

# Algebra of the 2x2x2 Rubik's Cube

Under the direction of Dr. John S. Caughman

William Brad Benjamin

## 1. Introduction

As children, many of us spent countless hours playing with Rubik's Cube. At the time, it seemed like little more than a fascinating and slightly frustrating puzzle. While taking courses in abstract algebra, I – as many others – started thinking of how to organize the puzzle as an algebraic structure. I had little success. Once an orientation for the cube is determined, the first thing one will notice is that a right turn followed by a left turn is different than a left turn followed by a right turn. Thus the group structure of the cube is nonabelian. The next thing one might realize is that the whole group of the cube is very large. When considering the order of the group of the cube, you must not only consider the permutations of the pieces, but you must also account of the orientation of the corners and edge pieces. Contained in the group of the Rubik's cube is a subgroup with two generators. For the miniature (2x2x2) Rubik's cube, the two-generator group (generated by rotations of adjacent faces) is of order 29,160 – which will be shown later – and has some very nice algebraic properties. In this paper, I will explore Daniel Bump and Daniel Auerbach's paper analyzing the two-generator group of the miniature Rubik's cube.

## 2. The two-generator group

We will let  $G$  denote the two-generator group of the miniature (2x2x2) Rubik's cube. The two generator group will consist of 90 degree clockwise rotations of two adjacent faces. Let  $R$  denote a clockwise rotation of the right face of the cube, and let  $U$  denote a clockwise rotation of the top face of the cube. Thus  $G = \langle R, U \rangle$ . Using standard notation, I will sometimes denote  $R^{-1}$  by  $R'$  and  $U^{-1}$  by  $U'$ . We will let  $K$  denote the subgroup of  $G$  that only changes orientations of any of the 6 corner cubes. This is to say,  $K$  fixes the position of the cube pieces of  $G$  while only affecting orientation.

**Proposition 2.0.1.**  *$K$  is an abelian, normal subgroup of  $G$  of order  $3^5$ .*

**Proof.** Let  $g \in G$  and  $k \in K$  be arbitrary elements of their respective groups. By definition  $K$  only effects the orientations of the cube pieces without permuting them. The element  $g$  will scramble the Rubik's cube in some particular way, and it is clear that  $g^{-1}$  will unscramble the cube in the same fashion. Thus the element  $gkg^{-1}$  will, in effect, scramble the Rubik's cube, change the orientation of some of the scrambled pieces while leaving their position fixed, and then unscramble the cube yielding only a change in orientation. Thus the net effect of

the element  $gkg^{-1}$  is nothing more than changing orientation of specific pieces. Hence  $gkg^{-1} \in K$  and  $K$  is normal in  $G$ . Since the elements of  $K$  only change orientation of cube pieces, and order of the orientation changes does not depend upon the order they are preformed in,  $K$  is clearly abelian.

To get a bound on the order of  $K$ , it is necessary to observe that for each of the 6 cube pieces that can be permuted, there are 3 possible orientations. This forces the order of  $K$  to be  $\leq 3^6$ . To get a good representation of the cube we will label each possible twist by different numbers: 0 representing no change of orientation, 1 for a clockwise twist, and 2 for a counterclockwise twist (or two clockwise twists).

Since the sum of the orientation shifts is 0 for any one change of orientation, it must be 0 for any changes of orientation, i.e. it will be 0 for any orientations of the corner triples. Since the solved cube is a pattern in which the sum of the orientation shifts was 0, any possible pattern must have a 0 sum of shifts. In particular, if we reach a pattern  $i$  which each corner is in its correct place, we can readily see the orientation shifts as the amounts the corners are twisted and so the total twist of corners must add to 0. This is always taken modulo 3. Thus the number of corner twists must be  $\equiv 0$  modulo 3 (proof from Singmaster's book on the cube).

This tells us that we have free choice for any 5 of the 6 movable corners. The remaining corner's orientation is determined by the choice of the the previous 5 and the constraint that the total sum of orientation changes must be  $\equiv 0$  modulo 3, hence  $|k| \leq 3^5$ .

It is left to show  $|k| \geq 3^5$ .

The diagram below, figure 1, shows that the operation  $RUR'URU^2R'U^2 \in K$  twist the three corners labeled 2, infinity and 0 clockwise by one click.

For the following calculations we will use the labeling of the cube as it is seen is figure 2. It follows from the following table and calculations that the operation above, together with its conjugates in  $G$ , generate the group that contains all of the operations that change the orientation of the corners such

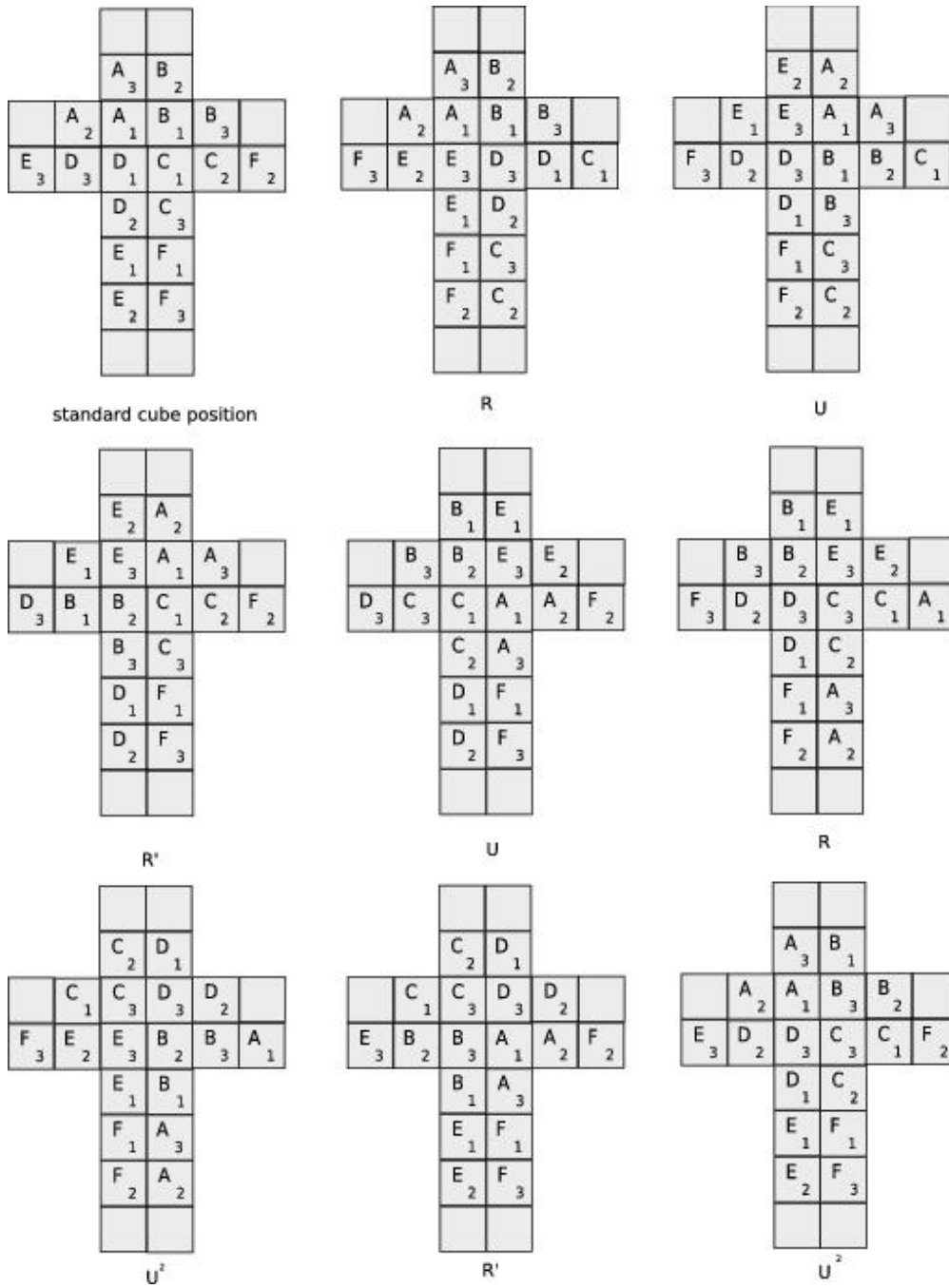


Figure 1: Orientation changes via  $RUR'URU^2R'U^2$

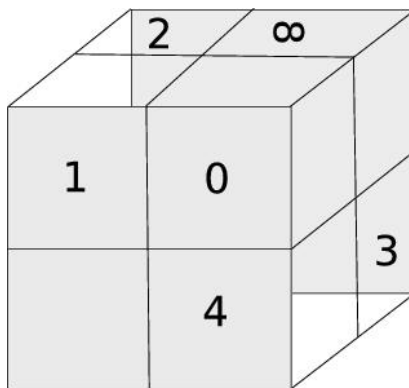


Figure 2: 3 dimensional cube labeling

that the total number of twists is  $\equiv 0$  modulo 3.

<i>Moves</i>	0	1	2	3	4	$\infty$
$K$	1	0	1	0	0	1
$UKU^{-1}$	0	1	1	0	0	1
$RKU^{-1}$	1	0	1	0	1	0
$(RU)K(RU)^{-1}$	1	1	1	0	0	0
$(UR)K(UR)^{-1}$	0	1	0	0	1	1
$U^3kU^{-3}$	1	1	0	0	0	1
$R^2KR^{-2}$	0	0	1	1	1	0
$R^3KR^{-3}$	0	0	1	1	0	1
$(U^2R^2)K(U^2R^2)^{-1}$	1	0	0	1	1	0
$(R^2U^2)K(R^2U^2)^{-1}$	0	1	1	1	0	0
$(R^2U)K(R^2U)^{-1}$	0	1	1	0	1	0
$(R^3U^{-1}R^2U^2)K(R^3U^{-1}R^2U^2)^{-1}$	1	0	1	1	0	0
$(R^3U^{-1})K(R^3U^{-1})^{-1}$	0	1	0	1	0	1
$(R^3U^{-1}R)K(R^3U^{-1}R)^{-1}$	1	1	0	1	0	0
$(U^3R^2)K(U^3R^2)^{-1}$	0	0	0	1	1	1
$(U^3R^2U)K(U^3R^2U)^{-1}$	0	0	1	0	1	1
$(RU^3)K(RU^3)^{-1}$	1	1	0	0	1	0
$(R^2U^3)K(R^2U^3)^{-1}$	0	1	0	1	1	0
$(U^2R^3U)K(U^2R^3U)^{-1}$	1	0	0	1	0	1
$(U^2R^2U)K(U^2R^2U)^{-1}$	1	0	0	0	1	1

From the table above it is clear that we can twist any three corners of our choosing by  $120^\circ$ . I will now show that these elements of  $K$  are enough to generate the twisting of any corners such that the total number of twists is  $\equiv 0$  modulo 3. To do this I will show the element  $(RU)K(RU)^{-1}$ ,  $(1,1,1,0,0,0)$ , along with the other elements of  $K$  can generate the 6-tuple  $(0,1,2,0,0,0)$ . Together  $(1,1,1,0,0,0)$  and  $(0,1,2,0,0,0)$  generate any possible orientation combination of

the corners labeled 0,1 and 2 which must be  $\equiv 0$  modulo 3. Since I arbitrarily labeled the columns, without loss of generality this can be done for any three corners, thus the elements of K seen above generate all of K.

$$\begin{array}{r}
(1 \ 1 \ 1 \ 0 \ 0 \ 0) \\
+ (1 \ 0 \ 1 \ 1 \ 0 \ 0) \\
\hline
(2 \ 1 \ 2 \ 1 \ 0 \ 0) \\
+ (1 \ 0 \ 0 \ 0 \ 1 \ 1) \\
\hline
(0 \ 1 \ 2 \ 1 \ 1 \ 1) \\
+ (0 \ 0 \ 0 \ 1 \ 1 \ 1) \\
\hline
(0 \ 1 \ 2 \ 2 \ 2 \ 2) \\
+ (0 \ 0 \ 0 \ 1 \ 1 \ 1) \\
\hline
(0 \ 1 \ 2 \ 0 \ 0 \ 0)
\end{array}$$

So  $|K| \geq 3^5$  and hence  $|K|=3^5$ .  $\square$

Two pieces of the cube are unaffected by any operation in G, thus the operations in G only affect the locations and orientation of 6 pieces. The corners that move will be labeled with the elements of the projective line  $\mathbb{P}^1(\mathbb{F}_5)$  (see Figure 2). The quotient  $G/K$  acts faithfully as a group of permutations of  $\mathbb{P}^1(\mathbb{F}_5)$  ignoring orientation, therefore the quotient is a subgroup of  $S_6$  where the elements are those of  $\mathbb{P}^1(\mathbb{F}_5)$ .

One group of permutations of  $\mathbb{P}^1(\mathbb{F}_5)$  is  $PGL(2, \mathbb{F}_5)$  acting on  $\mathbb{P}^1(\mathbb{F}_5)$  by fractional linear transformations. The group  $GL(2, \mathbb{F}_5)$  acts on elements of  $\mathbb{P}^1(\mathbb{F}_5)$  by the fractional linear transformation

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} : x \mapsto \frac{ax+b}{cx+d}, x \in \mathbb{F}_5 \cup \{\infty\},$$

where if  $x=\infty$  then  $\frac{ax+b}{cx+d} = \frac{a}{c}$ , and if  $cx+d = 0$  then  $\frac{ax+b}{cx+d} = \infty$ . The center Z of  $GL(2, \mathbb{F}_5)$  is all scalar matrices of the identity matrix. A simple calculation shows that the center acts trivially on  $\mathbb{P}^1(\mathbb{F}_5)$ , thus the action on the projective line is really an action of  $GL(2, \mathbb{F}_5)/Z$  which is defined to be the projective general linear group  $PGL(2, \mathbb{F}_5)$ .

**Proposition 2.0.2.** *As a permutation group acting on  $\mathbb{P}^1(\mathbb{F}_5)$ , we have  $G/K=PGL(2, \mathbb{F}_5)$ .*

**Proof.** I will first show that generators of  $G/K$  are contained in  $PGL(2, \mathbb{F}_5)$ . The elements R and U generate G.  $UUUUR=R$  since  $U^4$  is the identity, thus U and UR generate G. So I will show that U, UR are contained in  $PGL(2, \mathbb{F}_5)$ . Using the labeling in Figure 2 and the fractional linear transform described above, the element U corresponds to the cycle (0,1,2, $\infty$ ) and the element UR corresponds to the cycle (0,1,2,3,4). I will now verify that U and UR do in fact have the following fractional transformations I described above:

$$U = \begin{pmatrix} 0 & 1 \\ 2 & 1 \end{pmatrix} \in PGL(2, \mathbb{F}_5)$$

Yields the following fractional linear transform

$$\begin{pmatrix} 0 & 1 \\ 2 & 1 \end{pmatrix} : x \mapsto \frac{1}{2x+1}$$

Thus working modulo  $\mathbb{F}_5$ ,

$$\begin{aligned} 0 &\mapsto \frac{1}{2 \cdot 0 + 1} = \frac{1}{1} = 1, \\ 1 &\mapsto \frac{1}{2 \cdot 1 + 1} = \frac{1}{3} = 3^{-1} \equiv 2, \\ 2 &\mapsto \frac{1}{2 \cdot 2 + 1} = \frac{1}{5} \equiv \frac{1}{0} = \infty \text{ by definition} \\ 3 &\mapsto \frac{1}{2 \cdot 3 + 1} = \frac{1}{7} \equiv \frac{1}{2} = 2^{-1} = 3, \\ 4 &\mapsto \frac{1}{2 \cdot 4 + 1} = \frac{1}{9} \equiv \frac{1}{4} \equiv 4 \\ \text{inf} &\mapsto \frac{1}{\text{inf}} = 0 \end{aligned}$$

To see that

$$UR = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in PGL(2, \mathbb{F}_5)$$

Yields the following fractional linear transform:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} : x \mapsto \frac{x+1}{1}$$

Still working modulo  $\mathbb{F}_5$ , it is easy to see that  $0 \mapsto 1$ ,  $1 \mapsto 2$ ,  $2 \mapsto 3$ ,  $3 \mapsto 4$ ,  $4 \mapsto 5 \equiv 0$ , and  $\infty \mapsto \infty$ .

Thus  $G/K \subset PGL(2, \mathbb{F}_5)$ . It is also easy to verify that these two elements generate  $PGL(2, \mathbb{F}_5)$ .

**Claim.**  $U$  and  $UR$  generate  $PGL(2, \mathbb{F}_5)$ .

**proof.** To see that the two elements  $U$  and  $UR$  generate  $PGL(2, \mathbb{F}_5)$  I will show that they generate subgroups of order 3, 5 and 8. The order of  $PGL(2, \mathbb{F}_5)$  is 120, which will be shown in a corollary below.  $120 = 2^3 \cdot 3 \cdot 5$  so by showing subgroups of each order we can be sure that  $U$  and  $UR$  will generate the specific group of order 120. The subgroups of order 3 and 5 are cyclic while the subgroup of order 8 is isomorphic to the dihedral group on 4 elements  $D_4$ . Keep in mind that the multiplication performed in the following computations is done modulo 5 and scalar matrices are in the same coset of  $G/K$ .

The order 3 subgroup can be seen by the element  $U \cdot UR \cdot U =$

$$\begin{pmatrix} 0 & 1 \\ 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}$$

and

$$\left\langle \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle = \left\{ \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 2 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

Thus  $U \cdot UR \cdot U$  is a subgroup of order 3. The order 5 subgroup is just the cyclic subgroup generated by UR.

$$\left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle = \left\{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

Hence  $\langle UR \rangle$  is an order 5 subgroup of  $\text{PGL}(2, \mathbb{F}_5)$ . I found the order 8 subgroup by conjugating order two subgroups. The order two subgroups I used were  $U \cdot (UR)^2$ ,  $UR \cdot U \cdot UR$  and  $U^3 \cdot UR \cdot U^3 \cdot UR$ . Notice that  $U^3 \cdot UR \cdot U^3 \cdot UR$  is nothing more than  $R^2$  since  $U^4$  is congruent to the identity.

$$U \cdot UR^2 = \begin{pmatrix} 0 & 1 \\ 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}$$

$$UR \cdot U \cdot UR = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 4 \\ 2 & 3 \end{pmatrix}$$

$$U^3 \cdot UR \cdot U^3 \cdot UR = \begin{pmatrix} 0 & 1 \\ 2 & 1 \end{pmatrix}^3 \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 2 & 1 \end{pmatrix}^3 \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 4 & 0 \\ 3 & 1 \end{pmatrix}$$

$$\left\langle \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 4 \\ 2 & 3 \end{pmatrix}, \begin{pmatrix} 4 & 0 \\ 3 & 1 \end{pmatrix} \right\rangle =$$

$$\left\{ \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 4 \\ 2 & 3 \end{pmatrix}, \begin{pmatrix} 4 & 0 \\ 3 & 1 \end{pmatrix}, \begin{pmatrix} 3 & 1 \\ 3 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 3 \\ 4 & 3 \end{pmatrix}, \right.$$

$$\left. \begin{pmatrix} 0 & 2 \\ 1 & 4 \end{pmatrix}, \begin{pmatrix} 2 & 3 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

Since we have shown subgroups of order 3, 5 and 8, by Lagrange the group generated by U and UR is of size at least  $3 \cdot 5 \cdot 8 = 120$ . Hence U and UR generate  $\text{PGL}(2, \mathbb{F}_5)$ .  $\square$

**Corollary 2.0.3.**  $|G/K| = 5!$  and  $G/K \cong S_5$ .

**Proof.** To see that  $|G/K| = 5!$  I will show the size of  $\text{PGL}(2, \mathbb{F}_5)$  is  $5!$ . This will first be done by counting  $\text{GL}(2, \mathbb{F}_5)$  then finding the size of the the group quotiented by scalar matrices.  $\text{GL}(2, \mathbb{F}_5)$  consists of all two by two matrices with nonzero determinant and entries from  $\mathbb{F}_5$ .  $\text{M}(2, \mathbb{F}_5)$  is the set of all matrices with entries in  $\mathbb{F}_5$  and has 5 choices for each of the 4 entries. Thus  $\text{M}(2, \mathbb{F}_5)$  has  $5 \cdot 5 \cdot 5 \cdot 5 = 5^4 = 625$  elements. I will subtract off the zero determinant cases of  $\text{M}(2, \mathbb{F}_5)$  to determine the size of  $\text{GL}(2, \mathbb{F}_5)$ . Consider the matrix

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Thus the determinant of M is  $a \cdot d - b \cdot c$  and we are looking for where  $\det(M) \equiv_5 0$ .

Case 1:  $a \neq 0$  ;  $d \neq 0$ . Then there are 4 choices for a, 4 choices for d, 4 choices for b, but that will fix c since there are nozerodivisors in a field. Thus this case yields  $4 \cdot 4 \cdot 4 \cdot 1=64$  possibilities.

Case 2:  $a \neq 0$  ;  $d=0$  ;  $b=0$ . There are 4 choices for a, both b and d are fixed as 0 and thus there are 5 choices for c. Case 2 yields  $4 \cdot 1 \cdot 1 \cdot 5=20$  possibilities.

Case 3:  $a=0$  ;  $d \neq 0$  ;  $b=0$ . This case is analogous to case 2 and thus yields 20 possibilities.

Case 4:  $a \neq 0$  ;  $d=0$  ;  $b \neq 0$ . There are 4 choices for a, 1 choice for d, 4 choice for b and 1 choice for c namely 0. Thus this case yields  $4 \cdot 1 \cdot 4 \cdot 1=16$  possibilities.

Case 5:  $a=0$  ;  $d \neq 0$  ;  $b \neq 0$ . This case is analogous to case 4, thus there are 16 possibilities.

Case 6:  $a=d=0$ . Either b or c must be 0. If b is 0 there are 5 choices for c, and if c is 0 there are 5 choices for b. This double counts when the are both b and c are 0. Hence this case yields  $(1 \cdot 1 \cdot 1 \cdot 5)+(1 \cdot 1 \cdot 5 \cdot 1)-1=9$  possibilities.

This covers all 0 determinant cases. Thus there are  $64+20+20+16+16+9=145$  total cases. This tells us that  $GL(2, \mathbb{F}_5)$  has  $625-145=480$  elements. Since  $PGL(2, \mathbb{F}_5)$  is the quotient  $GL(2, \mathbb{F}_5)/Z$ , where

$$Z = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix} \right\}$$

has order 4,  $PGL(2, \mathbb{F}_5)$  has order  $\frac{480}{4}=120=5!$

The isomorphism between  $PGL(2, \mathbb{F}_5)$  and  $S_5$  will be checked by labeling  $\mathbb{P}^1(\mathbb{F}_5)$  with the elements of the 5-Sylow subgroups of  $S_5$  in the following way:

$$\infty = \langle (12345) \rangle = \{(12345), (13524), (14253), (15432), (1)\}$$

$$0 = \langle (12354) \rangle = \{(12354), (13425), (15243), (14532), (1)\}$$

$$1 = \langle (12453) \rangle = \{(12453), (14325), (15234), (13542), (1)\}$$

$$2 = \langle (12543) \rangle = \{(12543), (15324), (14235), (13452), (1)\}$$

$$3 = \langle (12534) \rangle = \{(12534), (15423), (13245), (14352), (1)\}$$

$$4 = \langle (12435) \rangle = \{(12435), (14523), (13254), (15342), (1)\}$$

$S_5$  acts on  $\mathbb{P}^1(\mathbb{F}_5)$  by conjugating its 5-Sylow subgroups. Conjugation the group of permutations of the projective line group is nothing more than the action of  $PGL(2, \mathbb{F}_5)$  on the projective line group. To see that the permutation group obtained contains  $PGL(2, \mathbb{F}_5)$  it is sufficient to check for generators of  $S_5$  where conjugation of the 5-Sylow subgroups by the generators induces a linear fractional transformation. Consider conjugation by the cycle (12345):

$$(12345)(12345)(12345)^{-1} = (12345) : \infty \mapsto \infty$$

$$(12345)(12354)(12345)^{-1} = (15234) : 0 \mapsto 1$$

$$(12345)(12453)(12345)^{-1} = (14235) : 1 \mapsto 2$$



$$\begin{aligned}
(12345)(12543)(14235)^{-1} &= (12534) : 2 \mapsto 3 \\
(12345)(12534)(12345)^{-1} &= (14523) : 3 \mapsto 4 \\
(12345)(14523)(12345)^{-1} &= (13425) : 4 \mapsto 0
\end{aligned}$$

thus conjugation by (12345) correspond to the fractional linear transformation  $x \mapsto x+1$ , which in turn corresponds to the matrix  $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \text{GL}(2, \mathbb{F}_5)$ .

Now let us see how conjugation by the cycle (45) affects the 5-Sylow subgroups. Since (45) is a transposition  $(45)^{-1}=(45)$ , that is it is its own inverse.

$$\begin{aligned}
(45)(12345)(45) &= (12354) : \infty \mapsto 0 \\
(45)(12354)(45) &= (12345) : 0 \mapsto \infty \\
(45)(12453)(45) &= (12543) : 1 \mapsto 2 \\
(45)(12543)(45) &= (12453) : 2 \mapsto 1 \\
(45)(12534)(45) &= (12435) : 3 \mapsto 4 \\
(45)(12435)(45) &= (12534) : 4 \mapsto 3
\end{aligned}$$

so  $\infty \leftrightarrow 0$ ,  $1 \leftrightarrow 2$  and  $3 \leftrightarrow 4$ . This action has the fractional linear transform  $x \mapsto \frac{2}{x}$ . This can be seen by:

$$\begin{aligned}
0 &\mapsto \frac{2}{0} = \infty, \\
1 &\mapsto \frac{2}{1} = 2, \\
2 &\mapsto \frac{2}{2} = 1, \\
3 &\mapsto \frac{2}{3} = 2 \cdot 3^{-1} = 2 \cdot 2 = 4, \\
4 &\mapsto \frac{2}{4} = 2 \cdot 4^{-1} = 2 \cdot 4 = 8 \equiv_5 3.
\end{aligned}$$

The fractional linear transform  $x \mapsto \frac{2}{x}$  corresponds to the matrix  $\begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix} \in \text{GL}(2, \mathbb{F}_5)$ . Since  $S_5$  is generated by (12345) and (45) (see lemma below), conjugation by any element of  $S_5$  of the 5-Sylow subgroups labeled a s such is contained in  $\text{PGL}(2, \mathbb{F}_5)$ . The net effect is a homomorphism  $S_5 \mapsto \text{PGL}(2, \mathbb{F}_5)$ . Since the order of  $S_5$  is  $5!$ , the two groups have the same order. The only nontrivial normal subgroup of  $S_5$  is  $A_5$  and the element (12345)  $\in A_5$  acts nontrivially, hence the homomorphism is nontrivial and must be an isomorphism.  $\square$

**Lemma 2.0.4.** *The elements (45) and (12345) generate  $S_5$ .*

**Proof.** I will be performing various products in  $\langle (45), (12345) \rangle$  to get all the transpositions of  $S_5$ . Since every element in  $S_n$  is a product of transpositions,

when we get all transpositions of  $S_5$  from  $\langle (45), (12345) \rangle$  we will have shown that  $\langle (45), (12345) \rangle = S_5$ .

Recall:

$$\langle (12345) \rangle = \{(12345), (13524), (14253), (15432), (1)\}$$

$$(45)(12345) = (4)(5123) = (1235),$$

$$\langle (1235) \rangle = \{(1), (1235), (13)(25), (1532)\}$$

$$(12345)(45) = (4123)(5) = (1234),$$

$$\langle (1234) \rangle = \{(1), (1234), (13)(24), (1432)\}.$$

We have two products of disjoint transpositions  $(13)(25)$  and  $(13)(24)$  so we can use their product and its cyclic subgroup to get transpositions.

$$(13)(25)(13)(24) = (25)(24) = (245), \text{ and } \langle (245) \rangle = \{(1), (245), (254)\}$$

$(245)(45) = (24)$  and  $(45)(245) = (25)$  so we now have three of the ten transpositions needed.

Using  $(13524)$  from above,  $(13524)(45) = (42)(513) = (135)(24)$ , and we have  $(24)$  thus we have  $(135)(24)(24) = (135)$ .  $\langle (135) \rangle = \{(1), (15)(13), (13)(15)\}$ . Similarly  $(45)(13524) = (134)(52) = (134)(25)$ , and we have  $(25)$  thus we have  $(134)(25)(25) = (134)$ .  $\langle (134) \rangle = \{(1), (14)(13), (13)(14)\}$ . So we have  $(15)(14)$  and  $(14)(13)$  and their product  $(15)(13)(13)(14) = (15)(14) = (145)$ .  $\langle (145) \rangle = \{(1), (145), (154)\}$ . So we have  $(145)(45) = (14)$  and  $(154)(45) = (15)$ . Getting either of these transpositions guarantees us  $(13)$  from the product of transpositions above. Thus we have three more transpositions, yielding six of ten.

We can use the transpositions  $(14)$  and  $(24)$  to get  $(12)$ . Notice  $(14)(24) = (241) = (142)$  and  $\langle (142) \rangle = \{(1), (12)(14), (14)(12)\}$ . We have  $(14)$ , so we have  $(12)(14)(14) = (12)$ . Now we are up to seven of the ten transpositions.

Now I will use  $(12345)$  and the transposition  $(12)$  to get  $(35)$ .  $(12345)(12) = (1345)$  and  $\langle (1345) \rangle = \{(1), (1345), (14)(35), (1543)\}$ . We already have  $(14)$  thus we have  $(14)(14)(35) = (35)$  collecting the eighth transposition.

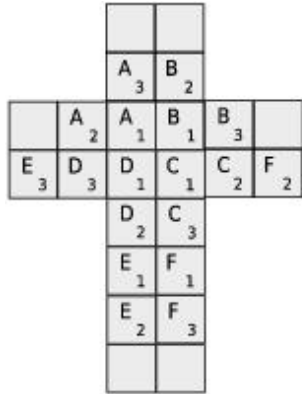
I will use  $(25)$  and  $(35)$  to get  $(23)$ .  $(25)(35) = (325) = (253)$  and  $\langle (253) \rangle = \{(1), (23)(25), (25)(23)\}$ . We have  $(25)$  so we get  $(25)(25)(23) = (23)$ , the ninth transposition.

To get  $(34)$  I will use  $(35)$  and  $(45)$ .  $(35)(45) = (435) = (354)$  and  $\langle (354) \rangle = \{(1), (34)(35), (35)(34)\}$ . We have  $(35)$  so  $(35)(35)(34) = (34)$  and we have the final transposition.

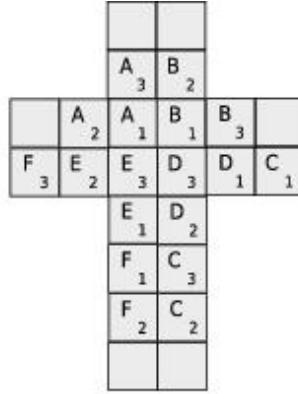
Since we have all 10 transpositions,  $\{(12), (13), (14), (15), (23), (24), (25), (34), (35), (45)\}$ , of  $S_5$ , and every element of  $S_5$  can be written as a product of transpositions, hence  $\langle (45), (12345) \rangle = S_5$ .  $\square$

Now We will show that  $G$  is a semidirect product of  $K \rtimes H$  for some subgroup  $H$ . By definition of a semidirect product, we must verify three things. First that  $H \cap K = \{e\}$  (where  $e$  is the identity of  $G$ ), second that  $G = HK$  and finally that  $K \triangleleft G$ , which was already shown.

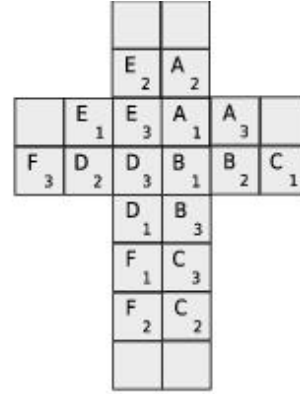




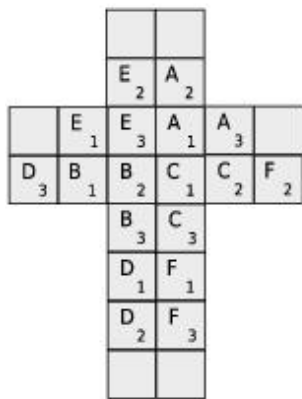
Standard Cube



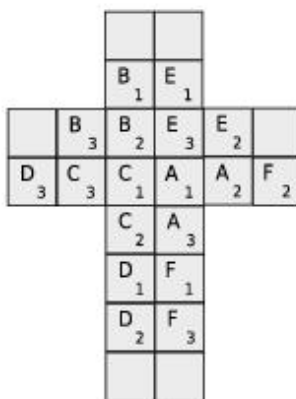
R



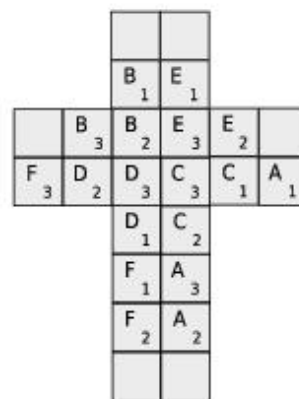
U



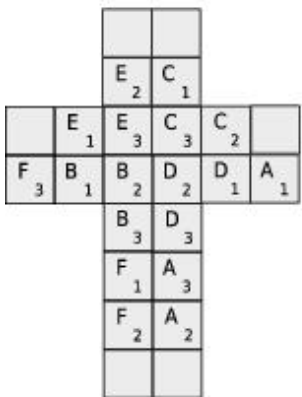
R'



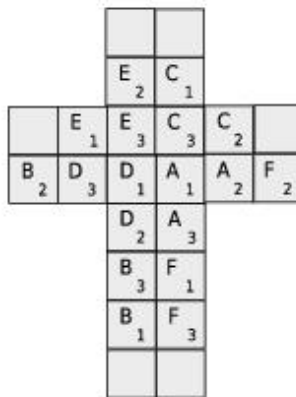
U



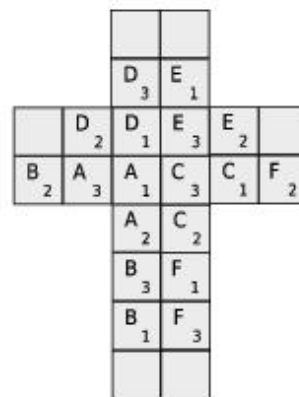
R



U'



R'



U

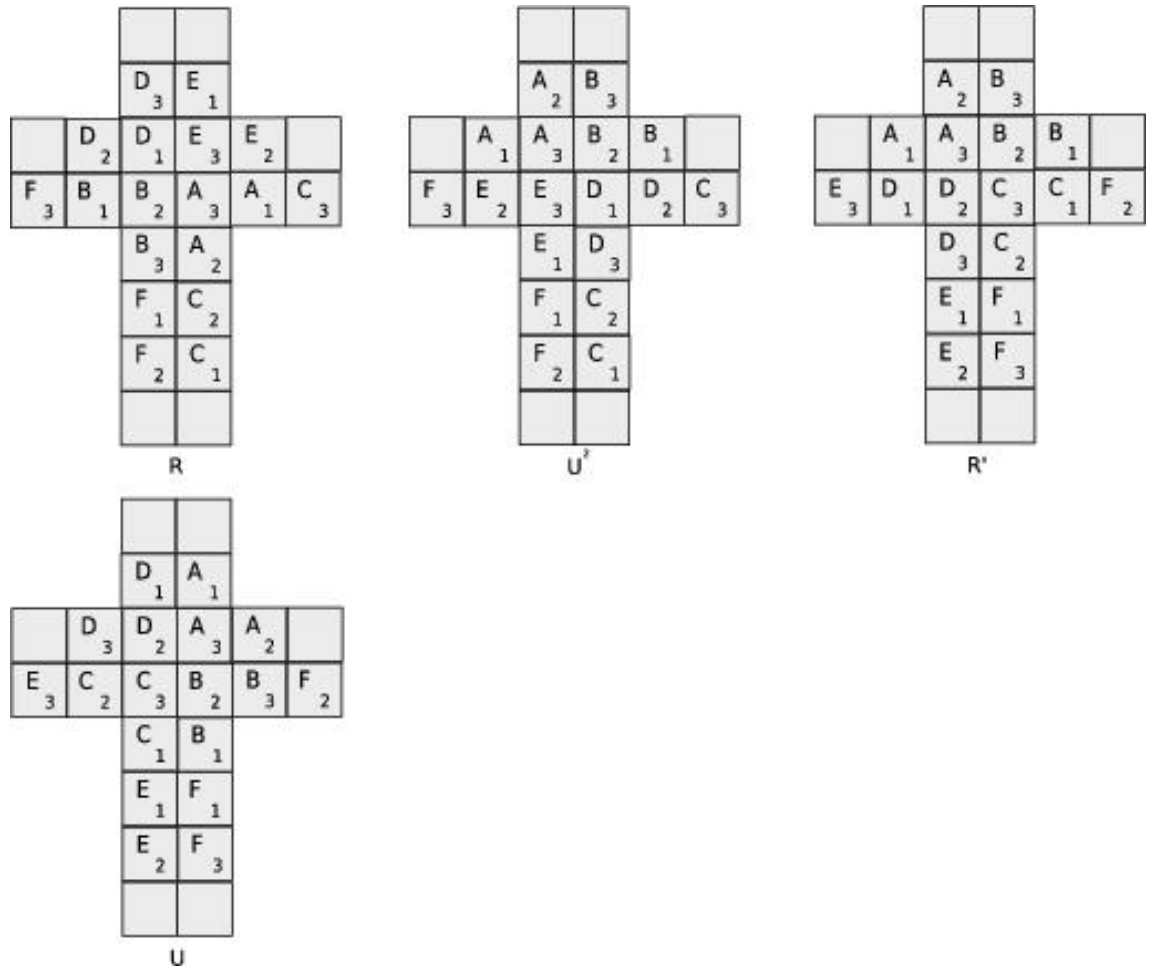
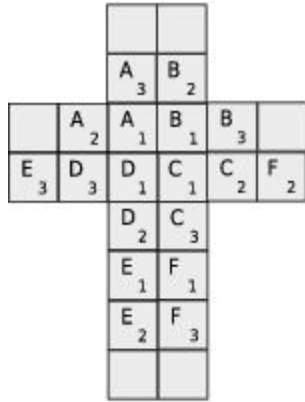
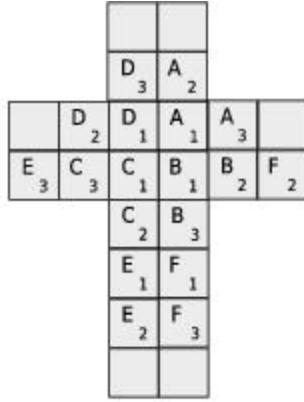


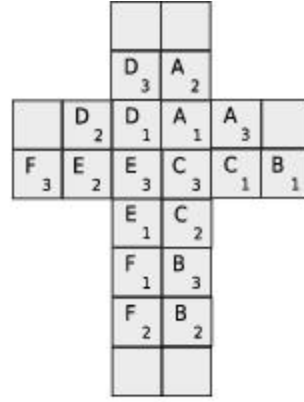
Figure 3: The image of  $h_1$  in H



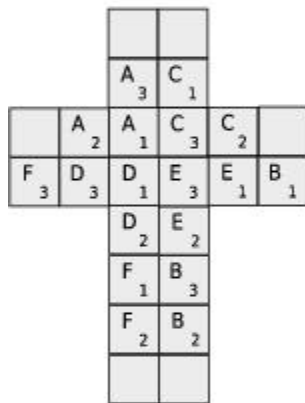
Standard Cube



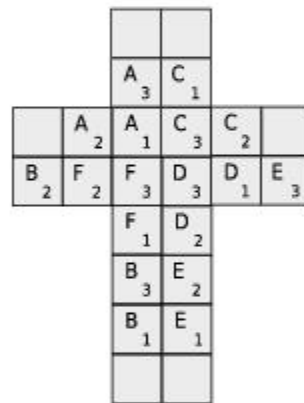
U



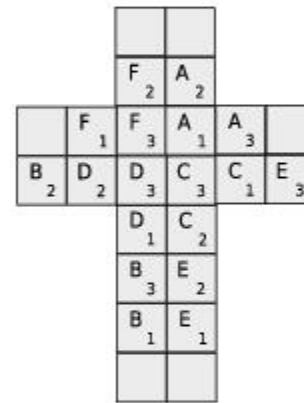
R



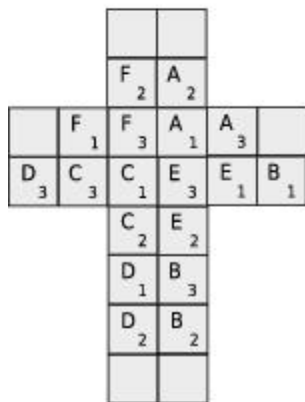
U'



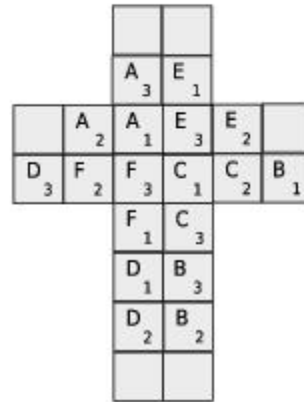
R



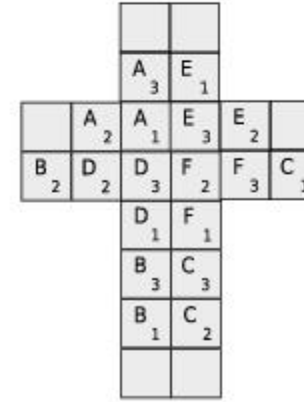
U



R'



U'



R

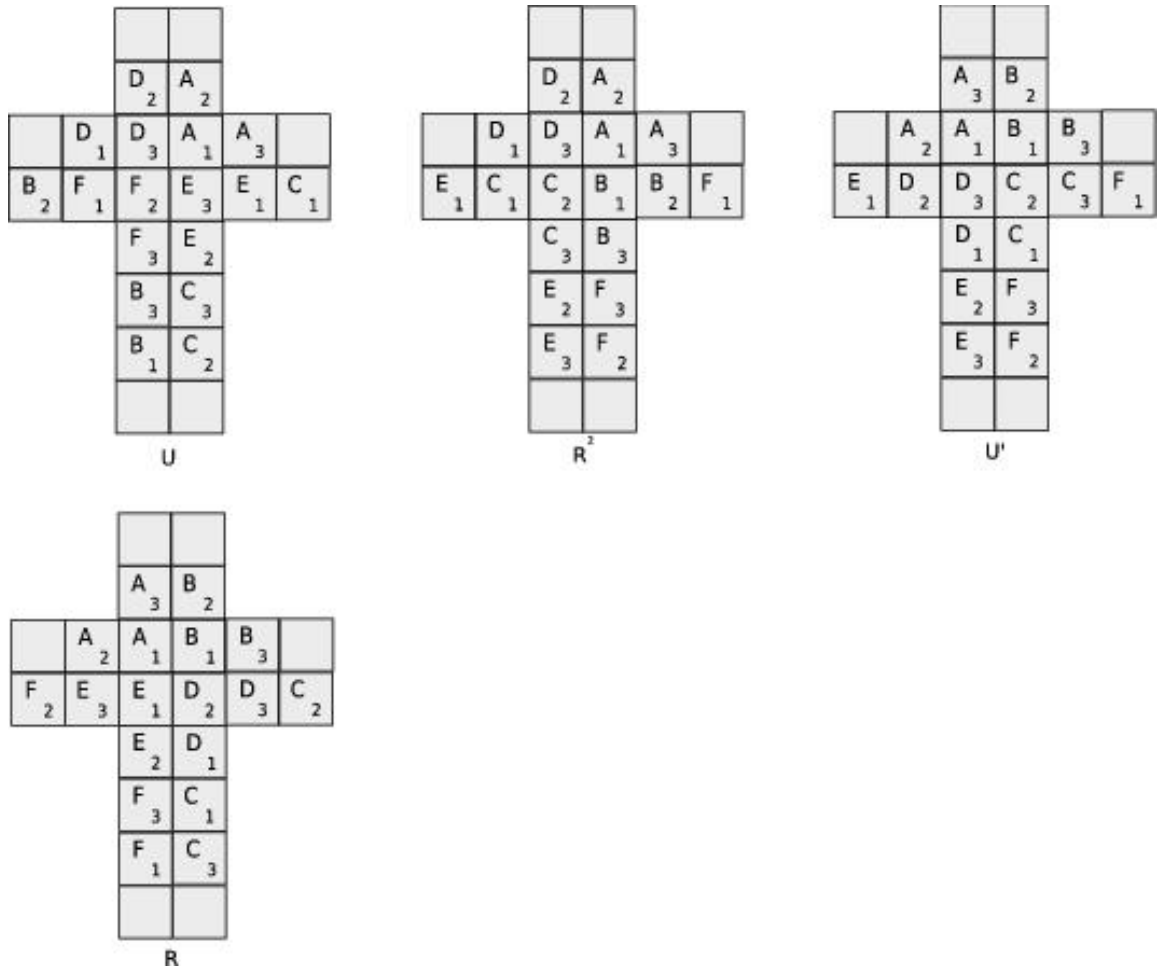


Figure 4: The image of  $h_2$  in H