Lecture 21:
Rubik's Cube: Subgroups of the Cube Group

Contents

In this lecture, we consider various collections of moves on Rubik's cube and determine the subgroups they generate. We also see what the Fundamental Theorem of Cubology tells us about the structure of the group operation on RC_3 and we show the only move sequence that commutes with *ever* other move sequence is the *superflip*.

21.1 Building Big Groups from Smaller Ones

Starting with a collection of groups we can stick them together to form a new, larger group.

Given a finite collection of groups $G_1, G_2, \dots G_n$, the **direct product** of $G_1, G_2, \dots G_n$ is

$$G_1 \oplus G_2 \cdots \oplus G_n = \{(g_1, g_2, \dots, g_n) \mid g_i \in G_i\}$$

which is a group under the operation:

$$(g_1, g_2, \dots, g_n)(h_1, h_2, \dots, h_n) = (g_1h_1, g_2h_2, \dots, g_nh_n).$$

It is understood that each product g_ih_i is performed with the operation of group G_i.

To see why $G_1 \oplus G_2 \cdots \oplus G_n$ is a group under this operation we observe:

1) It is closed since each G_i is closed under its operation.

2) The operation is associative since the operations on each of the G_i's is associative.

3) The identity is $(e_1, e_2, \dots, e_n)$ where each e_i is the identity of G_i.

4) The inverse of an element $(g_1, g_2, \dots, g_n)$ is $(g_1^{-1}, g_2^{-1}, \dots, g_n^{-1})$.

Example 21.1 *The direct product of* S_3 *and* C_5 *consists of* $3! \cdot 5 = 30$ *elements. For example* $((1,3,2),4)$*, and* $((1,2),3)$ *are two elements in* $S_3 \oplus C_5$*. The product of these elements is*

$$((1,3,2),4)\ ((1,2),3) = ((1,3,2)(1,2), 4+3) = ((1,3),2).$$

For simplicity let's just limit our attention to the direct product of two groups: $G \oplus H$. The subset

$$G \oplus \{e_H\} := \{(g, e_H) \mid g \in G\}$$

is a subgroup of $G \oplus H$ which essentially a copy of G. Similarly,

$$\{e_G\} \oplus H := \{(e_G, h) \mid h \in H\}$$

is a subgroup of $G \oplus H$ which essentially a copy of H, In other words, we have used G and H to build a bigger group $G \oplus H$ in which G and H are subgroups.

Example 21.2 *The group* $C_2^3 := C_2 \oplus C_2 \oplus C_2$ *is a group of order* 8*, and every non-identity elements have order* 2.

The group $C_2 \oplus C_3$ *is a cyclic group of order* 6*, since the element* $(1, 1)$ *has order* 6 *(check this).*

$$C_2 \oplus C_3 = \{(0, 0), (0, 1), (0, 2), (1, 0), (1, 1), (1, 2)\}.$$

For a group G, we denote the direct product with itself n-times, $G \oplus G \cdots \oplus G$, by G^n.

21.2 Some Subgroups of RC_3

In this section we investigate some of the types of groups that appear as subgroups of the Rubik's cube. In Chemistry, one my be interested in what elements make up a compound. As an analogy, think of the Rubik's cube group as the "compound", and the "elements" that make it up are the subgroups. We'd like to see what kinds of groups live inside RC_3.

It is particularly interesting to "realize" a finite group A as a subgroup of the cube. This can be done for all groups of order < 13; the smallest abelian group which is not a subgroup of RC_3 is C_{13} (since $13 \nmid |RC_3|$, and the smallest non-abelian group is D_{13}. In the next few sections, we'll see a few examples of some groups that live inside RC_3.

21.2.1 Cyclic subgroups and orders of elements in RC_3

The easiest type of subgroup to look for are the cyclic subgroups. Since the order of an element is precisely the size of the cyclic group it generates then we are really just interested in what are the possible orders of elements in RC_3.

An element of order 4 is R. So RC_3 contains a cyclic group of order 4 as a subgroup: $C_4 = \langle R \rangle$.

The move sequence R^2U^2 has order 6, so RC_3 contains as cyclic subgroup of order 6: $C_6 = \langle R^2U^2 \rangle$.

The move sequence RU has order 105 and the move sequence RU^{-1} has order 63. Therefore, RC_3 contains copies of C_{63} and and C_{105} as subroups.

SAGE

```
sage: S48=SymmetricGroup(48)
sage: R=S48("(25,27,32,30)(26,29,31,28)(3,38,43,19)(5,36,45,21)(8,33,48,24)")
sage: L=S48("(9,11,16,14)(10,13,15,12)(1,17,41,40)(4,20,44,37)(6,22,46,35)")
sage: U=S48("(1,3,8,6)(2,5,7,4)(9,33,25,17)(10,34,26,18)(11,35,27,19)")
sage: D=S48("(41,43,48,46)(42,45,47,44)(14,22,30,38)(15,23,31,39)(16,24,32,40)")
sage: F=S48("(17,19,24,22)(18,21,23,20)(6,25,43,16)(7,28,42,13)(8,30,41,11)")
sage: B=S48("(33,35,40,38)(34,37,39,36)(3,9,46,32)(2,12,47,29)(1,14,48,27)")
sage: RC3=S48.subgroup([R,L,U,D,F,B])
sage: (R*U).order()
105
sage: (R*U^(-1)).order()
63
```

There exist precisely 73 different orders of elements in RC_3 and the maximum order is 1260. The move sequence $RU^2D^{-1}BD^{-1}$ has order 1260.

21.2.2 Two Squares Group: $\langle R^2, U^2\rangle$

Let $H = \langle R^2, U^2\rangle$ denote the group generated by the square moves R^2 and U^2. The group contains the useful 2-pair edge swap: $(R^2U^2)^3$.

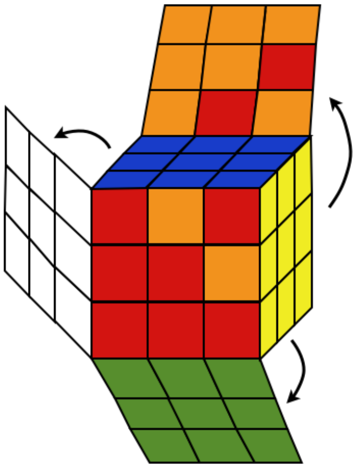

Figure 1: The two pair edge swap $(R^2U^2)^3$ in $H = \langle R^2, U^2\rangle$.

We can find all the elements of this group fairly easily:

$$\begin{aligned} H =&\{1, R^2, R^2U^2, R^2U^2R^2, (R^2U^2)^2, (R^2U^2)^2R^2, (R^2U^2)^3, \\ &(R^2U^2)^3R^2, (R^2U^2)^4, (R^2U^2)^4R^2, (R^2U^2)^5, (R^2U^2)^5R^2\}, \end{aligned}$$

Therefore, $|H| = 12$. Note that $1 = (R^2U^2)^6$, $U^2 = (R^2U^2)^5R^2$, and $U^2R^2 = (R^2U^2)^5$.

We can compute the order of each element one by one and see that the maximum order is 6. This can also be done quickly in SAGE.

SAGE

```
sage: S48=SymmetricGroup(48)
sage: R=S48("(25,27,32,30)(26,29,31,28)(3,38,43,19)(5,36,45,21)(8,33,48,24)")
sage: L=S48("(9,11,16,14)(10,13,15,12)(1,17,41,40)(4,20,44,37)(6,22,46,35)")
sage: U=S48("(1,3,8,6)(2,5,7,4)(9,33,25,17)(10,34,26,18)(11,35,27,19)")
sage: D=S48("(41,43,48,46)(42,45,47,44)(14,22,30,38)(15,23,31,39)(16,24,32,40)")
sage: F=S48("(17,19,24,22)(18,21,23,20)(6,25,43,16)(7,28,42,13)(8,30,41,11)")
sage: B=S48("(33,35,40,38)(34,37,39,36)(3,9,46,32)(2,12,47,29)(1,14,48,27)")
sage: RC3=S48.subgroup([R,L,U,D,F,B])
sage: H=S48.subgroup([R^2,U^2])
sage: [g.order() for g in H]
[1, 2, 2, 2, 2, 3, 2, 6, 2, 3, 2, 6]
```

We've just discovered that H is a group of order 12, with two elements of order 6, two elements of order 3, and seven elements of order 2. This seems eerily reminiscent of the dihedral group D_6. Let check to see H is really D_6 in disguise.

SAGE

```
sage: H.is_isomorphic(DihedralGroup(6))
True
```

It is! We've just discovered that the dihedral group D_6 lives inside the Rubik's cube group. [1]

21.2.3 The Slice Squared Group: $\langle S\ell_R^2, S\ell_U^2, S\ell_F^2\rangle$

Let $H = \langle S\ell_R^2, S\ell_U^2, S\ell_F^2\rangle$ denote the group generated by the square slice moves.

Each of the generators $S\ell_R^2, S\ell_U^2, S\ell_F^2$ has order 2, and each of the products

$$S\ell_R^2 S\ell_F^2, \quad S\ell_R^2 S\ell_U^2, \quad S\ell_F^2 S\ell_U^2$$

has order 2 also (play with your cube to see this). This means that H is an abelian group where *every* element has order 2.

For simplicity of notation let $a = S\ell_R^2$, $b = S\ell_F^2$ and $c = S\ell_U^2$ then it is straightforward to see that:

$$H = \{1, a, b, c, ab, ac, bc, abc\},$$

is a group of order 8. In fact, $H \approx C_2 \oplus C_2 \oplus C_2$ under the correspondence

$$\begin{aligned} 1 &\leftrightarrow (0,0,0) \\ a &\leftrightarrow (1,0,0) \\ b &\leftrightarrow (0,1,0) \\ c &\leftrightarrow (0,0,1) \\ ab &\leftrightarrow (1,1,0) \\ ac &\leftrightarrow (1,0,1) \\ bc &\leftrightarrow (0,1,1) \\ abc &\leftrightarrow (1,1,1) \end{aligned}$$

21.3 Structure of the Cube Group RC_3

Let X and Y be two elements of RC_3 with corresponding position vectors $(\rho, \sigma, \boldsymbol{v}, \boldsymbol{w})$ and $(\rho^*, \sigma^*, \boldsymbol{v}^*, \boldsymbol{w}^*)$, respectively.

Recall, this notation means that corner cubie i moved to cubicle $\rho(i)$ and v_i is the label on the sticker beneath the primary faced labeled "+", and edge cubie i moved to edge cubicle $\sigma(i)$ with label w_i on the sticker in the primary facet labeled "+". If we compose the moves X and Y then the position vector of XY can be obtained as follows:

- corner cubie i moves to $(\rho\rho^*)(i) = \rho^*(\rho(i))$,
- edge cubie i moves to $(\sigma\sigma^*)(i) = \sigma^*(\sigma(i))$,
- the label on the i^{th} corner cubie, which is in the primary facet of the cubicle to which it was moved, is $v_i + v^*_{\rho(i)} \pmod 3$.
- the label on the i^{th} edge cubie, which is in the primary facet of the cubicle to which it was moved, is $w_i + w^*_{\sigma(i)} \pmod 2$.

---

[1] We say two groups G_1 and G_2 are **isomorphic** if they have the same group structure (i.e. same Cayley table), but the names of the elements could be different. More precisely, we mean there is a map $\phi : G_1 \to G_2$ which is a bijection, and for any $g, h \in G_2$, $\phi(gh) = \phi(g)\phi(h)$. SAGE has built in functionality for checking whether two groups are really the same (i.e. isomorphic).

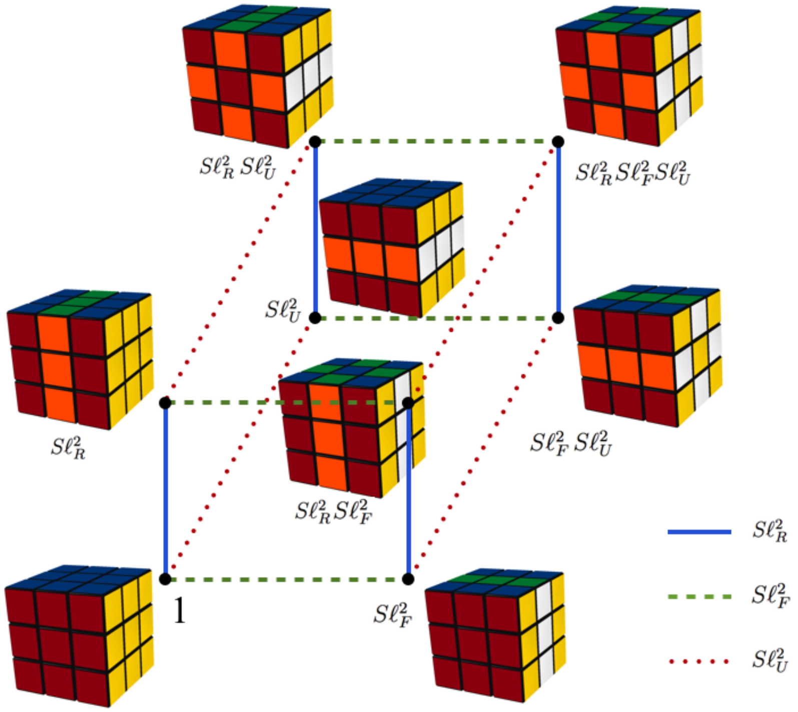

Figure 2: Cayley graph of H: The elements in the sliced squared group and their representations in terms of the generators.

If we define addition of 8-tuple (and 12-tuple) orientation vectors componentwise: i.e. $\boldsymbol{a}+\boldsymbol{b} = (a_1, a_2, \ldots, a_k) + (b_1, b_2, \ldots, b_k) = (a_1 + b_1, a_2 + b_2, \ldots, a_k + b_k)$ (i.e. think $C_3^8 = C_3 \oplus C_3 \oplus \cdots \oplus C_3$ and $C_2^{12} = C_2 \oplus C_2 \oplus \cdots \oplus C_2$) then the group operation on $RC_3 = S_8 \times S_{12} \times C_3^8 \times C_2^{12}$ is:

$$(\rho, \sigma, \boldsymbol{v}, \boldsymbol{w})(\rho^*, \sigma^*, \boldsymbol{v}^*, \boldsymbol{w}^*) = (\rho\rho^*, \sigma\sigma^*, \boldsymbol{v} + \rho(\boldsymbol{v}^*), \boldsymbol{w} + \sigma(\boldsymbol{w}^*)) \tag{1}$$

where $\rho(\boldsymbol{v}^*)$ represents the orientation vector obtained from $\boldsymbol{v}^*$ by replacing the i^{th} component v_i with $v_{\rho(i)}$:

$$\rho(\boldsymbol{v}^*) = \rho((v_1^*, v_2^*, \ldots, v_8^*)) = (v_{\rho(1)}^*, v_{\rho(2)}^*, \ldots, v_{\rho(8)}^*).$$

and $\sigma(\boldsymbol{w}^*)$ represents:

$$\sigma(\boldsymbol{w}^*) = \sigma((w_1^*, w_2^*, \ldots, w_{12}^*)) = (w_{\sigma(1)}^*, w_{\sigma(2)}^*, \ldots, w_{\sigma(12)}^*).$$

Let

$$G_1 = \{g = (\rho.\sigma, \boldsymbol{v}, \boldsymbol{w}) \in RC_3 \mid \boldsymbol{v} = \boldsymbol{0}, \boldsymbol{w} = \boldsymbol{0}\}$$
$$G_2 = \{g = (\rho.\sigma, \boldsymbol{v}, \boldsymbol{w}) \in RC_3 \mid \rho = \varepsilon, \sigma = \varepsilon\}.$$

Then G_1 and G_2 are subgroups of RC_3. G_1 is the subgroup of all move sequences which preserves the orientation of all the pieces. G_2 is the subgroup of all move sequences which leaves every cubie in its own cubicle, but may flip/twist the cubies.

The following theorem describes how the subgroups G_1 and G_2 are interlinked in order to form RC_3. Some of the terms are not explained as it is a more advanced theorem. I include it here only for the benefit of those who know about: normal subgroups, isomorphisms, and semidirect products.

Theorem 21.1

(a) G_1 *is a subgroup,* G_2 *is a normal subgroup of* RC_3. [2]

(b) $G_1 \approx \{(\rho,\sigma) \in S_8 \times S_{12} \mid \textit{sign}(\rho) = \textit{sign}(\sigma)\}$, $G_2 \approx C_8^7 \times C_2^{11}$.

(c) RC_3 *is the semidirect product of* G_1 *with* G_2.

21.3.1 The Centre of the Cube group, $Z(RC_3)$, and the Superflip

Recall that for any group G, the **centre** of G, denoted by $Z(G)$ is the set of all elements that commute with every element of G:

$$Z(G) = \{a \in G \mid ag = ga \text{ for all } g \in G\}.$$

The centre is a subgroup of G. (See Section 11.3)

Theorem 21.2 *The centre of* RC_3 *consists of two elements: the identity* ε *and the superflip* X_{SF}. *The superflip, is the configuration in which every cubie is in its home location but all the edge cubies are flipped (see Figure 3).*

$$Z(RC_3) = \{\varepsilon.X_{SF}\}.$$

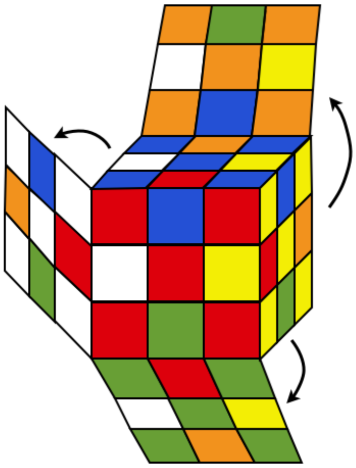

Figure 3: The superflip configuration of Rubik's cube: X_{SF}.

Proof: Let $g = (\rho, \sigma, \boldsymbol{v}, \boldsymbol{w}) \in Z(RC_3)$. Since the centre of the symmetric group S_n, for $n \geq 3$, is trivial and since every $\rho^* \in S_8$ appears as a first coordinate of the position vector, it immediately follows from Equation 1 that $\rho = \varepsilon$, and similarly $\sigma = \varepsilon$. That is, $g = (\varepsilon, \varepsilon, \boldsymbol{v}, \boldsymbol{w}) \in G_2$. Thus, $gg^* = g^*g$ simply becomes $\boldsymbol{v} + \boldsymbol{v}^* = \boldsymbol{v}^* + \rho^*(\boldsymbol{v})$, i.e. $\boldsymbol{v} = \rho^*(\boldsymbol{v})$ for all $\rho^* \in S_8$, and $\boldsymbol{w} + \boldsymbol{w}^* = \boldsymbol{w}^* + \sigma^*(\boldsymbol{w})$, i.e. $\boldsymbol{w} = \sigma^*(\boldsymbol{w})$ for all $\sigma^* \in S_{12}$. This means the $\boldsymbol{v}$ and $\boldsymbol{w}$ are constant (i.e. $v_i = v_j$ for all $1 \leq i,j \leq 8$ and $w_i = w_j$ for all $1 \leq i,j \leq 12$). So we have

$$\boldsymbol{v} = (0,0,0,0,0,0,0,0) = \mathbf{0} \quad \text{or} \quad \boldsymbol{v} = (1,1,1,1,1,1,1,1) = \mathbf{1} \quad \text{or} \quad \boldsymbol{v} = (2,2,2,2,2,2,2,2) = \mathbf{2}$$

and

$$\boldsymbol{w} = (0,0,0,0,0,0,0,0,0,0,0,0) = \mathbf{0} \quad \text{or} \quad \boldsymbol{w} = (1,1,1,1,1,1,1,1,1,1,1,1) = \mathbf{1}.$$

The first fundamental theorem of cubology excludes the cases $\boldsymbol{v} = \mathbf{1}, \mathbf{2}$, therefore $\boldsymbol{v} = \mathbf{0}$. Both choices for $\boldsymbol{w}$ are possible. This means g is either $(\varepsilon, \varepsilon, \mathbf{0}, \mathbf{0})$ or $(\varepsilon, \varepsilon, \mathbf{0}, \mathbf{1})$. Therefore,

$$Z(RC_3) = \{(\varepsilon, \varepsilon, \mathbf{0}, \mathbf{0}), (\varepsilon, \varepsilon, \mathbf{0}, \mathbf{1})\}.$$

---

[2] A **normal subgroup** is a subgroup H of a group G with the property that all its left and right cosets are equal: $aH = Ha$ for all $a \in G$. Such subgroups are extremely important in advanced group theory.

The configuration $(\varepsilon, \varepsilon, \mathbf{0}, \mathbf{1})$ is the superflip. □

21.4 Exercises

1. Consider the direct product $S_3 \oplus D_4$ of the symmetric group and the dihedral group.
   - (a) How many elements does $S_3 \oplus D_4$ have. That is, what is $|S_3 \oplus D_4|$.
   - (b) Find the product of $((1,3), H)$ and $((1,2,3), R_{90})$.
   - (c) What is the order of the element $((1,3), H)$?
   - (d) What is the order of the element $((1,2,3), R_{90})$?
2. Show that $C_3 \oplus C_5$ is a cyclic group of order 15.
   (Hint: What is the order of the element $(1,1)$?)
3. Is $C_2 \oplus C_6$ a cyclic group? Explain.