# The Rubik's Cube: A Pocket Group

Le Rubik's Cube, Groupe de Poche

-

Re-TEXed by Seewoo Lee*

Pierre Colmez

Last updated: July 16, 2025

## Introduction

The Rubik's cube is made up of 27 small cubes, of which 7 are fixed (the central cube and those at the center of the faces), and 20 are movable (the 8 corners and the 12 edges; we denote by **X** and **Y** the sets of corners and edges, respectively). An ingenious mechanism allows each of the outer layers to rotate, thereby scrambling the movable cubes; this is physically visible since the outer faces of the movable cubes are colored (an outer face remains on the outside while rotating the layers). Solving the Rubik's Cube means returning it to the *initial* state, where each face is a single color. We will explain why, if you disassemble a Rubik's Cube and reassemble it randomly, you have a $\frac{1}{12}$ chance of being able to solve it. This will require transforming the Rubik's Cube into a group[1].

## 1 The Rubik's Group

Let $\mathbf{E}$ denote the set of all possible states of the cube. This set is the product of the set $\mathbf{E_X}$ of corner states and the set $\mathbf{E_Y}$ of edge states. Since there are 8 corners that can be permuted freely, and each corner, once its position is chosen, can be placed in 3 different orientations (the outer faces must be visible), we have $|\mathbf{E_X}| = 8! \times 3^8$. Similarly, the 12 edges can be freely permuted, and each can be flipped once its position is fixed; therefore, $|\mathbf{E_Y}| = 12! \times 2^{12}$, and hence $|\mathbf{E}| = 12! \times 8! \times 3^8 \times 2^{12} = 2^{29} \times 3^{15} \times 5^3 \times 7^2 \times 11$.

Now, there is a group $\mathbf{G}$ that acts naturally on $\mathbf{E}$; it is the group of all Rubik's Cube configurations (i.e., all possible scramblings), described more explicitly below (we allow ourselves to disassemble the Rubik's Cube and reassemble it, with the colored faces on the outside). There is a natural bijection between $\mathbf{G}$ and $\mathbf{E}$, consisting of letting an element $g \in \mathbf{G}$ act on the initial

*seewoo5@berkeley.edu. Most of the translation is due to ChatGPT, and I only fixed a little.

[1] It is one of the rare groups you can walk down the street with; you can do the same with Artin's braid group, but it tends to get tangled easily.

state of the Rubik's Cube[2]. However, it is important to distinguish[3] between **G** and **E** in order to understand in what sense the Rubik's Cube forms a group.

Let **Rub** denote the Rubik's group, which is the subgroup of **G** generated by the 6 rotations of the layers (thus, it is the subgroup of scramblings that can be achieved without taking the cube apart). The statement we aim to prove can then be expressed as the following, which is a purely group-theoretic result.

**Theorem 1.** The index of the subgroup **Rub** of **G** is 12.

This result is a consequence of a more precise description (see Theorem 5) of **Rub** as a subgroup of **G**. Since the size of **G** is known, we can deduce that of **Rub**, which is nothing other than the number of cube states that can be reached through a sequence of legal moves (given the size of this number, it is difficult to hope to solve the Rubik's Cube by relying on pure chance).

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

## 2 Uncovering the Scrambling Group

- *Seperation of edges and corners.* Since it is not possible to swap a corner and an edge, and since the corners and edges can be scrambled completely independently, the group **G** is the direct product $\mathbf{G} = \mathbf{G_X} \times \mathbf{G_Y}$ of the group $\mathbf{G_X}$ of corner moves and the group $\mathbf{G_Y}$ of edge moves. Thus, every element $g$ of $G$ can be written in the form

$$g = (\pi_{\mathbf{X}}(g), \pi_{\mathbf{Y}}(g)),$$

  where $\pi_{\mathbf{X}}(g) \in \mathbf{G_X}$ and $\pi_{\mathbf{Y}}(g) \in \mathbf{G_Y}$. Moreover,

$$\pi_{\mathbf{X}} : \mathbf{G} \to \mathbf{G_X} \quad \text{and} \quad \pi_{\mathbf{Y}} : \mathbf{G} \to \mathbf{G_Y}$$

  are group homomorphisms. The groups $\mathbf{G_X}$ and $\mathbf{G_Y}$ are the subgroups of **G** that fix **Y** and **X**, respectively; they are also the kernels of $\pi_{\mathbf{Y}}$ and $\pi_{\mathbf{X}}$, respectively.

- *The group of scrambling corners.* By considering only the positions of the corners, ignoring their orientations, gives a natural group homomorphism $g \mapsto \sigma_{\mathbf{X}}(g)$ from $\mathbf{G_X}$ to the group of permutations $\mathbf{Perm_X}$ of the set **X** of corners. This morphism is surjective, since all the corners are physically identical. The kernel of this morphism is the group $\mathbf{Rot_X}$ of corner rotations, which is isomorphic[4] to $(\mathbb{Z}/3\mathbb{Z})^{\mathbf{X}} = \prod_{x \in \mathbf{X}} (\mathbb{Z}/3\mathbb{Z})$. We can also view $\mathbf{Perm_X}$ as a subgroup of $\mathbf{G_X}$ by selecting a distinguished (visible) face of each corner cube $x \in \mathbf{X}$: if $\sigma \in \mathbf{Perm_X}$,

[2] In fact, we could have started from any state $e$, and obtained a bijection $g \mapsto g \cdot e$ from $G$ to $E$; in summary, one can go from any state of the cube to any other by letting $G$ act, and this through the action of a unique element of $G$. We say that $E$ is a principal homogeneous space under the action of $G$. A similar situation occurs when $E$ is an affine space and $G$ is the associated vector space: the choice of an origin $O$ in $E$ defines a bijection $v \mapsto O + v$ from $G$ to $E$, and one can go from any point in $E$ to any other point by translating by a vector from $G$, and in a unique way. Likewise, the set of bases of a vector space of dimension $n$ over a field $K$ is a principal homogeneous space under the action of the group $\mathrm{GL}_n(K)$.

[3] This amounts to distinguishing between the pieces that make up the cube and their positions: the group of moves acts on the positions, and an element $g \in G$ sends the piece $x$ located at position $p$ to position $g(p)$, independently of the initial position of $x$ in the cube's initial state.

[4] If $(n_x)_{x \in \mathbf{X}}$ is an element of $(\mathbb{Z}/3\mathbb{Z})^{\mathbf{X}}$, the corresponding rotation rotates the corner $x$ by $n_x$ thirds of a turn (in the clockwise direction) around the axis going from the center of the Rubik's Cube through the corner of the cube corresponding to $x$.

then $\sigma$ sends the cube located at corner $x$ to corner $x' = \sigma(x)$, with the distinguished face of $x$ placed onto the distinguished face of $x'$. Thus, any element $g$ in $\mathbf{G_X}$ can be uniquely written in the form $g = \rho\sigma$, where $\rho \in \mathbf{Rot_X}$ and $\sigma \in \mathbf{Perm_X}$. This expresses the fact that any move involving the corners can be decomposed into a permutation of the corners (aligning distinguished faces), followed by a rotation of the corners.

Note that the groups $\mathbf{Rot_X}$ and $\mathbf{Perm_X}$ do not commute: if $\rho = (n_x)_{x\in\mathbf{X}}$ and $\sigma \in \mathbf{Perm_X}$, then $\sigma\rho\sigma^{-1}$ is the rotation $(n'_x)_{x\in\mathbf{X}}$, with $n'_x = n_{\sigma(x)}$. Therefore, the group $\mathbf{G_X}$ is not the direct product[5] of $\mathbf{Rot_X}$ and $\mathbf{Perm_X}$.

If $g = \rho\sigma$, where $\rho = (n_x)_{x\in\mathbf{X}}$ and $\sigma \in \mathbf{Perm_X}$, then we define the *total rotation* $\mathrm{rt}_\mathbf{X}(g)$ of $g$ by the formula $\mathrm{rt}_\mathbf{X}(g) = \sum_{x\in\mathbf{X}} n_x$; it is an element of $\mathbb{Z}/3\mathbb{Z}$.

**Lemma 3.** $\mathrm{rt}_\mathbf{X} : \mathbf{G_X} \to \mathbb{Z}/3\mathbb{Z}$ is a group homomorphism.[6]

*Proof.* If $g = \rho\sigma$ and $g' = \rho'\sigma'$, with $\rho = (n_x)_{x\in\mathbf{X}}$ and $\rho' = (n'_x)_{x\in\mathbf{X}}$, then $gg' = \rho''\sigma''$, where $\rho'' = \rho \cdot \sigma\rho'\sigma^{-1}$ and $\sigma'' = \sigma\sigma'$. Now, $\sigma\rho'\sigma^{-1} = (m_x)_{x\in\mathbf{X}}$, with $m_x = n'_{\sigma(x)}$, and so, if $\rho'' = (n''_x)_{x\in\mathbf{X}}$, we have: $n''_x = n_x + n'_{\sigma(x)}$. It follows that $\mathrm{rt}_\mathbf{X}(gg') = \sum_{x\in\mathbf{X}}(n_x + n'_{\sigma(x)})$, and since $\sum_{x\in\mathbf{X}} n'_{\sigma(x)} = \sum_{x\in\mathbf{X}} n'_x$, because $x \mapsto \sigma(x)$ is a bijection of $\mathbf{X}$, we finally obtain: $\mathrm{rt}_\mathbf{X}(gg') = \sum_{x\in\mathbf{X}} n_x + \sum_{x\in\mathbf{X}} n'_x = \mathrm{rt}_\mathbf{X}(g) + \mathrm{rt}_\mathbf{X}(g')$, which completes the argument. □

- *The group of scrambling edges.* A similar discussion can be made for the edges: we have a natural group homomorphism $g \mapsto \sigma_\mathbf{Y}(g)$ from $\mathbf{G_Y}$ to the group of permutations $\mathbf{Perm}(\mathbf{Y})$ of the set $\mathbf{Y}$ of edges. This homomorphism is surjective, and its kernel is the group $\mathbf{Rot_Y}$ of edge flips, which is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^\mathbf{Y}$. We can again view $\mathbf{Perm_Y}$ as a subgroup of $\mathbf{G_Y}$ by selecting a preferred visible face for each edge $y \in \mathbf{Y}$, which allows any element $g \in \mathbf{G_Y}$ to be uniquely written in the form $g = \rho\sigma$, where $\rho \in \mathbf{Rot_Y}$ and $\sigma \in \mathbf{Perm_Y}$. We define the total rotation (flip) $\mathrm{rt}_\mathbf{Y}(g)$ of an element $g \in \mathbf{G_Y}$ by $\mathrm{rt}_\mathbf{Y}(g) = \sum_{y\in\mathbf{Y}} n_y$, if $g = \rho\sigma$ with $\rho = (n_y)_{y\in\mathbf{Y}}$ and $\sigma \in \mathbf{Perm_Y}$. As before, we obtain a group homomorphism $\mathrm{rt}_\mathbf{Y} : \mathbf{G_Y} \to \mathbb{Z}/2\mathbb{Z}$.

  We can describe the morphism $\mathrm{rt}_\mathbf{Y}$ a bit more directly: let $\mathbf{F}$ be the set of visible faces of the edges (since each edge has two visible faces, we have $|\mathbf{F}| = 2|\mathbf{Y}| = 24$). The group $\mathbf{G_Y}$ permutes the elements of $\mathbf{F}$, which gives rise to a group homomorphism $\sigma_\mathbf{F} : \mathbf{G_Y} \to \mathbf{Perm_F}$.

  **Proposition 4.** If $g \in \mathbf{G_Y}$, then $(-1)^{\mathrm{rt}_\mathbf{Y}(g)}$ is the signature of the permutation $\sigma_\mathbf{F}(g)$.

  *Proof.* We want to verify that the two group homomorphisms $g \mapsto \mathrm{sgn}(\sigma_\mathbf{F}(g))$ and $g \mapsto (-1)^{\mathrm{rt}_\mathbf{Y}(g)}$ coincide. To do so, it suffices to verify the equality in two cases: For $g \in \mathbf{Perm_Y}$, since $\sigma_\mathbf{F}(g)$ is a permutation of the faces of the edges, it permutes each face an even number of times, so $\mathrm{sgn}(\sigma_\mathbf{F}(g)) = 1$. For $g \in \mathbf{Rot_Y}$ that flips a single edge—since such flips generate $\mathbf{Rot_Y}$, and $\mathbf{G_Y}$ is generated by $\mathbf{Rot_Y}$ and $\mathbf{Perm_Y}$.

[5] It is the semidirect product of $\mathbf{Rot_X}$ and $\mathbf{Perm_X}$ (this situation is rather rare: in general, if $\varphi : G \to H$ is a surjective group homomorphism, it is impossible to find a subgroup of $G$, isomorphic to $H$, that maps bijectively onto $H$ via $\varphi$).

[6] One might wonder to what extent the previous constructions depend on the choice of distinguished faces. Let $(f_x)_{x\in\mathbf{X}}$ and $(f'_x)_{x\in\mathbf{X}}$ be two choices of faces, and let $\iota$ and $\iota'$ denote the injections of $\mathbf{Perm_X}$ into $\mathbf{G_X}$ determined by these two choices. There exists a unique $r \in \mathbf{Rot_X}$ that sends $f_x$ to $f'_x$ for all $x \in \mathbf{X}$, and we have $\iota'(\sigma) = r \cdot \iota(\sigma) \cdot r^{-1}$ for all $\sigma \in \mathbf{Perm_X}$. Indeed, by definition, $\iota'(\sigma)$ sends the face $f'_x$ of corner $x$ to the face $f'_{\sigma(x)}$ of corner $\sigma(x)$, which is also what $r \cdot \iota(\sigma) \cdot r^{-1}$ does, since: $r^{-1}(f'_x) = f_x$, $\iota(\sigma)(f_x) = f_{\sigma(x)}$, and $r(f_{\sigma(x)}) = f'_{\sigma(x)}$. It follows that if $g$ decomposes as $g = \rho\sigma$, where $\rho = (n_x)_{x\in\mathbf{X}}$, with the choice $(f_x)_{x\in\mathbf{X}}$, and as $g = \rho'\sigma'$, where $\rho' = (n'_x)_{x\in\mathbf{X}}$, with the choice $(f'_x)_{x\in\mathbf{X}}$, then $\sigma' = \sigma$ and $\rho' = \rho \cdot r^{-1} \cdot \iota'(\sigma) \cdot r \cdot \iota'(\sigma)^{-1}$. Now, if $r = (m_x)_{x\in\mathbf{X}}$, then $\iota'(\sigma) \cdot r \cdot \iota'(\sigma)^{-1} = (m'_x)_{x\in\mathbf{X}}$, with $m'_x = m_{\sigma(x)}$, and thus $n'_x = n_x + m_x - m_{\sigma(x)}$. We then deduce that $\sum_{x\in\mathbf{X}} n'_x = \sum_{x\in\mathbf{X}} n_x$, which proves that $\mathrm{rt}_\mathbf{X}$ is independent of the choice of distinguished faces.

- If $g \in \mathbf{Rot_Y}$ flips only one edge, then $\mathrm{rt}_\mathbf{Y}(g) = 1$, hence $(-1)^{\mathrm{rt}_\mathbf{Y}(g)} = -1$. Furthermore, $\sigma_\mathbf{F}(g)$ is the transposition swapping the two faces of that edge, so $\mathrm{sgn}(\sigma_\mathbf{F}(g)) = -1$ as well.
- If $g \in \mathbf{Perm_Y}$, then $\mathrm{rt}_\mathbf{Y}(g) = 0$, so $(-1)^{\mathrm{rt}_\mathbf{Y}(g)} = 1$. Now, if we denote $f_\mathbf{Y}$ as the preferred face of $y \in \mathbf{Y}$, and $f'_\mathbf{Y}$ as the other one, then $\sigma_\mathbf{F}(g)$ permutes $f_\mathbf{Y}$ and $f'_\mathbf{Y}$ in the same way. As a result, every cycle length in the cycle decomposition of $\sigma_\mathbf{F}(g)$ appears an even number of times, so $\mathrm{sgn}(\sigma_\mathbf{F}(g)) = 1$ as well.

This completes the proof. □

- *A global invariant.* Let $\varepsilon$ be the homomorphism from $G$ to $\{\pm 1\}$, mapping $g \in G$ to the signature of the permutation $\sigma_{\mathbf{X}\cup\mathbf{Y}}(g)$ induced on the positions $\mathbf{X} \cup \mathbf{Y}$ of the Rubik's Cube, ignoring orientations.

  The permutation group of $\mathbf{X} \cup \mathbf{Y}$ contains the product $\mathbf{Perm_X} \times \mathbf{Perm_Y}$, and $\sigma_{\mathbf{X}\cup\mathbf{Y}}(g)$ corresponds to the element $(\sigma_\mathbf{X} \circ \pi_\mathbf{X}(g), \sigma_\mathbf{Y} \circ \pi_\mathbf{Y}(g))$ of that product; hence we have:

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

## 3 The Rubik's Group as a Subgroup of the Scrambling Group

By combining the three group homomorphisms defined above, we obtain a group homomorphism:

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

This morphism is clearly surjective; its kernel **H** therefore has index 12 in G, and Theorem 1 is thus a consequence of the following result:

**Theorem 5.** We have **Rub** = **H**. In other words, an element $g$ of $G$ belongs to the Rubik's group **Rub** if and only if: $\pi_\mathbf{X}(g)$ and $\pi_\mathbf{Y}(g)$ have total rotation zero, and $g$ induces an even permutation on the cube's positions.

The proof of this result consists of two parts: the first (Proposition 6), rather pleasant, is to verify that every element of **Rub** satisfies the conditions above, and the second (Proposition 12), a bit more tedious, requires showing that every element of **G** satisfying the theorem's conditions can be written as a product of layer rotations of the cube; this amounts to describing a solution algorithm[7] for the Rubik's Cube.

**Proposition 6.** The group **Rub** is a subgroup of **H**.

*Proof.* Since **H** is the intersection of the kernels of $\mathrm{rt}_\mathbf{X} \circ \pi_\mathbf{X}$, $\mathrm{rt}_\mathbf{Y} \circ \pi_\mathbf{Y}$, and $\varepsilon$, and since **Rub** is generated by the layer rotations, it suffices to prove that these layer rotations belong to each of those kernels. Let $g$ be a layer rotation.

- From Proposition 4, the kernel of $\mathrm{rt}_\mathbf{Y}$ is also the set of elements of $\mathbf{G_Y}$ that induce a permutation of signature 1 on the set $F$ of edge faces. But $g$ induces a product of two 4-cycles on these 24 faces, so its signature is 1. We deduce that $g$ belongs to the kernel of $\mathrm{rt}_\mathbf{Y} \circ \pi_\mathbf{Y}$.

[7] The resulting algorithm is not very efficient: it has been verified, with the help of a computer, that it is always possible to solve the Rubik's Cube under 25 rotations. Its value is more theoretical; it serves to illustrate the effect of conjugation on the action of a group on a set.

- We may define the distinguished faces as those on the top and bottom of the cube; then horizontal layer rotations contribute zero rotation at each corner, so the total corner rotation is zero. If a vertical slice is rotated, the four corners not on that slice have zero rotation, and the four involved corners have rotations of 1, 2, 1, and 2, whose sum is indeed 0 in $\mathbb{Z}/3\mathbb{Z}$. Thus, in all cases, $g$ belongs to the kernel of $\mathrm{rt}_{\mathbf{X}} \circ \pi_{\mathbf{X}}$.
- $g$ induces a 4-cycle on the corners and a 4-cycle on the edges; hence $\varepsilon(g) = 1$, which shows that $g$ lies in the kernel of $\varepsilon$.

This completes the proof of $\mathbf{Rub} \subseteq \mathbf{H}$. □

## 4 Solving Rubik's Cube

The algorithm described below[8] consists of:

- Placing the edges in their correct positions.
- Flipping them two at a time to orient them correctly.
- Placing the corners in their correct positions without disturbing the edges.
- Rotating the corners two at a time to orient them correctly.

With some thought, the first two steps and the last two can be combined.

- *Notations.* We denote the faces of the Rubik's Cube by $a$, $b$, $c$, $d$, $e$, and $f$. If $r$ is a face, we also denote by $r$ the quarter-turn rotation of the cube layer corresponding to face $r$ (clockwise, with the axis oriented from the center of the cube toward the center of face $r$). By definition, **Rub** is the subgroup of **G** generated by $a$, $b$, $c$, $d$, $e$, $f$, and if $r$ is a face, then $r^{-1}$ is the quarter-turn rotation of the corresponding layer of the cube in the counterclockwise direction (i.e., a quarter-turn opposite to $r$).

  If $r$ and $s$ are two faces that share an edge, we denote this edge by $y_{rs}$ (or $y_{sr}$), and if $r$, $s$, $t$ are three faces that share a corner, we denote this corner by $x_{rst}$ (or $x_{srt}$, etc.).

  We index the faces so that $(a, f)$, $(b, e)$, and $(c, d)$ form pairs of opposite faces, and such that $a$ sends $y_{ab} \to y_{ac}$, then $y_{ac} \to y_{ae}$, $y_{ae} \to y_{ad}$, and $y_{ad} \to y_{ab}$. The 8 corners are then: $x_{abc}$, $x_{ace}$, $x_{aed}$, $x_{adb}$, $x_{fcb}$, $x_{fec}$, $x_{fde}$, and $x_{fbd}$.
- *Placing the edges.* The placement of edges uses the element $(a^2b)^5$ from **Rub** and its conjugates. This element has the property of swapping $y_{ac}$ and $y_{ad}$ by rotating face $a$, while leaving all other edges fixed[9]. In particular, its image in $\mathbf{Perm}_{\mathbf{Y}}$ via $\sigma_{\mathbf{Y}} \circ \pi_{\mathbf{Y}}$ is the transposition of edges $y_{ac}$ and $y_{ad}$.

  Moreover, it is easy to verify that if $y$ and $y'$ are any two distinct elements of $Y$, then there exists some $g \in \mathbf{Rub}$ sending $y_{ac} \to y$ and $y_{ad} \to y'$. Then the image of $g(a^2b)^5g^{-1}$ under $\sigma_{\mathbf{Y}} \circ \pi_{\mathbf{Y}}$ is the transposition swapping $y$ and $y'$. It follows that $\sigma_{\mathbf{Y}} \circ \pi_{\mathbf{Y}}(\mathbf{Rub})$ contains all transpositions, and since these generate $\mathbf{Perm}_{\mathbf{Y}}$, this proves the following result.

[8] It is easier to follow with a Rubik's Cube in hand, but with a bit of determination, paper and pencil can suffice (though it's a pity to miss out on the existence of a physical version of the Rubik's group).

[9] The move $a^2b$ moves 7 edges, forming one cycle of length 5 and one of length 2; its 5th power therefore eliminates the 5-cycle, but it is somewhat miraculous that it does not flip any element of that cycle.

**Lemma 7.** The composition $\sigma_{\mathbf{Y}} \circ \pi_{\mathbf{Y}}$ induces a surjection from **Rub** onto $\mathbf{Perm}_{\mathbf{Y}}$.

- *Edge orientation.* The move $d^2fbd^{-1}$ flips $y_{ad}$ and leaves $y_{ac}$ fixed; thus the element

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

flips both $y_{ac}$ and $y_{ad}$ without affecting the other edges. If $y$ and $y'$ are two distinct elements of $Y$, and if $g \in \mathbf{Rub}$ sends $y_{ac} \to y$ and $y_{ad} \to y'$, then $ghg^{-1}$ flips $y$ and $y'$ without affecting the other edges. It follows that $\pi_{\mathbf{Y}}(\mathbf{Rub} \cap \ker(\sigma_{\mathbf{Y}} \circ \pi_{\mathbf{Y}}))$ contains the flips of any two edges. Since such elements generate the subgroup $\mathbf{Rot}^0_{\mathbf{Y}}$ of $\mathbf{Rot}_{\mathbf{Y}}$ consisting of total rotation zero (i.e., even numbers of edge flips), this proves the following:

**Lemma 8.** $\pi_{\mathbf{Y}}$ induces a surjection from $\mathbf{Rub} \cap \ker(\sigma_{\mathbf{Y}} \circ \pi_{\mathbf{Y}})$ onto $\mathbf{Rot}^0_{\mathbf{Y}}$.

- *Placing the corners.* Placing the corners uses the element $(b^{-1}a^{-1}ba)^3$ from **Rub**. This element has the property of fixing the edges—and therefore belongs to $\mathbf{Rub} \cap \mathbf{G}_{\mathbf{X}}$, and it swaps the corners $x_{abc}$ and $x_{fcb}$ (by swapping faces $a$ and $f$), and also $x_{adb}$ and $x_{dae}$ (by swapping faces $b$ and $e$), while leaving the others fixed. In particular, its image in $\mathbf{Perm}_{\mathbf{X}}$ is a product of two transpositions with disjoint support.

**Lemma 9.** If $x_1, x_2, x_3, x_4$ and $x'_1, x'_2, x'_3, x'_4$ are two families of four distinct elements of **X**, then there exists $g \in \mathbf{Rub}$ such that $\pi_{\mathbf{X}}(g) \cdot x_i = x'_i$ for[10] $i = 1, 2, 3, 4$.

*Proof.* It suffices to prove that one can map any family to a fixed family, for example: $x_{abc}, x_{fcb}, x_{adb}, x_{dae}$; indeed, if $g \cdot x_1 = x_{abc}$, $g \cdot x_2 = x_{fcb}$, $g \cdot x_3 = x_{adb}$, and $g \cdot x_4 = x_{dae}$, and likewise $g' \cdot x'_1 = x_{abc}$, $g' \cdot x'_2 = x_{fcb}$, $g' \cdot x'_3 = x_{adb}$, and $g' \cdot x'_4 = x_{dae}$, then $((g')^{-1}g) \cdot x_i = x'_i$ for $i = 1, 2, 3, 4$.

It is very easy to bring any two corners onto $x_{abc}$ and $x_{fcb}$, and since $d$ and $e$ fix $x_{abc}$ and $x_{fcb}$, we are reduced to proving that if $x \neq x'$ are two distinct corners from among $x_{abc}$ and $x_{fcb}$, there exists an element $g$ in the subgroup $\mathbf{G}_{d,e}$ of **Rub**, generated by $d$ and $e$, such that $g \cdot x = x_{adb}$ and $g \cdot x' = x_{dae}$.

Now, there exists $h \in \mathbf{G}_{d,e}$ such that $h \cdot x = x_{adb}$, and there are three cases:

- $h \cdot x' = x_{ade}$: take $g = h$.
- $h \cdot x' = x_{bdf}$: take $g = d^{-1}h$.
- $h \cdot x'$ is not on face $b$: then there exists $k$ such that $e^k \cdot (h \cdot x') = x_{ade}$, and take $g = e^k h$.

This completes the proof. □

**Lemma 10.** The image of $\mathbf{Rub} \cap \mathbf{G}_{\mathbf{X}}$ in $\mathbf{Perm}_{\mathbf{X}}$ is the subgroup $\mathbf{Alt}_{\mathbf{X}}$ of permutations of signature 1 (i.e., the alternating group on **X**).

*Proof.* The image is contained in $\mathbf{Alt}_{\mathbf{X}}$ because **Rub** is included in the kernel of $\varepsilon$, and an element of $\mathbf{G}_{\mathbf{X}}$ acts trivially on **Y**. Moreover, the properties of $(b^{-1}a^{-1}ba)^3$ show that its image in $\mathbf{Perm}_{\mathbf{X}}$ contains a product of two disjoint transpositions $(x_1, x_2)(x_3, x_4)$. Now, for any $g \in \mathbf{Rub}$, the element $g(b^{-1}a^{-1}ba)^3g^{-1}$ belongs to $\mathbf{Rub} \cap \mathbf{G}_{\mathbf{X}}$, and its image in $\mathbf{Perm}_{\mathbf{X}}$ is $(g \cdot x_1, g \cdot x_2)(g \cdot x_3, g \cdot x_4)$. Using the previous lemma, we deduce that the image contains all products of two disjoint transpositions. Since $|\mathbf{X}| > 5$, such products generate $\mathbf{Alt}_{\mathbf{X}}$, which completes the proof. □

[10] We say that **Rub** acts 4-transitively on **X**, or that the action of **Rub** on **X** is 4-transitive.

- *Orientation of the corners.* Let $\mathbf{Rot}_{\mathbf{X}}^0$ be the subgroup of $\mathbf{Rot}_{\mathbf{X}}$ consisting of elements of total rotation zero (i.e., the kernel of $\mathrm{rt}_{\mathbf{X}}$). We also have $\mathbf{Rot}_{\mathbf{X}}^0 = \mathbf{H} \cap \mathbf{Rot}_{\mathbf{X}}$, since an element of $\mathbf{Rot}_{\mathbf{X}}$ is already in the kernels of $\mathrm{rt}_{\mathbf{Y}} \circ \pi_{\mathbf{Y}}$ and $\varepsilon$.

  **Lemma 11.** We have $\mathbf{Rot}_{\mathbf{X}}^0 \subset \mathbf{Rub}$.

  *Proof.* Observe that the element $ede^{-1}d^{-1}e$ fixes $x_{abc}$, $x_{fcb}$, and $x_{adb}$, and rotates $x_{aed}$ by one third of a turn. Now, the element $(b^{-1}a^{-1}ba)^3$ belongs to $\mathbf{Rub} \cap \mathbf{G}_x$ and swaps the corners $x_{abc}$ and $x_{fcb}$, as well as $x_{adb}$ and $x_{dae}$, while fixing the others. It follows that

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

  is an element of $\mathbf{Rub} \cap \ker(\pi_{\mathbf{Y}})$ that fixes all corners except $x_{dae}$ and $x_{adb}$, each of which it rotates by one-third of a turn (in opposite directions, since the total rotation is zero). In other words, letting $x_1 = x_{adb}$ and $x_2 = x_{dae}$, this element is $(n_x)_{x \in \mathbf{X}}$ in $\mathbf{Rot}_{\mathbf{X}}^0$, with: $n_x = 0$ if $x \notin \{x_1, x_2\}$, and $n_{x_1} + n_{x_2} = 0$, and $n_{x_1} \neq 0$. Since $\mathbf{Rub}$ acts 4-transitively on $\mathbf{X}$ (and thus in particular 2-transitively), and since $ghg^{-1} = (n'_x)_{x \in \mathbf{X}}$ with $n'_x = n_{g \cdot x}$, if $h = (n_x)_{x \in \mathbf{X}}$, it follows that $\mathbf{Rub} \cap \mathbf{Rot}_{\mathbf{X}}^0$ contains all elements of this type. Because these generate $\mathbf{Rot}_{\mathbf{X}}^0$, we get $\mathbf{Rub} \cap \mathbf{Rot}_{\mathbf{X}}^0 = \mathbf{Rot}_{\mathbf{X}}^0$. This completes the proof. □

- *The inclusion* $\mathbf{H} \subseteq \mathbf{Rub}$. We can now prove the following result, which completes the proof of Theorem 5.

  **Proposition 12.** We have $\mathbf{H} \subseteq \mathbf{Rub}$.

  *Proof.* Let us begin by noting that since $\mathbf{Rub} \subseteq \mathbf{H}$, the product of an element of $\mathbf{Rub}$ and an element of $\mathbf{H}$ is still an element of $\mathbf{H}$. Let $h \in \mathbf{H}$.

  – Since $\sigma_{\mathbf{Y}} \circ \pi_{\mathbf{Y}}$ induces (cf. Lemma 7) a surjection from $\mathbf{Rub}$ onto $\mathbf{Perm}_{\mathbf{Y}}$, there exists $g_1 \in \mathbf{Rub}$ such that $\sigma_{\mathbf{Y}} \circ \pi_{\mathbf{Y}}(g_1) = \sigma_{\mathbf{Y}} \circ \pi_{\mathbf{Y}}(h)$, and then $h_1 = g_1^{-1}h$ is an element of $\mathbf{H}$ that lies in the kernel of $\sigma_{\mathbf{Y}} \circ \pi_{\mathbf{Y}}$.

  – By Lemma 8, there exists $g_2 \in \mathbf{Rub}$ such that $\pi_{\mathbf{Y}}(g_2) = \pi_{\mathbf{Y}}(h_1)$, and so $h_2 = g_2^{-1}h_1$ is an element of $\mathbf{H}$ that belongs to $\mathbf{G}_{\mathbf{X}}$.

  – We have $\varepsilon(h_2) = 1$, and since $h_2$ acts as the identity on $\mathbf{Y}$, the permutation $\sigma_{\mathbf{X}}(h_2)$ belongs to $\mathbf{Alt}_{\mathbf{X}}$. By Lemma 10, this implies there exists $g_3 \in \mathbf{Rub} \cap \mathbf{G}_{\mathbf{X}}$ such that $\sigma_{\mathbf{X}}(g_3) = \sigma_{\mathbf{X}}(h_2)$, and then $g_4 = g_3^{-1}h_2$ is an element of $\mathbf{H} \cap \mathbf{Rot}_{\mathbf{X}}$. Now, $\mathbf{H} \cap \mathbf{Rot}_{\mathbf{X}} = \mathbf{Rot}_{\mathbf{X}}^0$, which is included in $\mathbf{Rub}$ by Lemma 11; thus $g_4 \in \mathbf{Rub}$.

  – Since $h = g_1g_2g_3g_4$, it follows that $h \in \mathbf{Rub}$, which completes the proof.

  □