LE RUBIK'S CUBE, GROUPE DE POCHE

par

Pierre COLMEZ

Résumé. — Ce petit texte vise à expliquer pourquoi, si on démonte le cube de Rubik et qu'on le remonte au hasard, on a une chance sur douze de pouvoir le résoudre. La démonstration est un joli exercice de théorie des groupes utilisant, en particulier, la notion d'action de groupe opérant sur un ensemble.

Pierre COLMEZ, C.M.L.S., École Polytechnique, 91128 Palaiseau Cedex, France.
Courriel : colmez@math.jussieu.fr.

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 [1].

1. Le groupe de Rubik

On note E l'ensemble des états possibles du cube. Cet ensemble est le produit de l'ensemble $\mathrm{E_X}$ des états des coins par celui $\mathrm{E_Y}$ 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 $|\mathrm{E_X}| = 8! \cdot 3^8$. De même, les 12 bords peuvent être permutés comme on veut et chacun peut être retourné, une fois son emplacement choisi ; on a donc $|\mathrm{E_Y}| = 12! \cdot 2^{12}$, et $|\mathrm{E}| = 12! \cdot 8! \cdot 3^8 \cdot 2^{12} = 2^{29} \cdot 3^{15} \cdot 5^3 \cdot 7^2 \cdot 11$.

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 consiste à faire agir $g \in \mathrm{G}$ sur l'état initial du Rubik's cube [2], mais il est important de faire la distinction [3] entre G et E pour comprendre en quel sens le Rubik's cube est un groupe.

On note 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.

---

1. 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.

2. 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 $\vec{v} \mapsto \mathrm{O} + \vec{v}$ 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 $\mathrm{GL}_n(\mathrm{K})$.

3. 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 $g \in \mathrm{G}$ 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.

Théorème 1. — *Le sous-groupe* Rub *est d'indice* 12 *dans* G.

Ce résultat est une conséquence d'une description (cf. th. 5) plus précise de Rub comme sous-groupe de G. Comme on connaît le cardinal de G, on peut en déduire celui de 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. — $|\mathrm{Rub}| = \frac{1}{12} \cdot 12! \cdot 8! \cdot 2^{12} \cdot 3^8 = 43\,252\,003\,274\,489\,856\,000$.

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 $\mathrm{G_X} \times \mathrm{G_Y}$ du groupe $\mathrm{G_X}$ des mélanges des coins et du groupe $\mathrm{G_Y}$ des mélanges des bords. On peut donc écrire tout élément g de G sous la forme $g = (\pi_{\mathrm{X}}(g), \pi_{\mathrm{Y}}(g))$, où $\pi_{\mathrm{X}}(g) \in \mathrm{G_X}$ et $\pi_{\mathrm{Y}}(g) \in \mathrm{G_X}$; de plus $\pi_{\mathrm{X}} : \mathrm{G} \to \mathrm{G_X}$ et $\pi_{\mathrm{Y}} : \mathrm{G} \to \mathrm{G_Y}$ sont des morphismes de groupes. Les groupes $\mathrm{G_X}$ et $\mathrm{G_Y}$ sont les sous-groupes de G laissant fixes Y et X respectivement ; ce sont aussi les noyaux respectifs de π_{Y} et π_{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 $g \mapsto \sigma_{\mathrm{X}}(g)$ de $\mathrm{G_X}$ dans le groupe des permutations $\mathrm{Perm_X}$ 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 $\mathrm{Rot_X}$ des rotations des coins, qui est isomorphe [4] à $(\mathbf{Z}/3\mathbf{Z})^{\mathrm{X}} = \prod_{x \in \mathrm{X}} (\mathbf{Z}/3\mathbf{Z})$. On peut aussi voir $\mathrm{Perm_X}$ comme un sous-groupe de $\mathrm{G_X}$ en privilégiant une des faces visibles de x, pour tout $x \in \mathrm{X}$: si $\sigma \in \mathrm{Perm_X}$, alors σ 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 $\mathrm{G_X}$, de manière unique, sous la forme $g = \rho\sigma$, où $\rho \in \mathrm{Rot_X}$ et $\sigma \in \mathrm{Perm_X}$, 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 $\mathrm{Rot_X}$ et $\mathrm{Perm_X}$ ne commutent pas : si $\rho = (n_x)_{x \in \mathrm{X}}$ et si $\sigma \in \mathrm{Perm_X}$, alors $\sigma\rho\sigma^{-1}$ est la rotation $(n'_x)_{x \in \mathrm{X}}$, avec $n'_x = n_{\sigma(x)}$. Le groupe $\mathrm{G_X}$ n'est donc pas le produit direct [5] des groupes $\mathrm{Rot_X}$ et $\mathrm{Perm_X}$.

4. Si $(n_x)_{x \in \mathrm{X}}$ est un élément de $(\mathbf{Z}/3\mathbf{Z})^{\mathrm{X}}$, 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.

5. C'est le *produit semi-direct* de $\mathrm{Rot_X}$ et $\mathrm{Perm_X}$ (cette situation est assez rare : en général, si $\varphi : \mathrm{G} \to \mathrm{H}$ 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 φ).

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

Lemme 3. — $\mathrm{rt}_{\mathrm{X}} : \mathrm{G}_{\mathrm{X}} \to \mathbf{Z}/3\mathbf{Z}$ *est un morphisme de groupes*[6].

Démonstration. — Si $g = \rho\sigma$ et $g' = \rho'\sigma'$, avec $\rho = (n_x)_{x\in \mathrm{X}}$ et $\rho' = (n'_x)_{x\in \mathrm{X}}$, alors $gg' = \rho''\sigma''$, où $\rho'' = \rho\sigma\rho'^{-1}$ et $\sigma'' = \sigma\sigma'$. Or $\sigma\rho'^{-1} = (m_x)_{x\in \mathrm{X}}$, avec $m_x = n'_{\sigma(x)}$, et donc, si $\rho'' = (n''_x)_{x\in \mathrm{X}}$, on a $n''_x = n_x + n'_{\sigma(x)}$. Il s'ensuit que $\mathrm{rt}_{\mathrm{X}}(gg') = \sum_{x\in \mathrm{X}}(n_x + n'_{\sigma(x)})$, et comme $\sum_{x\in \mathrm{X}} n'_{\sigma(x)} = \sum_{x\in \mathrm{X}} n'_x$, puisque $x \mapsto \sigma(x)$ est une bijection de X, on obtient finalement $\mathrm{rt}_{\mathrm{X}}(gg') = \sum_{x\in \mathrm{X}} n_x + \sum_{x\in \mathrm{X}} n'_x = \mathrm{rt}_{\mathrm{X}}(g) + \mathrm{rt}_{\mathrm{X}}(g')$, 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 $g \mapsto \sigma_{\mathrm{Y}}(g)$ de G_{Y} dans le groupe des permutations $\mathrm{Perm}_{\mathrm{Y}}$ de l'ensemble Y des bords. Ce morphisme est surjectif et son noyau est le groupe $\mathrm{Rot}_{\mathrm{Y}}$ des retournements des bords, qui est isomorphe à $(\mathbf{Z}/2\mathbf{Z})^{\mathrm{Y}}$. On peut encore voir $\mathrm{Perm}_{\mathrm{Y}}$ comme un sous-groupe de G_{Y} en privilégiant une des faces visibles de m, pour tout $y \in \mathrm{Y}$, ce qui permet d'écrire tout élément g de G_{Y}, de manière unique, sous la forme $g = \rho\sigma$, où $\rho \in \mathrm{Rot}_{\mathrm{Y}}$ et $\sigma \in \mathrm{Perm}_{\mathrm{Y}}$. On définit la *rotation totale* $\mathrm{rt}_{\mathrm{Y}}(g)$ de $g \in \mathrm{G}_{\mathrm{Y}}$ par $\mathrm{rt}_{\mathrm{Y}}(g) = \sum_{y\in \mathrm{Y}} n_y$, si $g = \rho\sigma$, avec $\rho = (n_y)_{y\in \mathrm{Y}} \in \mathrm{Rot}_{\mathrm{Y}}$ et $\sigma \in \mathrm{Perm}_{\mathrm{Y}}$. On obtient, comme ci-dessus, un morphisme de groupes $\mathrm{rt}_{\mathrm{Y}} : \mathrm{G}_{\mathrm{Y}} \to \mathbf{Z}/2\mathbf{Z}$.

On peut décrire le morphisme 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 $|\mathrm{F}| = 2|\mathrm{Y}| = 24$). Le groupe G_{Y} permute les éléments de F, d'où un morphisme de groupe $\sigma_{\mathrm{F}} : \mathrm{G}_{\mathrm{Y}} \to \mathrm{Perm}_{\mathrm{F}}$.

Proposition 4. — *Si $g \in \mathrm{G}_{\mathrm{Y}}$, alors $(-1)^{\mathrm{rt}_{\mathrm{Y}}(g)}$ est la signature de la permutation $\sigma_{\mathrm{F}}(g)$.*

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

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

---

6. On peut se demander en quoi les constructions précédentes dépendent du choix des faces privilégiées. Soient donc $(f_x)_{x\in \mathrm{X}}$ et $(f'_x)_{\in \mathrm{X}}$ deux choix de faces, et notons ι et ι' les injections de $\mathrm{Perm}_{\mathrm{X}}$ dans G_{X} déterminées par ces deux choix. Il existe un unique $r \in \mathrm{Rot}_{\mathrm{X}}$ envoyant f_x sur f'_x, pour tout $x \in \mathrm{X}$, et on a ι'^{-1} pour tout $\sigma \in \mathrm{Perm}_{\mathrm{X}}$. 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 $\rho = (n_x)_{x\in \mathrm{X}}$, avec le choix $(f_x)_{x\in \mathrm{X}}$ et sous la forme $g = \rho'\sigma'$, où $\rho' = (n'_x)_{x\in \mathrm{X}}$, avec le choix $(f'_x)_{x\in \mathrm{X}}$, alors $\sigma' = \sigma$ et $\rho'^{-1}\iota'(\sigma)r\iota'^{-1}$. Maintenant, si $r = (m_x)_{x\in \mathrm{X}}$, alors $\iota'(\sigma)r\iota'^{-1} = (m'_x)_{x\in \mathrm{X}}$, avec $m'_x = m_{\sigma(x)}$, et donc $n'_x = n_x + m_x - m_{\sigma(x)}$. On en déduit que $\sum_{x\in \mathrm{X}} n'_x = \sum_{x\in \mathrm{X}} n_x$, ce qui prouve que rt_{X} est indépendant du choix des faces privilégiées.

• Si $g \in \mathrm{Perm_Y}$, alors $\mathrm{rt_Y}(g) = 0$, et donc $(-1)^{\mathrm{rt_Y}(g)} = 1$. Maintenant, si on note f_y la face privilégiée de $y \in \mathrm{Y}$ et f'_y l'autre, alors $\sigma_{\mathrm{F}}(g)$ 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 $\sigma_{\mathrm{F}}(g)$, et donc que $\mathrm{sign}(\sigma_{\mathrm{F}}(g))$ est aussi égal à 1.

Ceci permet de conclure.

• *Un invariant global.*— On note ε le morphisme de G dans $\{\pm 1\}$ envoyant $g \in \mathrm{G}$ sur la signature de la permutation $\sigma_{\mathrm{X}\cup\mathrm{Y}}(g)$ induite sur les emplacements $\mathrm{X}\cup\mathrm{Y}$ du Rubik's cube, en oubliant les orientations. Le groupe des permutations de $\mathrm{X}\cup\mathrm{Y}$ contient le produit de $\mathrm{Perm_X}$ et $\mathrm{Perm_Y}$, et $\sigma_{\mathrm{X}\cup\mathrm{Y}}(g)$ correspond à l'élément $(\sigma_{\mathrm{X}} \circ \pi_{\mathrm{X}}(g), \sigma_{\mathrm{Y}} \circ \pi_{\mathrm{Y}}(g))$ de ce produit ; on a donc aussi

$$\varepsilon(g) = \mathrm{sign}(\sigma_{\mathrm{X}} \circ \pi_{\mathrm{X}}(g))\,\mathrm{sign}(\sigma_{\mathrm{Y}} \circ \pi_{\mathrm{Y}}(g)).$$

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

$$\mathrm{rt} : \mathrm{G} \to (\mathbf{Z}/3\mathbf{Z}) \times (\mathbf{Z}/2\mathbf{Z}) \times \{\pm 1\}, \quad \text{avec } \mathrm{rt}(g) = (\mathrm{rt_X} \circ \pi_{\mathrm{X}}(g), \mathrm{rt_Y} \circ \pi_{\mathrm{Y}}(g), \varepsilon(g)).$$

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* $\mathrm{Rub} = \mathrm{H}$. *Autrement dit, un élément* g *de* G *appartient à* Rub *si et seulement si* $\pi_{\mathrm{X}}(g)$ *et* $\pi_{\mathrm{Y}}(g)$ *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 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 [7] du Rubik's cube.

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

Démonstration. — Comme H est l'intersection des noyaux de $\mathrm{rt_X} \circ \pi_{\mathrm{X}}$, $\mathrm{rt_Y} \circ \pi_{\mathrm{Y}}$ et ε, et comme Rub est engendré par les rotations de tranche, il suffit, pour démontrer que $\mathrm{Rub} \subset \mathrm{H}$, 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 $\mathrm{rt_Y}$ est aussi l'ensemble des éléments de $\mathrm{G_Y}$ induisant une permutation de signature 1 sur l'ensemble F des faces des bords. Or g induit un produit de deux

7. 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.

4-cycles sur ces 24 faces, et donc est de signature 1. On en déduit l'appartenance de g au noyau de $\mathrm{rt}_{\mathrm{Y}} \circ \pi_{\mathrm{Y}}$.

• 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 $\mathrm{rt}_{\mathrm{X}} \circ \pi_{\mathrm{X}}$.

• 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 ε.

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

4. Résolution du Rubik's cube

L'algorithme décrit ci-dessous [8] 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 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} ...).

On indexe les faces de telle sorte que (a, f), (b, e) et (c, d) forment des couples de faces opposées et que a envoye 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_{fbd}.

• *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

8. 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).

fixes les autres bords [9]. En particulier, son image dans $\mathrm{Perm_Y}$ par $\sigma_\mathrm{Y} \circ \pi_\mathrm{Y}$ 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 $g \in \mathrm{Rub}$ envoyant y_{ac} sur y et y_{ad} sur y'. L'image de $g(a^2b)^5g^{-1}$ par $\sigma_\mathrm{Y} \circ \pi_\mathrm{Y}$ est alors la transposition échangeant y et y'. Il en résulte que $\sigma_\mathrm{Y} \circ \pi_\mathrm{Y}(\mathrm{Rub})$ contient toutes les transpositions, et comme celles-ci engendrent $\mathrm{Perm_Y}$, cela démontre le résultat suivant.

Lemme 7. — *La composée $\sigma_\mathrm{Y} \circ \pi_\mathrm{Y}$ induit une surjection de* Rub *sur* $\mathrm{Perm_Y}$.

• *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 $g \in \mathrm{Rub}$ 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 $\pi_\mathrm{Y}(\mathrm{Rub} \cap \ker(\sigma_\mathrm{Y} \circ \pi_\mathrm{Y}))$ contient les retournements de deux bords quelconques, et comme ces éléments engendrent le sous-groupe $\mathrm{Rot_Y^0}$ de $\mathrm{Rot_Y}$ des éléments de rotation totale nulle (un élément de $\mathrm{Rot_Y^0}$ est composé d'un nombre pair de retournements de bords), cela démontre le résultat suivant.

Lemme 8. — *π_Y induit une surjection de* $\mathrm{Rub} \cap \ker(\sigma_\mathrm{Y} \circ \pi_\mathrm{Y})$ *sur* $\mathrm{Rot_Y^0}$.

• *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 $\mathrm{Rub} \cap \mathrm{G_X}$, 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 $\mathrm{Perm_X}$ 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 $g \in \mathrm{Rub}$ tel que $\pi_\mathrm{X}(g) \cdot x_i = x'_i$, pour* [10] $i = 1, 2, 3, 4$.

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 $\mathrm{G}_{d,e}$ de Rub engendré par d et e tel que $g \cdot x = x_{adb}$ et $g \cdot x' = x_{dae}$. Or il existe $h \in \mathrm{G}_{d,e}$ tel que $h \cdot x = x_{adb}$, et il y a trois cas :

- $h \cdot x' = x_{ade}$, et on prend $g = h$,
- $h \cdot x' = x_{bdf}$, et on prend $g = d^{-1}h$,

9. 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.

10. On dit que Rub *agit 4-transitivement* sur X ou que l'action de Rub sur X est 4-*transitive*.

• $h \cdot x'$ 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* $\mathrm{Rub} \cap \mathrm{G_X}$ *dans* $\mathrm{Perm_X}$ *est le sous-groupe* $\mathrm{Alt_X}$ *des permutations de signature* 1.

Démonstration. — L'image est incluse dans $\mathrm{Alt_X}$ car Rub est inclus dans le noyau de ε et qu'un élément de $\mathrm{G_X}$ 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 $g \in \mathrm{Rub}$, alors $g(b^{-1}a^{-1}ba)^3 g^{-1}$ appartient à $\mathrm{Rub} \cap \mathrm{G_X}$, et son image dans $\mathrm{Perm_X}$ 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 $|\mathrm{X}| \geqslant 5$, ceux-ci engendrent [11] $\mathrm{Alt_X}$, ce qui permet de conclure.

• *Orientation des coins.*— On note $\mathrm{Rot_X^0}$ le sous-groupe de $\mathrm{Rot_X}$ des éléments de rotation totale nulle (i.e le noyau de $\mathrm{rt_X}$). On a aussi $\mathrm{Rot_X^0} = \mathrm{H} \cap \mathrm{Rot_X}$, puisqu'un élément de $\mathrm{Rot_X}$ est déjà dans les noyaux de $\mathrm{rt_Y} \circ \pi_\mathrm{Y}$ et de ε.

Lemme 11. — *On a* $\mathrm{Rot_X^0} \subset \mathrm{Rub}$.

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 $\mathrm{Rub} \cap \mathrm{G_X}$, 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 $\mathrm{Rub} \cap \ker \pi_\mathrm{Y}$ 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 $\mathrm{rt_X}$ est nulle). Autrement dit, si on note x_1 et x_2 les coins x_{abd} et x_{dae}, cet élément est l'élément $(n_x)_{x \in \mathrm{X}}$ de $\mathrm{Rot_X^0}$, 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 $ghg^{-1} = (n'_x)_{x \in \mathrm{X}}$, avec $n'_x = n_{g \cdot x}$, si $h = (n_x)_{x \in \mathrm{X}}$, il en résulte que $\mathrm{Rub} \cap \mathrm{Rot_X^0}$ contient tous les éléments du type ci-dessus, et comme ceux-ci forment une famille génératrice de $\mathrm{Rot_X^0}$, on a $\mathrm{Rub} \cap \mathrm{Rot_X^0} = \mathrm{Rot_X^0}$. Ceci permet de conclure.

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

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

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

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

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

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

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

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

Pierre COLMEZ