Groups in the Rubik's Cube

III. Subgroups of the Legal Rubik's Cube Group

Andrew R. Kozlik

MFF UK

Fall School of Algebra 2014

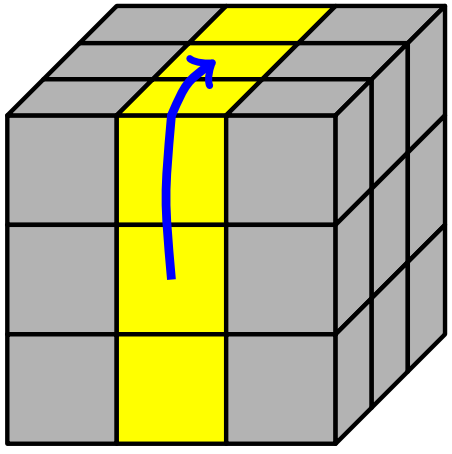
Cyclic subgroups

The Rubik's cube group contains cyclic subgroups of 73 different orders.

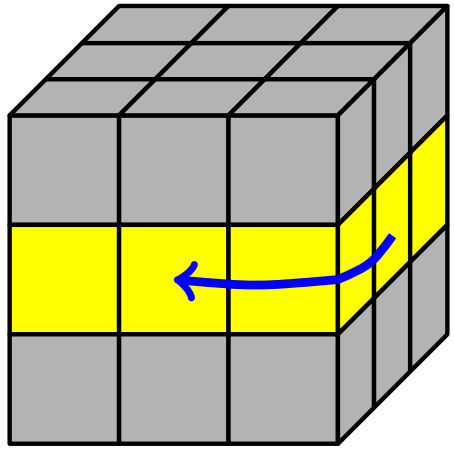
Example

- $\langle R \rangle \simeq \mathbb{Z}_4$
- $\langle R^2 U^2 \rangle \simeq \mathbb{Z}_6 \gtrsim \mathbb{Z}_3$
- $\langle RU^{-1} \rangle \simeq \mathbb{Z}_{63} \gtrsim \mathbb{Z}_{21} \gtrsim \mathbb{Z}_7$
- $\langle RU \rangle \simeq \mathbb{Z}_{105} \gtrsim \mathbb{Z}_5$
- The largest cyclic subgroup of G has order 1260, $\langle RU^2 D^{-1} B D^{-1} \rangle \simeq \mathbb{Z}_{1260}$.

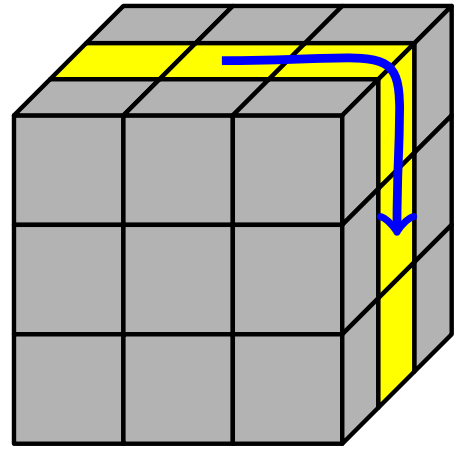
Middle slice moves



M_R

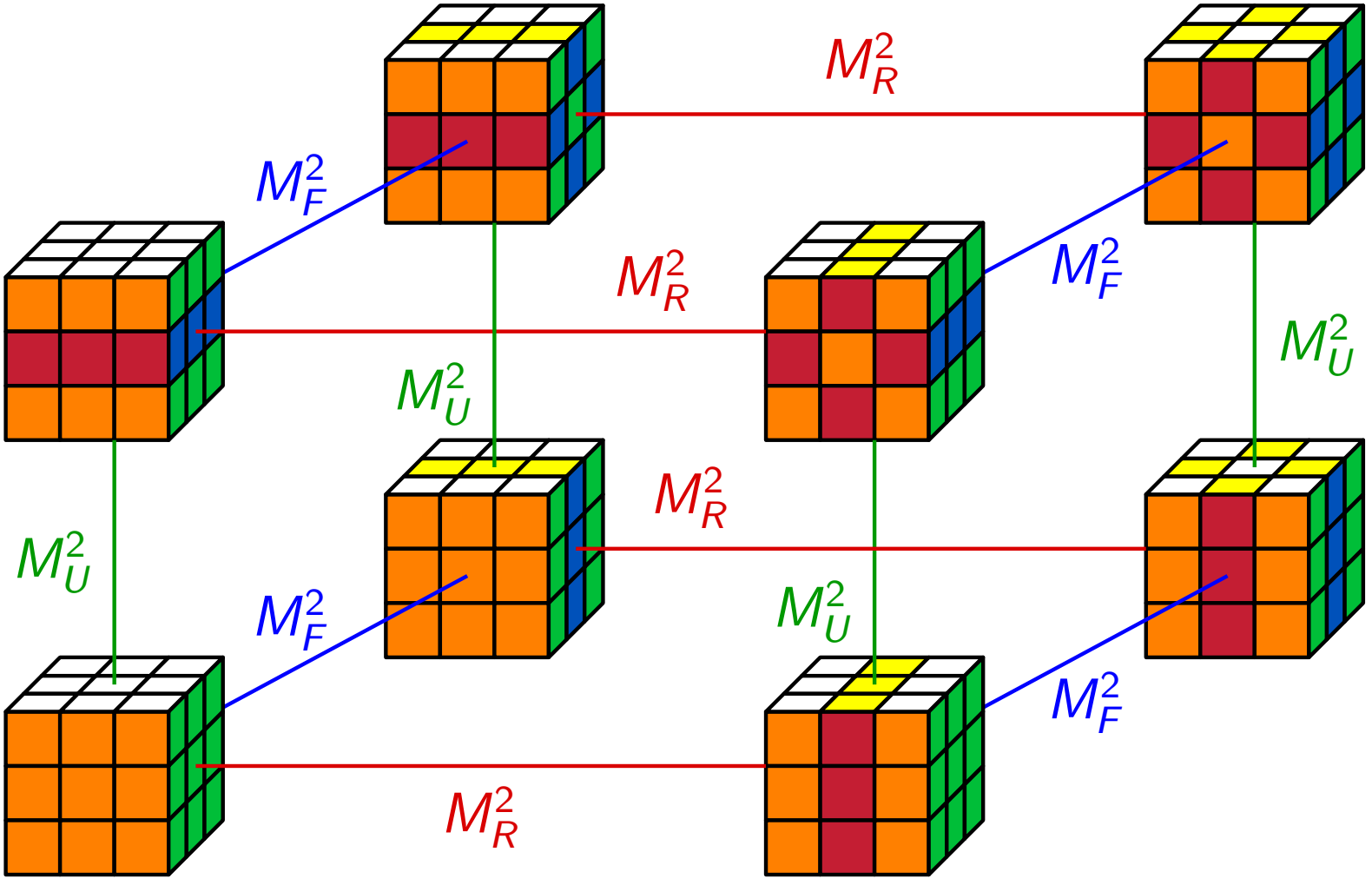


M_U



M_F

Slice square group $\langle M_R^2, M_U^2, M_F^2 \rangle$



$\langle M_R^2, M_U^2, M_F^2 \rangle \simeq \mathbb{Z}_2^3$

The two squares group

Definition

The group $\langle R^2, U^2 \rangle$ is called the *two squares* group.

Fact

The dihedral group of order 12 has presentation

$$D_6 = \langle\, a, b \mid a^6 = 1,\ b^2 = 1,\ abab = 1 \,\rangle.$$

Proposition

The two squares group is isomorphic to D_6.

Proof.

Let $a = R^2U^2$ and $b = R^2$. Then

- $\langle a, b \rangle = \langle R^2, U^2 \rangle$ is of order 12 and
- a and b satisfy the relations given above.

Quaternion group

Definition

The group

$$Q = \{\pm 1, \pm i, \pm j, \pm k\}, \quad \textit{where} \quad i^2 = j^2 = k^2 = ijk = -1,$$

is called the *quaternion group*.

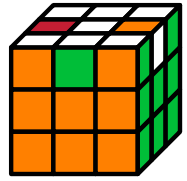
Fact

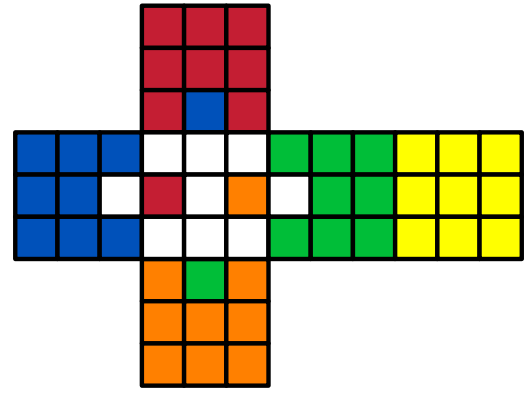
The quaternion group has presentation

$$Q = \langle\, a, b \mid a^2 = b^2,\ aba = b \,\rangle.$$

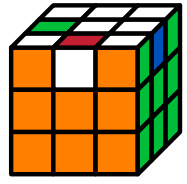
Quaternion group $Q = \langle a, b \mid a^2 = b^2,\ aba = b \rangle$

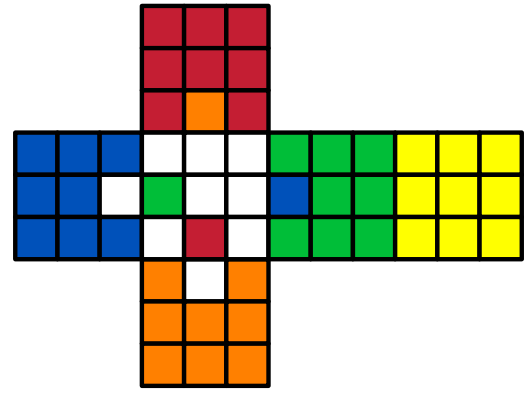
$a = F^2 M_R U^{-1} M_R^{-1} U^{-1} M_R U M_R^{-1} U F^2$



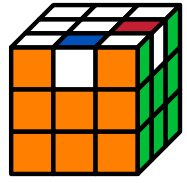


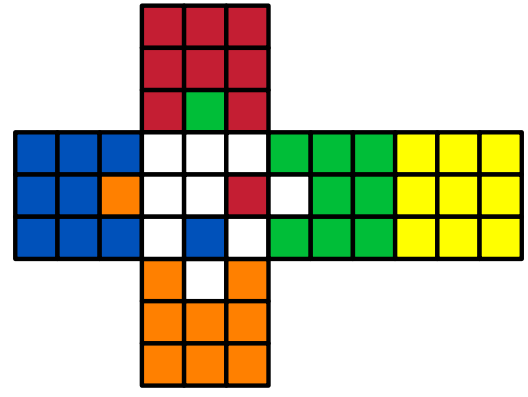
$b = F U^2 F^{-1} U^{-1} L^{-1} B^{-1} U^2 B U L$



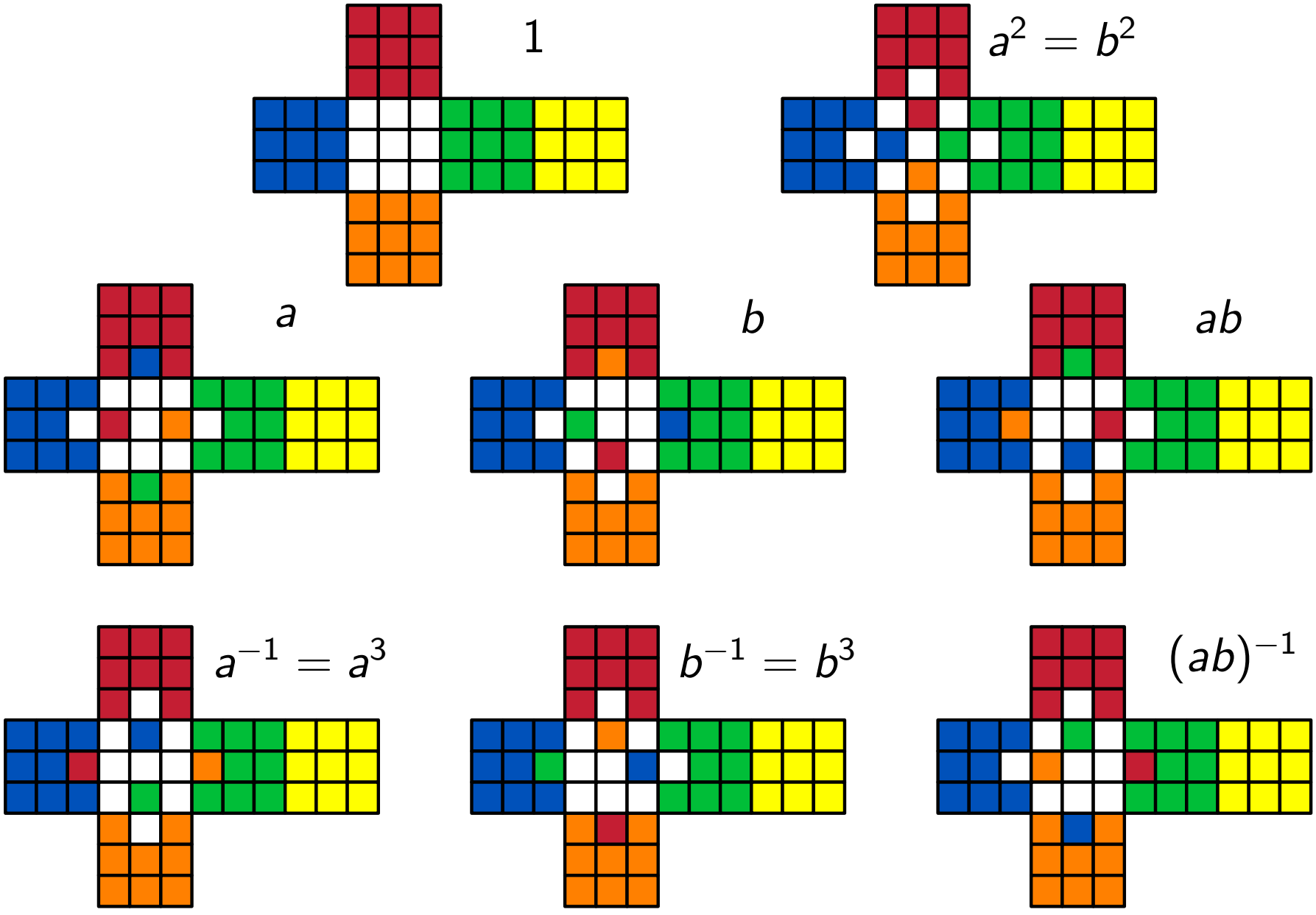


$a \cdot b$





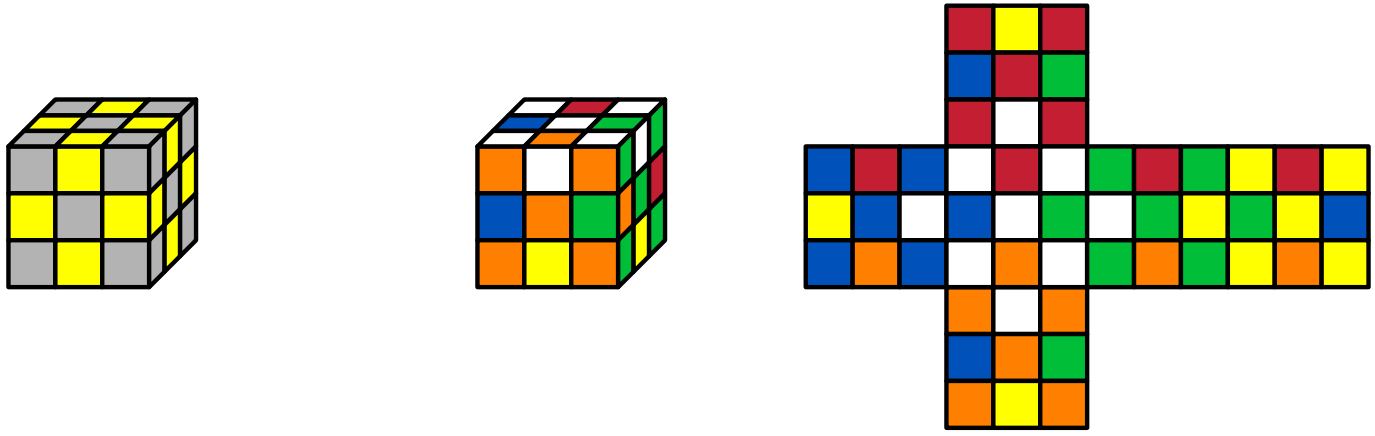
Quaternion group $Q = \langle a, b \mid a^2 = b^2,\ aba = b \rangle$



The superflip

The *superflip* is a configuration of the Rubik's cube such that

- all subcubes are in their solved positions,
- the corner pieces are correctly oriented,
- every edge piece is flipped.



Theorem (Reid, 1995)

The superflip requires 20 face moves to solve.

Example

$U\ R^2\ F\ B\ R\ B^2\ R\ U^2\ L\ B^2\ R\ U^{-1}\ D^{-1}\ R^2\ F\ R^{-1}\ L\ B^2\ U^2\ F^2$

The superflip is as hard as it gets

Theorem (Rokicki, Kociemba, Davidson, Dethridge, 2010)

Every valid configuration of the Rubik's cube can be solved in 20 face moves or less.

Proof.

Some group theory and 35 CPU-years of idle computer time donated by Google. □

Fundamental theorem of cube theory

Theorem

Let $\mathbf{v} \in \mathbb{Z}_3^8$, $\mathbf{w} \in \mathbb{Z}_2^{12}$, $r \in S_V$, $s \in S_E$. *Then* $(\mathbf{v}, r, \mathbf{w}, s)$ *corresponds to a legal move of the Rubik's cube if and only if all of the following conditions hold:*

(P) $\operatorname{sgn}(r) = \operatorname{sgn}(s)$,

(F) $w_1 + \cdots + w_{12} \equiv 0 \pmod 2$,

(T) $v_1 + \cdots + v_8 \equiv 0 \pmod 3$.

If we represent two elements of G as

$$(\mathbf{v}, r, \mathbf{w}, s), (\mathbf{v}', r', \mathbf{w}', s') \in \mathbb{Z}_3^8 \times S_V \times \mathbb{Z}_3^8 \times S_E$$

then the group operation is be given by

$$(\mathbf{v}, r, \mathbf{w}, s) \cdot (\mathbf{v}', r', \mathbf{w}', s') = (\mathbf{v} + P(r)\mathbf{v}', rr', \mathbf{w} + P(s)\mathbf{w}', ss'),$$

where $P(r)$ and $P(s)$ are permutation matrices corresponding to r and s.

The center of the Rubik's cube group

Definition

The *center* of a group G, denoted $Z(G)$, is the set of elements that commute with every element of G, i.e.

$$Z(G) = \{ z \in G : \forall g \in G, zg = gz \}.$$

Proposition

The center of the Rubik's cube group consists of two elements: the identity and the superflip element.

Proof.

- Let $G = \langle L, R, F, B, U, D \rangle$ be the Rubik's cube group.
- For any $g \in G$ denote the corresponding 4-tuple by $(\mathbf{v}_g, r_g, \mathbf{w}_g, s_g)$.

Proof (continued).

- Let $z \in Z(G)$.
- For any $g \in G$ we have
  $(\mathbf{v}_g, r_g, \mathbf{w}_g, s_g)\cdot(\mathbf{v}_z, r_z, \mathbf{w}_z, s_z) = (\mathbf{v}_z, r_z, \mathbf{w}_z, s_z)\cdot(\mathbf{v}_g, r_g, \mathbf{w}_g, s_g)$.
  That is

$$(\mathbf{v}_g + P(r_g)\mathbf{v}_z,\ r_g r_z,\ \mathbf{w}_g + P(s_g)\mathbf{w}_z,\ s_g s_z)$$
$$=(\mathbf{v}_z + P(r_z)\mathbf{v}_g,\ r_z r_g,\ \mathbf{w}_z + P(s_z)\mathbf{w}_g,\ s_z s_g).$$

- $r_g r_z = r_z r_g$ for all $g \in G$ implies $r_z = \mathrm{id}$.
- $s_g s_z = s_z s_g$ for all $g \in G$ implies $s_z = \mathrm{id}$.
- $\mathbf{v}_g + P(r_g)(\mathbf{v}_z) = \mathbf{v}_z + \mathbf{v}_g$ for all $g \in G$ implies that $\mathbf{v}_z$ is invariant under permutation of its coordinates.
- $\mathbf{w}_g + P(s_g)(\mathbf{w}_z) = \mathbf{w}_z + \mathbf{w}_g$ for all $g \in G$ implies that $\mathbf{w}_z$ is invariant under permutation of its coordinates.

Proof (continued).

- $\mathbf{v}_z \in \{(0,0,\ldots,0),(1,1,\ldots,1),(2,2,\ldots,2)\} \subset \mathbb{Z}_3^8$
- $\mathbf{w}_z \in \{(0,0,\ldots,0),(1,1,\ldots,1)\} \subset \mathbb{Z}_2^{12}$
- By the fundamental theorem, $(\mathbf{v}_z, \mathrm{id}, \mathbf{w}_z, \mathrm{id})$ corresponds to a legal move if and only if
  - the coordinates of $\mathbf{v}_z$ sum up to 0 modulo 3 and
  - the coordinates of $\mathbf{w}_z$ sum up to 0 modulo 2.
- Thus $\mathbf{v}_z = \mathbf{0}$.
- The center of G consists of
  1. $(\mathbf{0}, \mathrm{id}, (0,0,\ldots,0), \mathrm{id})$ and
  2. $(\mathbf{0}, \mathrm{id}, (1,1,\ldots,1), \mathrm{id})$.

The slice group H

Definition

The group $H = \langle M_R, M_U, M_F \rangle$ is called the *slice group* of the Rubik's cube.

Questions

- *Does H act transitively on the center pieces of the cube?*
  Yes.
- *Does H act transitively on the edge pieces of the cube?*
  No.
- *What are the orbits of the edge pieces under the action of H?*
  The edge pieces fall into three orbits E_{LR}, E_{UD}, E_{FB} corresponding to the three slices.

The action of H on the subcubes

- Denote by C the set of all center pieces.
- Each element of H determines a permutation of E_{LR}, E_{UD}, E_{FB} and C.
- The permutation of E_{LR} can be characterised by an element of $\mathbb{Z}_4$. (The same goes for permutations of E_{UD} and E_{FB}.)
- The permutation of C is equivalent to a rotational symmetry of a cube.
  Therefore it can be characterised by an element of S_4.
- Thus we have a homomorphism
$$f : H \to \mathbb{Z}_4^3 \times S_4.$$
- *Is f injective?*

  (In other words, does the permutation of the subcubes determine their orientation uniquely?)

  Yes.

The order of H

Lemma

The order of the slice group is at least 768.

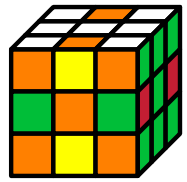
Proof.

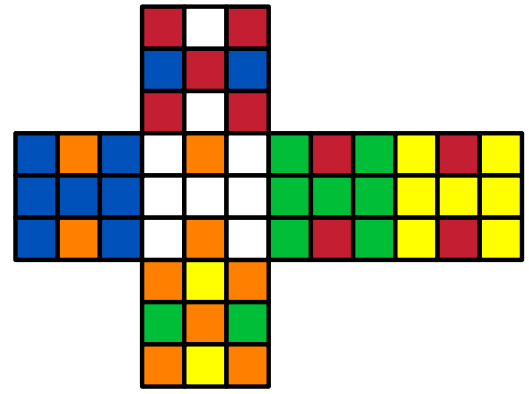
- The natural projection $p : H \to S_4$ is surjective.
- By the first isomorphism theorem $H/\ker p \simeq S_4$.
- There exists a subgroup $\langle g_1, g_2, g_3 \rangle \leq \ker p$ of order 32. (See next slide for details.)
- Thus $|H| = |S_4| \cdot |\ker p| \geq 24 \cdot 32 = 768$.

The subgroup $\langle g_1, g_2, g_3 \rangle \leq \ker p$ of order 32

$g_1 = M_R M_F M_U M_F^{-1}$

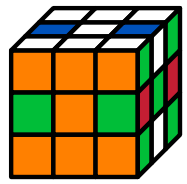
$f(g_1) = (1, 1, 0, \mathrm{id})$

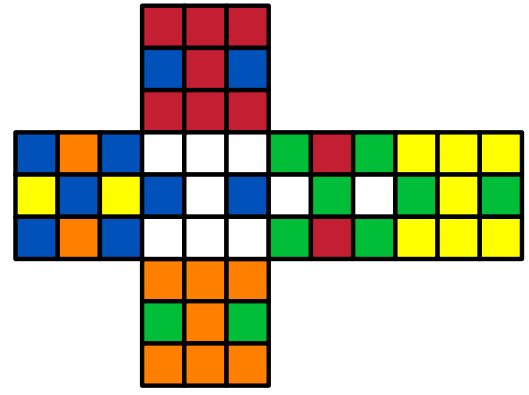




$g_2 = M_F M_R^{-1} M_U M_R$

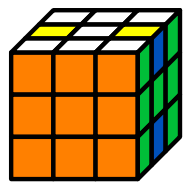
$f(g_2) = (0, 1, 1, \mathrm{id})$

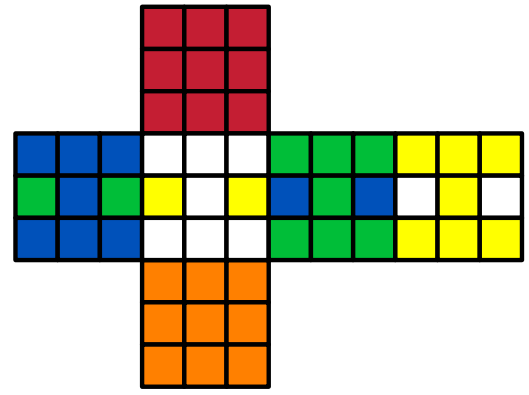




$g_3 = M_F M_U^{-1} M_R^{-1} M_U M_F M_U M_R M_U^{-1}$

$f(g_3) = (0, 0, 2, \mathrm{id})$





The slice group

Theorem

Let $s : \mathbb{Z}_4^3 \times S_4 \to \{\pm 1\}$ *be a homomorphism such that*

$$s : (x, y, z, w) \mapsto (-1)^{x+y+z} \cdot \operatorname{sgn}(w).$$

Then H *is isomorphic to* $\ker s$.

Proof.

- Observe that
$$s(f(M_R)) = 1, \quad s(f(M_U)) = 1, \quad s(f(M_F)) = 1.$$
Thus $f(H) \subseteq \ker s$.
- The kernel of s has order 768, since $4^3 \cdot 4!/|\ker s| = 2$.
- We know that H has order at least 768.
- Therefore $f(H) = \ker s$.
- Since f is injective, $H \simeq \ker s$.

The slice group

Corollary

The order of the slice group is 768.

Corollary

An element $(x, y, z, w) \in \mathbb{Z}_4^3 \times S_4$ *corresponds to an element of the slice group if and only if* $(-1)^{x+y+z} = \mathrm{sgn}(w)$.