $y_{ad}$  sur  $y'$ , alors  $ghg^{-1}$  retourne  $y$  et  $y'$  sans toucher aux autres bords. Il s'ensuit que  $\pi_Y(\text{Rub} \cap \ker(\sigma_Y \circ \pi_Y))$  contient les retournements de deux bords quelconques, et comme ces éléments engendrent le sous-groupe  $\text{Rot}_Y^0$  de  $\text{Rot}_Y$  des éléments de rotation totale nulle (un élément de  $\text{Rot}_Y^0$  est composé d'un nombre pair de retournements de bords), cela démontre le résultat suivant.

**Lemme 8.** —  *$\pi_Y$  induit une surjection de  $\text{Rub} \cap \ker(\sigma_Y \circ \pi_Y)$  sur  $\text{Rot}_Y^0$ .*

• *Mise en place des coins.*— La mise en place des coins utilise l'élément  $(b^{-1}a^{-1}ba)^3$  de Rub. Cet élément a pour vertu de fixer les bords, et donc d'appartenir à  $\text{Rub} \cap \text{G}_X$ , et d'échanger les coins  $x_{abc}$  et  $x_{fcb}$  (en échangeant les faces  $a$  et  $f$ ) ainsi que les coins  $x_{adb}$  et  $x_{dae}$  (en échangeant les faces  $b$  et  $e$ ), tout en laissant fixes les autres. En particulier, son image dans  $\text{Perm}_X$  est un produit de deux transpositions de supports disjoints.

**Lemme 9.** — *Si  $x_1, x_2, x_3, x_4$  et  $x'_1, x'_2, x'_3, x'_4$  sont deux familles de quatre éléments distincts de  $X$ , il existe  $g \in \text{Rub}$  tel que  $\pi_X(g) \cdot x_i = x'_i$ , pour<sup>(10)</sup>  $i = 1, 2, 3, 4$ .*

<sup>(9)</sup>Le mouvement  $a^2b$  bouge 7 bords, avec un cycle de longueur 5 et un de longueur 2; sa puissance 5-ième élimine donc le cycle de longueur 5, mais il est un peu miraculeux qu'elle ne retourne aucun élément de ce cycle.

<sup>(10)</sup>On dit que Rub agit 4-transitivement sur  $X$  ou que l'action de Rub sur  $X$  est 4-transitive.

*Démonstration.* — Il suffit de prouver que l'on peut passer de n'importe quelle famille à une famille fixe, par exemple  $x_{abc}, x_{fcb}, x_{adb}, x_{dae}$  : en effet, si  $g \cdot x_1 = x_{abc}, g \cdot x_2 = x_{fcb}, g \cdot x_3 = x_{adb}, g \cdot x_4 = x_{dae}$  et  $g' \cdot x'_1 = x_{abc}, g' \cdot x'_2 = x_{fcb}, g' \cdot x'_3 = x_{adb}, g' \cdot x'_4 = x_{dae}$  alors  $((g')^{-1}g) \cdot x_i = x'_i$ , pour  $i = 1, 2, 3, 4$ .

Il est très facile d'amener deux coins quelconques sur  $x_{abc}$  et  $x_{fcb}$ , et comme  $d$  et  $e$  fixent  $x_{abc}$  et  $x_{fcb}$ , on est ramené à prouver que si  $x \neq x'$  sont deux coins distincts de  $x_{abc}$  et  $x_{fcb}$ , il existe un élément  $g$  du sous-groupe  $G_{d,e}$  de Rub engendré par  $d$  et  $e$  tel que  $g \cdot x = x_{adb}$  et  $g \cdot x' = x_{dae}$ . Or il existe  $h \in G_{d,e}$  tel que  $h \cdot x = x_{adb}$ , et il y a trois cas :

- $h \cdot x' = x_{ade}$ , et on prend  $g = h$ ,
  - $h \cdot x' = x_{baf}$ , et on prend  $g = d^{-1}h$ ,
  - $h \cdot x'$  n'est pas sur la face  $b$ ; il existe alors  $k$  tel que  $e^k \cdot (h \cdot x') = x_{ade}$ , et on prend  $g = e^k h$ .
- Ceci permet de conclure.

**Lemme 10.** — *L'image de  $\text{Rub} \cap G_X$  dans  $\text{Perm}_X$  est le sous-groupe  $\text{Alt}_X$  des permutations de signature 1.*

*Démonstration.* — L'image est incluse dans  $\text{Alt}_X$  car Rub est inclus dans le noyau de  $\varepsilon$  et qu'un élément de  $G_X$  induit l'identité sur  $Y$ . Par ailleurs, les propriétés de  $(b^{-1}a^{-1}ba)^3$  montrent que cette image contient un produit de deux transpositions  $(x_1, x_2)(x_3, x_4)$  de supports disjoints. Maintenant, si  $g \in \text{Rub}$ , alors  $g(b^{-1}a^{-1}ba)^3 g^{-1}$  appartient à  $\text{Rub} \cap G_X$ , et son image dans  $\text{Perm}_X$  est  $(g \cdot x_1, g \cdot x_2)(g \cdot x_3, g \cdot x_4)$ , ce qui permet, en utilisant le lemme précédent, d'en déduire que l'image contient tous les produits de deux transpositions de supports disjoints. Comme  $|X| \geq 5$ , ceux-ci engendrent<sup>(11)</sup>  $\text{Alt}_X$ , ce qui permet de conclure.

• *Orientation des coins.* — On note  $\text{Rot}_X^0$  le sous-groupe de  $\text{Rot}_X$  des éléments de rotation totale nulle (i.e le noyau de  $\text{rt}_X$ ). On a aussi  $\text{Rot}_X^0 = H \cap \text{Rot}_X$ , puisqu'un élément de  $\text{Rot}_X$  est déjà dans les noyaux de  $\text{rt}_Y \circ \pi_Y$  et de  $\varepsilon$ .

**Lemme 11.** — *On a  $\text{Rot}_X^0 \subset \text{Rub}$ .*

*Démonstration.* — On constate que  $ede^{-1}d^{-1}e$  laisse fixe  $x_{abc}, x_{fcb}$  et  $x_{adb}$ , et fait tourner  $x_{aed}$  d'un tiers de tour. Comme  $(b^{-1}a^{-1}ba)^3$  est un élément de  $\text{Rub} \cap G_X$ , qui échange les coins  $x_{abc}$  et  $x_{fcb}$  ainsi que les coins  $x_{adb}$  et  $x_{dae}$ , tout en laissant fixe les autres, il s'ensuit que

$$(b^{-1}a^{-1}ba)^3(ede^{-1}d^{-1}e)(b^{-1}a^{-1}ba)^3(ede^{-1}d^{-1}e)^{-1}$$

est un élément de  $\text{Rub} \cap \ker \pi_Y$  qui fixe tous les coins sauf  $x_{dae}$  et  $x_{adb}$ , qu'il fait tourner chacun d'un tiers de tour (dans des sens différents, puisque son image par  $\text{rt}_X$  est nulle). Autrement dit, si on note  $x_1$  et  $x_2$  les coins  $x_{abd}$  et  $x_{dae}$ , cet élément est l'élément  $(n_x)_{x \in X}$  de  $\text{Rot}_X^0$ , avec  $n_x = 0$  si  $x \notin \{x_1, x_2\}$ , et  $n_{x_1} + n_{x_2} = 0$  et  $n_{x_1} \neq 0$ . Comme l'action de Rub sur  $X$  est 4-transitive, et donc a fortiori 2-transitive, et comme  $ghg^{-1} = (n'_x)_{x \in X}$ , avec  $n'_x = n_{g \cdot x}$ , si  $h = (n_x)_{x \in X}$ , il en

<sup>(11)</sup>Le groupe  $A_n$  est engendré par les 3-cycles, et si  $n \geq 5$ , alors  $(abc)$  est le produit de  $(ab)(ef)$  et  $(bc)(ef)$ , si  $e \neq f$  et  $\{e, f\} \cap \{a, b, c\} = \emptyset$ .

résulte que  $\text{Rub} \cap \text{Rot}_X^0$  contient tous les éléments du type ci-dessus, et comme ceux-ci forment une famille génératrice de  $\text{Rot}_X^0$ , on a  $\text{Rub} \cap \text{Rot}_X^0 = \text{Rot}_X^0$ . Ceci permet de conclure.

• *L'inclusion*  $H \subset \text{Rub}$ .— Nous pouvons maintenant prouver le résultat suivant, ce qui termine la démonstration du th. 5

**Proposition 12.** — *On a*  $H \subset \text{Rub}$ .

*Démonstration.* — Commençons par remarquer que,  $\text{Rub}$  étant inclus dans  $H$ , le produit d'un élément de  $\text{Rub}$  et d'un élément de  $H$  donne un élément de  $H$ . Soit  $h \in H$ .

• Comme  $\sigma_Y \circ \pi_Y$  induit (cf. lemme 7) une surjection de  $\text{Rub}$  sur  $\text{Perm}_Y$ , il existe  $g_1 \in \text{Rub}$  tel que  $\sigma_Y \circ \pi_Y(g_1) = \sigma_Y \circ \pi_Y(h)$ , et alors  $h_1 = g_1^{-1}h$  est un élément de  $H$  appartenant au noyau de  $\sigma_Y \circ \pi_Y$ .

• D'après le lemme 8, il existe  $g_2 \in \text{Rub}$  tel que  $\pi_Y(g_2) = \pi_Y(h_1)$ , et alors  $h_2 = g_2^{-1}h_1$  est un élément de  $H$  appartenant à  $G_X$ .

• On a  $\varepsilon(h_2) = 1$ , et comme  $h_2$  induit l'identité sur  $Y$ , la permutation  $\sigma_X(h_2)$  appartient à  $\text{Alt}_X$ . D'après le lemme 10, ceci implique qu'il existe  $g_3 \in \text{Rub} \cap G_X$  tel que  $\sigma_X(g_3) = \sigma_X(h_2)$ , et alors  $g_4 = g_3^{-1}h_2$  est un élément de  $H \cap \text{Rot}_X$ . Or  $H \cap \text{Rot}_X = \text{Rot}_X^0$  est inclus dans  $\text{Rub}$  d'après le lemme 11 ; on a donc  $g_4 \in \text{Rub}$ .

• Comme  $h = g_1g_2g_3g_4$ , on a  $h \in \text{Rub}$ , ce qui permet de conclure.