# RUBIK'S GROUPS

EDWARD C. TURNER
*Department of Mathematics and Statistics, SUNY at Albany, Albany, NY 12222*

KAREN F. GOLD
*Department of Mathematics, University of California at Los Angeles, Los Angeles, CA 90024*

**1. Introduction.** Few puzzles have captured the public fancy the way Rubik's cube has. The beauty of the puzzle, beyond its mechanical ingenuity and elegance and colorful appearance, lies in the contrast between the sheer impossibility of solving the cube by chance (better to bet on the proverbial snowball) and the existence of algorithms simple enough that many children master and even discover them. The value of the cube for the teacher of mathematics is that it provides a setting that is interesting in its own right and in which most of the important notions of elementary group theory are illustrated. The purpose of this article is two-fold. First we describe a uniform method—The Method—for solving *any* "Rubik's-type puzzle" (defined in the next section). As is the case with all descriptions of solution algorithms, we provide a list of basic moves, outline how to use them to unscramble a puzzle, and assure the reader that they will always suffice. Despite its generality, The Method is conceptually very simple, illustrating the fact that generalization often leads to simplification. The second purpose is to analyse the "Rubik's Group $\mathscr{R}$" whose elements are the various states of the puzzle and whose group operation describes composition of moves and to *prove* the adequacy of The Method. The analysis will involve an excursion into group theory in which permutation groups, direct sums, homomorphisms and exact sequences appear naturally and which leads to an explicit description of $\mathscr{R}$ as a semi-direct product of easily described factors. A by-product of this structure is a notation scheme that handles composition easily. We also discover that the octahedral puzzle is unique among Rubik's type puzzles in that edge flipping is impossible. In order to make the paper as accessible as possible to beginning students, we have collected in Appendix 1 a list of definitions of terms that might not be introduced in a first course in algebra. The first use of each term appears in italics.

This paper is an outgrowth of a senior research project by Gold under the direction of Turner. It began with a study of the Tetrahedron {Pyraminx} and the Cube; as more puzzles came on the market, namely the Impossiball, Alexander's Star and the Megaminx (a dodecahedron), the scope of the project widened to consideration of the general puzzle, resulting in the current analysis.

**2. The Method.** In this section we describe The Method—an algorithm that will solve any *Rubik type puzzle*. A Rubik type puzzle is a *regular solid* (see Appendix) composed of pieces corresponding to vertices, edges and faces of the solid and for which a basic move is the rotation of a face, including edge and vertex pieces. This gives 5 possibilities corresponding to the 5 regular solids, which are listed in Table 1 of the next section. The theory also applies to any puzzle whose moves are turns about a vertex—e.g., Alexander's star or the Impossiball—by the trick of dualization. Inside any regular solid is another whose vertices are the centers of the original faces (so a cube contains a smaller octahedron) and vertex turns on the larger correspond to face turns on the smaller. To solve a vertex turning puzzle, imagine the dual face turning puzzle inside and

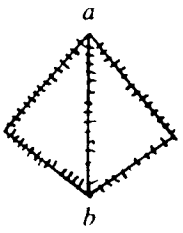
---

*Karen Gold*: I am presently a graduate student and teaching assistant in the Mathematics Department at UCLA. My primary mathematical interests are combinatorial group theory and algebraic geometry. My hobbies include Russian studies, folklore, boardgames, and the department's daily tea.

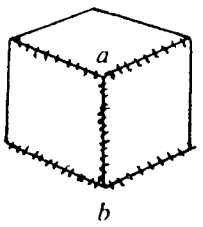
*Edward Turner*: I did my undergraduate work at the University of Rochester, graduate work at UCLA, and spent two years as an instructor at MIT before moving to SUNYA in 1971. My early mathematical interest was in differential topology, but in the last five years I have become increasingly interested in combinatorial group theory. My non-mathematical interests include running, squash, and folk dancing.

solve it. This gives another four puzzles (the dual of the tetrahedron is the tetrahedron). Each puzzle has simpler versions that don't have all three types of piece: the Impossiball has only faces, Alexander's Star only edges and the Rubik's Pocket Cube only vertices. Rubik's Revenge and obvious more general $n \times n \times n$ versions are not Rubik type puzzles in our sense. They admit another type of move not equivalent to any combination of face moves—the "slice" moves that turn a plane of pieces parallel to face.

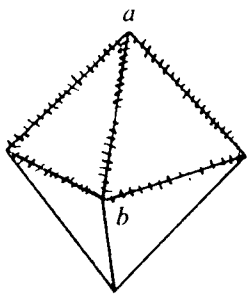
For each puzzle, consider one edge joining vertices $a$ and $b$ together with the adjacent edges on the two faces that meet at that edge, as indicated below.



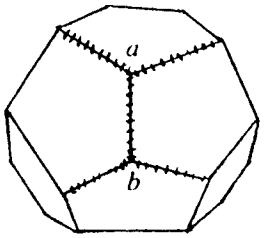

Tetrahedron



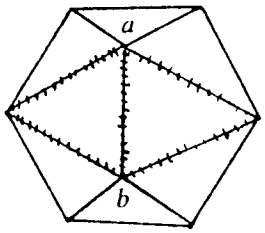

Cube




Octahedron

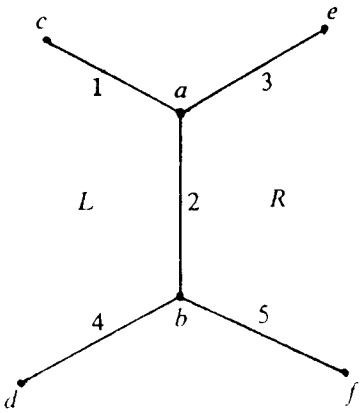



Dodecahedron




Icosahedron

We denote this schematically as shown in Fig. 1, with the understanding that $c = d$ and $e = f$ if faces are triangles and that there are other edges on top and bottom if the vertex degree is more than 3.




Small letters label vertices,
numbers edges,
and capitals face terms.

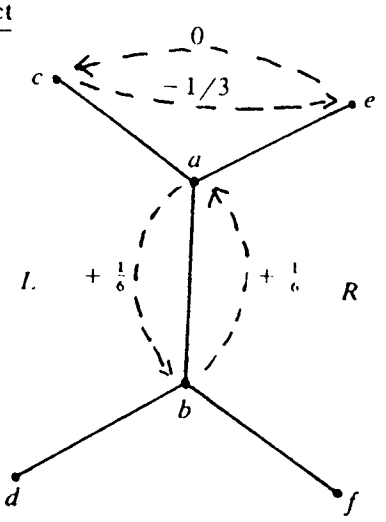
FIG. 1

We denote by $L$ and $R$ the clockwise rotations of the faces labeled $L$ and $R$ and use the convention that moves in a sequence are applied from left to right. After some experimentation with short sequences of basic moves, one discovers the usefulness of the *commutator* (see Appendix) of $L$ and $R^{-1}$, which has the effect shown in Fig. 2.

**C** is the basic building block of the solution which proceeds in four steps. The face pieces are in solved position by the nature of the puzzle and serve as references in placing vertex and edge pieces.

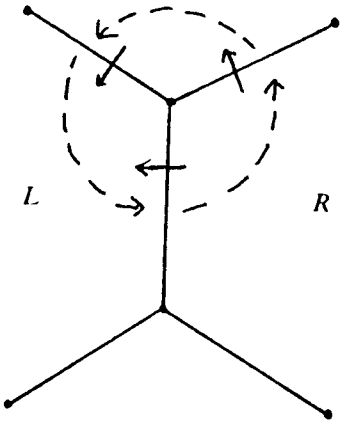
Effect of $\mathbf{C} = [L, R^{-1}] = LR^{-1}L^{-1}R$

Vertex effect




Rotation is referenced to direct parallel translation with positive fractions denoting clockwise rotations.

Edge effect




The effect of **C** on orientation is to preserve the small transverse arrows.

FIG. 2

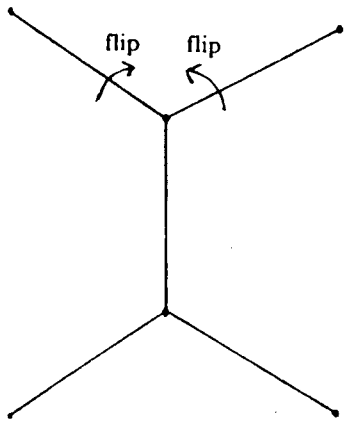
Step 1. Place the edges

**C** is a 3-cycle on edges. By conjugation we can obtain any 3-cycle of edges; for let $T$ be any sequence that moves 1 to 4, 2 to 5 and 3 to 6 (such $T$ always exists)—then $T^{-1}\mathbf{C}T$ cycles 4, 5 and 6. Since 3-cycles generate the alternating group, we can manage any even permutation of the edges. On all puzzles except the Cube, only even permutations are possible and we are done. On the Cube, if an odd edge permutation is desired, one basic move—inducing an odd edge permutation—converts it to an even permutation. Thus **C** and its *conjugates* (see Appendix) suffice to place all the edge pieces correctly.

Step 2. Orient the edges

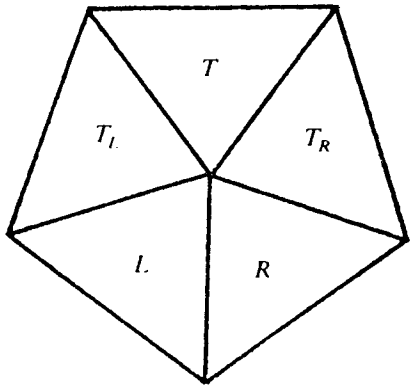
Flipping edges in pairs is particularly easy on puzzles with vertex degree 3: let $\rho$ denote clockwise rotation of the puzzle 1/3 of a turn about the diameter through vertex $a$. (Of course one never actually does the $\rho^{-1}$. This is the only time we use a rigid motion of the entire puzzle—we do so only for ease of description.) As the number of flipped edge pieces is always even, this move suffices to right them all. (See figure at the top of p. 620.)

Effect of $[C, \rho] = C\rho C^{-1}\rho^{-1}$ on edges




Edge flipping on the octahedron and icosahedron is complicated by the presence of other edges on top; we show in Lemma 2 of Section 3 that edge flipping on the octahedron is in fact impossible. A double edge flipper for the dodecahedron is shown below. (See Fig. 3.)

Dodecahedron




$[L, R^{-1}]T_L^{-1}T^{-1}[R^{-1}, T_R]TT_L$

FIG. 3

After steps 1 and 2 have been completed, the edges are in solved position. The remaining steps leave them there.

Step 3. Place the vertices

We will see that once edges are placed, the vertex permutation must be even and that it suffices to have a move that cycles 3 vertices without effecting the edges. Let $B$ denote clockwise rotation of the bottom face—the one across edge $bd$ from $L$ in Fig. 1. Then $[C, B]$ permutes vertices by $(abd)$ and has no effect on edges.

Step 4. Orient the vertices

We will see that it suffices to rotate two vertices in opposite directions. The move $[C^2, B]$ rotates $b$ clockwise and $d$ counterclockwise (as viewed from outside) and does not affect edges.

In the next two sections we will see that this algorithm will restore any scrambled puzzle to its original—often called pristine—state. It is surely inefficient in terms of time compared to others, but is conceptually quite simple and simple in practice in that very few conjugates of basic moves are necessary. In fact, the cube can be solved using conjugates only in Step 1. Furthermore, the list of basic moves is very short and easily remembered:

$$C \qquad [C, \rho] \qquad [C, B] \qquad [C^2, B]$$

(except for the exotic double edge flipper).

On puzzles lacking edges (like the Rubik's Pocket Cube and the Impossiball) steps 1 and 2 are unnecessary and on those lacking vertices (like Alexander's Star) steps 3 and 4 are unnecessary. There is, however, a complicating factor when faces are absent, as they are on all the above—it is much harder to decide what moves to make without reference face pieces. One learns from practice how to deal with this problem and we will ignore it.

**3. The Rubik's group $\mathscr{R}$.** With each regular solid is associated a Rubik's type puzzle and a Rubik's group, defined below. Table 1 gives the appropriate numbers for each puzzle and the last row sets our general notation.

| Regular Solid | Group | face degree | vertex degree | # of vertices | # of edges | # of faces |
|---|---|---|---|---|---|---|
| Tetrahedron | $\mathscr{T}$ | 3 | 3 | 4 | 6 | 4 |
| Cube | $\mathscr{C}$ | 4 | 3 | 8 | 12 | 6 |
| Octahedron | $\mathscr{O}$ | 3 | 4 | 6 | 12 | 8 |
| Dodecahedron | $\mathscr{D}$ | 5 | 3 | 20 | 30 | 12 |
| Icosahedron | $\mathscr{I}$ | 3 | 5 | 12 | 30 | 20 |
| Generic | $\mathscr{R}$ | $p$ | $q$ | $V$ | $E$ | $F$ |

TABLE 1

We imagine the central mechanism of the puzzle as fixed, so the face pieces don't move, and refer to the $F$ rotations of a face through $2\pi/p$ radians clockwise as "basic moves". An element of the group $\mathscr{R}$ is a sequence of basic moves, where it is understood that two sequences represent the same move if their effect on the puzzle is the same. Otherwise stated, $\mathscr{R}$ is the quotient of the *free group* (see Appendix) generated by the basic moves by the normal subgroup of expressions that leave all vertex and edge pieces in their original positions and orientations.

We analyse $\mathscr{R}$ by separating the position effect from the orientation effect and the vertex effect from the edge effect. Ignoring orientations, each element of $\mathscr{R}$ permutes the edges and vertices, defining a map pos (for position)

$$\mathscr{R} \xrightarrow{\text{pos}} S_E \times S_V,$$

where $S_n$ is the permutation group on $n$ letters. We denote the kernel of pos by $\mathscr{F}$, the position fixed subgroup of moves that do not move pieces from their original positions and the image of pos by $\Sigma$. Thus by definition we have an *exact sequence* (see Appendix)

$$1 \to \mathscr{F} \xrightarrow{i} \mathscr{R} \xrightarrow{\text{pos}} \Sigma \to 1,$$

where $i$ denotes inclusion.

The remainder of this section is devoted to identifying $\mathscr{F}$ and $\Sigma$—the analysis of $\mathscr{R}$ is completed in the next section with a description of how $\mathscr{F}$ and $\Sigma$ interact.

LEMMA 1.

(i) *If $\mathscr{R} \neq \mathscr{C}$, then $\Sigma = A_E \times A_V$.*

(ii) *If $\mathscr{R} = \mathscr{C}$, then $\Sigma = \{(\sigma, \mu) | \sigma$ and $\mu$ are both even or both odd$\}$.*

LEMMA 2. *There are exact sequences:*

(i) *If $\mathscr{R} \neq \mathscr{O}$,*

$$0 \to \mathscr{F} \xrightarrow{f \times r} \bigoplus_1^E \mathbb{Z}_2 \oplus \bigoplus_1^V \mathbb{Z}_q \xrightarrow{\text{Sum}} \mathbb{Z}_2 \times \mathbb{Z}_q \to 0,$$

*where*

$$\mathrm{Sum}((f_1,\dots,f_E),(r_1,\dots,r_v)) = \left(\sum_1^E f_i, \sum_1^V r_i\right).$$

(ii) *If* $\mathscr{R} = \mathscr{O}$,

$$0 \to \mathscr{F} \xrightarrow{r} \bigoplus_1^V \mathbb{Z}_2 \xrightarrow{\mathrm{Sum}} \mathbb{Z}_2 \to 0.$$

This is clearly a *split short exact sequence* (see Appendix), so this implies that $\mathscr{F}$ is isomorphic to

$$\bigoplus_1^{E-1} \mathbb{Z}_2 \oplus \bigoplus_1^{V-1} \mathbb{Z}_q.$$

The splitting is not *canonical* (see Appendix), however, and it is more natural to think of $\mathscr{F}$ as a subgroup of $\oplus_1^E \mathbb{Z}_2 \oplus \oplus_1^V \mathbb{Z}_q$.

*Proof of Lemma* 1. In case (i), the face degree $p$ is odd, so that each basic move induces an even permutation on both edges and faces: thus $\Sigma \subset A_E \times A_V$. $A_E$ is generated by 3-cycles and Step 1 of The Method shows how to achieve any desired 3-cycle of edges. Given $(\sigma,\mu) \in A_E \times A_V$, let $M$ be a sequence of basic moves so that $\mathrm{pos}(M) = (\sigma,\mu')$. Now $\mu'$ is even so $(\mu')^{-1}\mu \in A_V$ and Step 3 shows how to find a sequence of moves $N$ such that $\mathrm{pos}(N) = (\mathrm{id},(\mu')^{-1}\mu)$. Then $\mathrm{pos}(MN) = (\sigma,\mu)$, so pos is onto $A_E \times A_V$.

In case (ii), the face degree is 4, so each basic move induces an odd permutation on both edges and vertices—the total parity is even, so

$$\Sigma \subset A_E \times A_V \cup (S_E \setminus A_E) \times (S_V \setminus A_V).$$

The argument of case (i) shows that $\Sigma \supset A_E \times A_V$. If $\sigma$ and $\mu$ are both odd, then let $B$ be any basic move and consider $\mathrm{pos}(B)\cdot(\sigma,\mu) = (\sigma',\mu')$. $\sigma'$ and $\mu'$ are both even, so $(\sigma',\mu') \in \Sigma$; thus $(\sigma,\mu) \in \Sigma$ and we are done.

*Proof of Lemma* 2. The key to Lemma 2 is the question, "How do you measure the flipping of an edge piece or the rotation of a vertex piece when it has changed position?" It may seem paradoxical to ask this question when we are studying the position fixed subgroup—we do so because we need to think of elements of $\mathscr{F}$ as products of basic moves, which do move pieces. To answer the question, consider the graph whose vertices are the vertices of the puzzle and whose edges join two vertices that can be obtained one from the other by the application of a single basic move. (In fact, these will correspond to the edges of the puzzle, but they should be thought of in this way.) Now choose a *tree* (see Appendix) containing all the vertices, and for each edge of the tree, choose a basic move that moves a vertex piece along that edge.

Shown below, in heavy lines, is a particular choice of a vertex tree for $\mathscr{C}$. (See Fig. 4.)

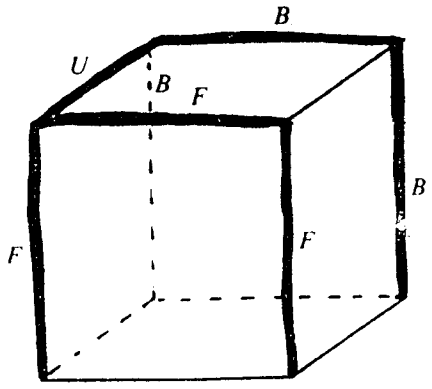



FIG. 4

The letters are the standard *Singmaster notation* (see Appendix). A tree has the property that there is only one way to get from one vertex to another in the tree. The answer to the key question, for vertex pieces, is then "compare the effect of the move in question to the effect of the unique sequence of basic moves that moves that vertex along the tree using the labeling moves on each edge." This gives a standard of comparison for every possible position change. Thus, for example, to move the lower-back-right vertex of $\mathscr{C}$ to the lower-front-right position, the standard sequence is $B^2U^{-1}F^2$. The move $R$, rotation clockwise of the right face, has a different effect—namely rotation $1/3$ of a turn clockwise from the standard.

On the general puzzle, for each move $M$ and each vertex piece $v$, we have an integer $r_v(M)$ (mod $q$) that measures how many $(2\pi/q)$ radian clockwise rotations are necessary to move the standard reference position for that vertex move to the one given by the move in question. In a similar manner, consider the edge graph whose vertices are the edge pieces of the puzzle and whose edges join pieces that can be gotten one from the other by a single basic move. The edge tree is any tree in the edge graph containing all its vertices—it is not necessary to label the edges of this tree since the moves are uniquely determined. Shown below is a particular choice of edge tree for $\mathscr{C}$, with labels included for convenience. (See Fig. 5.)

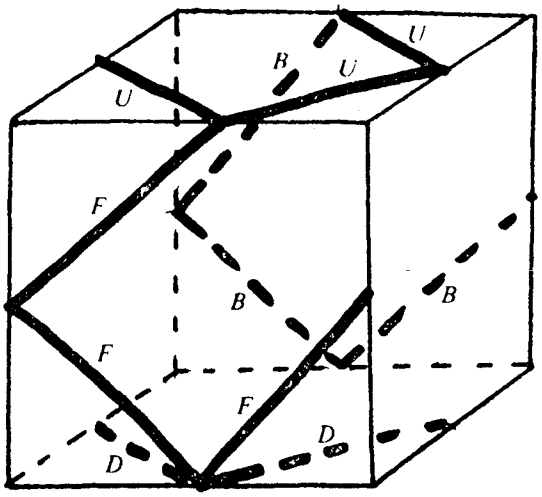



FIG. 5

Then to each move $M$ and edge piece $e$ we associate an integer $f_e(M)$ (mod 2) that measures whether or not the edge piece $e$ is flipped relative to the standard by the given move.

This defines a map

$$\mathscr{R} \xrightarrow{f\times r} \bigoplus_{1}^{E} \mathbb{Z}_2 \oplus \bigoplus_{1}^{V} \mathbb{Z}_q,$$

$$f(M) = \big(f_{e_1}(M),\ldots,f_{e_E}(M)\big), \quad r(M) = \big(r_{v_1}(M),\ldots,r_{v_V}(M)\big).$$

The proof of Lemma 2 for $\mathscr{R} \neq \mathcal{O}$ will be complete when we have verified the following claims.

*Claim* 1. $(f \times r)|\mathscr{F}$ is a homomorphism.

*Claim* 2. Image$(f \times r) \subset$ ker(Sum).

*Claim* 3. Image$(f \times r) \supset$ ker(Sum) if $\mathscr{R} \neq \mathcal{O}$.

Note that $f \times r$ is not a homomorphism on $\mathscr{R}$ because of the movement of edges and faces: in fact, it is easy to check that

$$(**) \qquad \begin{aligned} r_v(M_1M_2) &= r_v(M_1) + r_{\mu_1(v)}(M_2), \\ f_e(M_1M_2) &= f_e(M_1) + f_{\sigma_1(e)}(M_2), \end{aligned}$$

where $\text{pos}(M_1) = (\sigma_1, \mu_1)$.

Claim 1 is clear from equations (* *). It is also clear that $\text{Sum}(f \times r) = (\Sigma_e f_e, \Sigma_v r_v)$ is also a homomorphism, so that to verify Claim 2, it is only necessary to prove that $\text{Sum}(f \times r)(B) = 0$ for any basic move $B$. Suppose $B$ is the basic move of a face depicted below (we take $p = 5$ for ease of exposition—the argument is general; see Fig. 6).

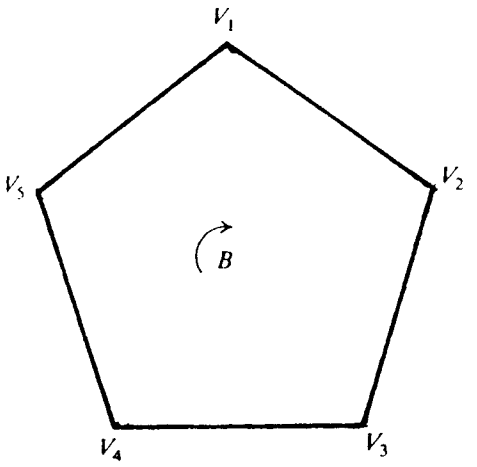



FIG. 6

The indicated vertices are the only ones moved, so

$$\text{Sum}(r(B)) = r_{v_1}(B) + r_{v_2}(B) + r_{v_3}(B) + r_{v_4}(B) + r_{v_5}(B).$$

But formula (* *) says that the right-hand side is $r_{v_1}(B^5)$, since $B^i(v_1) = v_{1+i}$. Since $B^5 = id$, $\Sigma_{i=1}^5 r_{v_i}(B) \equiv 0 \pmod 5$.

An analogous argument works on the edges.

(REMARK. It is at this point of the argument that (* *) is essential—an arbitrary method of measuring twisting and flipping would be inadequate.)

The proof of claim 3 for $\mathscr{R} \neq \mathscr{O}$ is an exercise in the use of The Method that is left to the reader: it involves explicit construction of moves whose images under $f \times r$ generate ker(Sum).

In the case of the octahedron, the above analysis holds except that:

(a) No edge flipping is possible, so that $\mathbb{Z}_2$ factors measuring flips are absent;

(b) the vertex rotations must come in units of $2(2\pi/4)$, not $2\pi/4$ as expected.

Both of these can be seen by dividing the faces into two classes—say rough-textured and smooth-textured—so that each edge separates a rough face from a smooth one. The possibility of doing this is easily seen to be equivalent to even vertex degrees. Then each basic move and so all of $\mathscr{O}$ preserves the texturing. It follows that edge pieces can't have their rough and smooth facelets interchanged nor can vertex pieces be rotated by $2\pi/4$ or $3(2\pi/4)$.

**4. The semi-direct product structure on $\mathscr{R}$.**

DEFINITION. Suppose $A$ and $B$ are groups and $\varphi$: $B \to \text{Aut}(A)$ is a homomorphism. Then the *semi-direct product* of $A$ and $B$ on $\varphi$ is $A \times B$ as a set with the product

$$(a, b)(a', b') = \big(a\varphi(b)(a'), bb'\big).$$

It is routine to check that this gives a group structure. It agrees with the direct product if and only if $\varphi$ is the trivial homomorphism. The following standard theorem describes three equivalent ways to express this notion: see for example, W. R. Scott, *Group Theory*, Prentice-Hall, NJ, 1964, p. 213.

PROPOSITION. *The following are equivalent*:

(i) *There is a split short exact sequence*

$$1 \to A \xrightarrow{\alpha} G \underset{\psi}{\overset{\beta}{\rightleftarrows}} B \to 1.$$

(ii) $G \simeq A \times_{\varphi} B$ *for some* $\varphi$.

(iii) $G$ *has two subgroups* $A$ *and* $B$ *so that*

$$A \lhd G, A \cap B = \{\mathrm{id}\} \quad \textit{and} \quad G = AB.$$

REMARK. Several $\psi$'s may correspond to the same $\varphi$: if $\psi_2(b) = \psi_1(b)c$, where $c \in$ Centralizer of $A$, then $\psi_1$ and $\psi_2$ will determine the same $\varphi$. In particular, this will happen if $A$ is abelian and $c \in A$. This illustrates how $\varphi$ may be canonical in a setting in which $\psi$ is not.

We now have the tools to complete the analysis of $\mathscr{R}$. Assume edge and vertex trees, with labels, have been chosen and let $\psi: \Sigma \to \mathscr{R}$ by

$$\psi(\sigma, \mu) = M,$$

where $\mathrm{pos}(M) = (\sigma, \mu)$ *and* $f_v(M) = r_p(M) = 0$ for all $v$ and $e$. $(**)$ implies that $\psi$ is a homomorphism. Corresponding to $\psi$, we have $\varphi: \Sigma \to \mathrm{Aut}(\mathscr{F})$ by

$$\varphi(\sigma, \mu)((f_1, \ldots, f_E), (r_1, \ldots, r_V)) = (\sigma(f_1, \ldots, f_E), \mu(r_1, \ldots, r_V)),$$

where $\sigma(f_1, \ldots, f_E)$ and $\mu(r_1, \ldots, r_V)$ are the sequences obtained by permuting the entries according to $\sigma$ and $\mu$.

THEOREM. (i) *The following is a split exact sequence*:

$$1 \to \mathscr{F} \to \mathscr{R} \underset{\psi}{\overset{\mathrm{pos}}{\rightleftarrows}} \Sigma \to 1.$$

(ii) $\mathscr{R} \simeq \mathscr{F} \times_{\varphi} \Sigma$.

(iii) $\mathscr{R}$ *has subgroups* $\mathscr{F}$ *and* $\psi(\Sigma)$ *such that* $\mathscr{F} \lhd \mathscr{R}$, $\mathscr{F} \cap \psi(\Sigma) = \{\mathrm{id}\}$ *and* $\mathscr{F}\Sigma = \mathscr{R}$.

*Proof.* By the proposition, it suffices to prove any one of the three and to check that $\psi$ and $\varphi$ are correctly related. That $\psi$ splits pos is immediate, verifying (i). The proposition says that $\varphi(\sigma, \mu)$ $(f)$ should "permute the edges and faces by $\sigma$ and $\mu$ without flips or twists—then flip and twist according to $f$—then restore edges and faces to their original positions without flips or twists." This is clearly just what $\varphi(\sigma, \mu)$ $(f)$ does. We point out that $\psi$ was not canonical, depending on the choice of tree, but $\varphi$ *is* canonical.

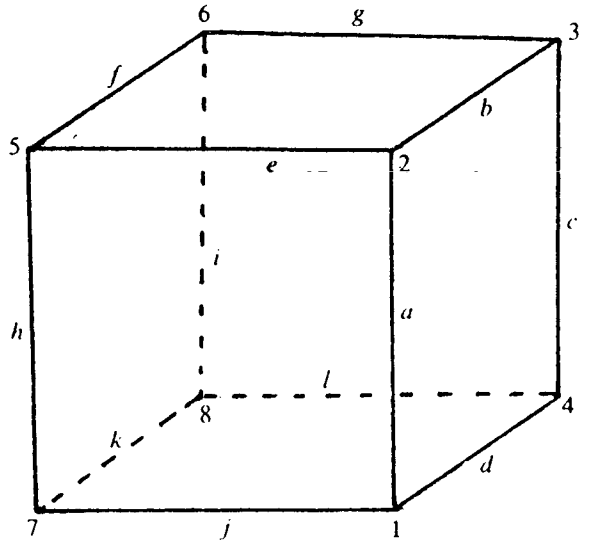



FIG. 7

The theorem gives an explicit description of $\mathscr{R}$ which provides a convenient notation that we illustrate for Rubik's Cube. We label the vertex and edge pieces of $\mathbf{C}$ with numbers and letters

respectively as below, relative to which the permutations induced by the basic moves in Singmaster's notation can be easily determined. (See Fig. 7.)

| Move | Value of pos |
|---|---|
| $R$ | $((a\ b\ c\ d),\ (1\ 2\ 3\ 4))$ |
| $L$ | $((i\ f\ h\ k),\ (5\ 7\ 8\ 6))$ |
| $U$ | $((b\ e\ f\ g),\ (3\ 2\ 5\ 6))$ |
| $D$ | $((d\ l\ k\ j),\ (1\ 4\ 8\ 7))$ |
| $F$ | $((a\ j\ h\ e),\ (2\ 1\ 7\ 5))$ |
| $B$ | $((c\ g\ i\ l),\ (4\ 3\ 6\ 8))$ |

Now using the vertex and edge trees for **C** given in §3, we can determine the flip or rotation effect on each piece moved—the effects are filled in below in the gap representing the piece move with the absence of a label indicating zero.

| Move | Extended notation |
|---|---|
| $R$ | $((a^1\ b^1\ c^1\ d^1),\ (1^1\ 2^1\ 3\ 4^1))$ |
| $L$ | $((i^1\ f^1\ h^1\ k^1),\ (5^1\ 7^1\ 8^1\ 6))$ |
| $U$ | $((b\ e\ f\ g),\ (3\ 2^1\ 5^1\ 6^1))$ |
| $D$ | $((d\ l\ k\ j),\ (1^1\ 4^1\ 8\ 7^1))$ |
| $F$ | $((a\ j\ h\ e),\ (2\ 1\ 7\ 5))$ |
| $B$ | $((c\ g\ i\ l),\ (4\ 3\ 6\ 8))$ |

Clearly the extended notation determines the move completely. Furthermore, composition of moves is described by multiplying permutations in the usual way (left one applied first) and filling each gap with the sum of the numbers in the gaps that give rise to it. For example

$$RU = \left((a^1\,b^1\,c^1\,d^1),(1^1\,2^1\,3\,4^1)\right)\cdot\left((b\,e\,f\,g),(3\,2^1\,5^1\,6^1)\right)$$
$$= \left((a^1\,e\,f\,g\,b^1\,c^1\,d^1),(1^2\,5^1\,6^1\,3\,4^1)(2^1)\right)$$

where, e.g.,

$$1 \xrightarrow[R]{1} 2\tfrac{1}{U}5 \Rightarrow 1 \xrightarrow[(RU)]{2} 5.$$

This notation allows us to easily draw a non-obvious conclusion. Note first that it is a relatively easy exercise to check that any move can be effected without using one of the six moves—The Method, for example, can be used to show how to obtain the effect of $F$ from the other 5.

CLAIM. *It is not generally possible to solve the cube using only* 4 *of the* 6 *moves.*

*Easy proof.* If the two stationary faces are adjacent, the edge piece between them can't be moved, and the claim is obvious. If not, they are opposite and we may assume, without loss of generality, that they are $R$ and $L$. But a glance at the chart shows that this makes edge flipping relative to the chosen tree impossible. Q.E.D.

**5. Some group theory related to the method.** In this section we describe some interesting subgroups of $\mathscr{R}$ generated by basic commutators which provide *almost* all the moves needed to solve a puzzle. We encounter two groups $K$ and $I$—discussed below—that are interesting in their own right. Verification of statements not explicitly discussed is tedious but routine.

DEFINITION. For group $\mathscr{R}$ and a degree $q$ vertex $v$ of the corresponding solid, $\mathscr{R}_v$ is the

subgroup generated by basic commutators of the form $\mathbf{C} = [L, R^{-1}]$ for the $q$ pairs of adjacent faces containing $v$. For an edge $e$, $\mathscr{R}_e$ is the subgroup generated by all commutators of moves of the two faces separated by $e$—namely $[L, R]$, $[L^{-1}, R]$, $[L, R^{-1}]$ and $[L^{-1}, R^{-1}]$.

*The groups $\mathscr{R}_v$*

$\mathscr{R}_v$ moves $q$ edges and $q + 1$ vertices. In all cases, any edge flip, corner rotation or even edge permutation of these pieces possible in $\mathscr{R}$ is also possible in $\mathscr{R}_v$—the interest lies in the realizable vertex permutations.

*Case* (i). $\mathscr{R} = \mathscr{T}, \mathscr{C}, \mathscr{D}$ $(q = 3)$; Image(pos) $= A_3 \times K$.

*Case* (ii). $\mathscr{R} = \mathscr{O}$ $(q = 4)$; Image(pos) $= A_4 \times A_5$.

*Case* (iii). $\mathscr{R} = \mathscr{I}$ $(q = 5)$; Image(pos) $= A_5 \times I$.

*The groups $\mathscr{R}_e$*

If faces have degree $p = 3$ (respectively $p = 4, 5$) then $\mathscr{R}_e$ moves 5 edges and 4 vertices (respectively 5 edges and 6 vertices). $\mathscr{R}_e$ has no flip or rotation effect (pick the right tree) so $\mathscr{R}_e$ is isomorphic to Image(pos).

*Case* (i). $\mathscr{R} = \mathscr{T}, \mathscr{O}, \mathscr{I}$ $(p = 3)$ Image(pos) $= A_5 \times K$.

*Case* (ii). $\mathscr{R} = \mathscr{C}, \mathscr{D}$ $(p = 4, 5)$ Image(pos) $= A_5 \times I$.

*The Klein four group K*

$K$ is the four element subgroup of $A_4$ consisting of double transpositions. That double transpositions do not generate $A_4$ (as they do $A_n$ for $n \geqslant 5$) indicates why it is necessary to bring in the move $B$ in Step 3 of The Method. Abstractly, $K$ is just $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

*The icosahedral group I*

$I$ is the subgroup of $A_6$ generated by the two 5-cycles $X = (12345)$ and $Y = (16235)$ obtained as follows. For $\mathscr{R}_v$, case (iii), label vertices as shown in Fig. 8 and let $\mathbf{C}_1, \mathbf{C}_2, \ldots, \mathbf{C}_5$ be the basic commutators corresponding to edges 1–6, 2–6, ..., 5–6; then

$$X = (12345) = \mathbf{C}_4^{-1}\mathbf{C}_1\mathbf{C}_2\mathbf{C}_4$$

$$Y = X^{-1}(\mathbf{C}_1\mathbf{C}_5)^2 X.$$

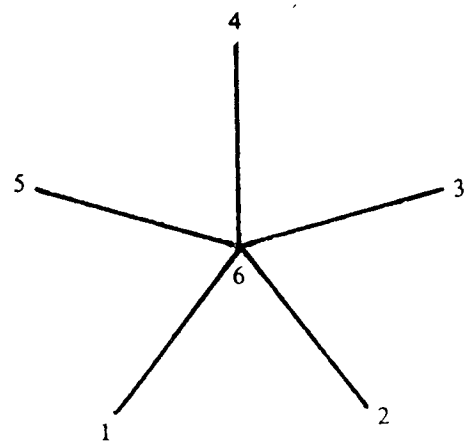



FIG. 8

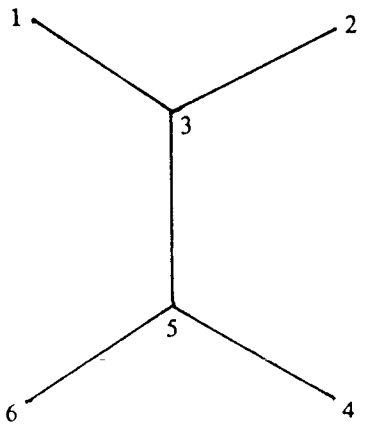



FIG. 9

$\mathbf{A} = [L, R]$

$\mathbf{B} = [L^{-1}, R]$

$\mathbf{C} = [L, R^{-1}]$

$\mathbf{D} = [L^{-1}, R^{-1}]$

For $\mathscr{R}_e$, case (ii), label vertices as shown in Fig. 9; then $X = \mathbf{CA}$, $Y = (\mathbf{CD})^2$.

$I$ is a very famous group which occurs naturally in a number of different settings and is known by names that reflect its various origins. It has order 60 and is the smallest example of a non-abelian simple group (see Appendix). We end with four descriptions of $I$ other than as Image(pos).

(1) $I \simeq \langle X, Y | X^5 = Y^5 = (XY)^3 = (Y^{-1}X)^2 = 1 \rangle$.

This notation, from combinational group theory, means that $I$ is a group characterized by the fact that it has two generators $X$ and $Y$ satisfying the listed relations and such that any other relations are derivable from these together with the group axioms. Descriptions of this type, called presentations, are completely general and very efficient but rarely display the special characteristics that make a group interesting.

(2) $I \simeq A_5$, *the alternating group on 5 letters*.

This is the most familiar form of $I$. Here

$$X = (12534),$$
$$Y = (13452).$$

In this form, it is clear that $I$ has elements of orders 1, 2, 3 and 5 only and it's easy to count how many of each there are. Furthermore, all elements of order 2 are conjugate, all of order 3 conjugate and there are two conjugacy classes of elements of order 5.

(3) $I \simeq \mathrm{PSL}(2,5)$.

$$\mathrm{SL}(2,5) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a, b, c, d \in \mathbb{Z}_5, ad - bc = 1 \right\}.$$

$$\mathrm{PSL}(2,5) = \frac{\mathrm{SL}(2,5)}{\{\pm I\}}.$$

Here

$$X = \left[ \begin{pmatrix} 4 & 1 \\ 1 & 3 \end{pmatrix} \right] \quad \text{and} \quad Y = \left[ \begin{pmatrix} 1 & 0 \\ -3 & 1 \end{pmatrix} \right].$$

(4) $I \simeq$ *the symmetry group of the icosahedron*.

In this incarnation, $I$ is the group of rigid motions of the icosahedron—i.e., length and angle preserving linear maps (orthogonal maps) of $\mathbb{R}^3$ that carry an icosahedron centered at the origin back onto itself. Every orthogonal map of $\mathbb{R}^3$ is a rotation about some straight line through the origin and those in the icosahedral group are of three types depending on whether the line passes through the center of an edge, the center of a face or a vertex. If $L$ and $R$ denote adjacent faces as well as clockwise rotation about the line through the center of the faces, then

$$X = R,$$
$$Y = L^2.$$

It is a delightful coincidence that the icosahedral group appears in the analysis of the icosahedral puzzle.

**Appendix 1—Definitions.**

*Regular Solid.* A regular or Platonic solid is a convex solid bounded by planar faces each of which is a regular polygon with the same number of edges and such that the same number of faces meet at each vertex. It was known to the ancient Greeks that Table 1 lists all possibilities—a proof appears in Book 13 of Euclid's Elements.

*Commutator.* The commutator of $x$ and $y$ in a group $G$ is $[x, y] = xyx^{-1}y^{-1}$. (Some authors

use $[x, y] = x^{-1}y^{-1}xy$.) It measures the degree to which $x$ and $y$ fail to commute with one another.

*Conjugate.* In a group $G$, $a$ is conjugate to $b$ if there is a $c$ so that $a = cbc^{-1}$. Conjugate permutations always have the same cycle structure.

*Free group.* A free group is a group free of any relations not demanded by the group axioms. A group free on symbols $X_1, \ldots, X_n$ is the set of all strings—called words—of $X_i$'s with exponents $\pm 1$ in which occurrences of $X_i X_i^{-1}$ and $X_i^{-1} X_i$ have been deleted, together with 1 interpreted as the empty word. The multiplication is just juxtaposition followed by the above deletions. The discipline of combinatorial group theory views all groups as quotients of free groups as in the first description of $I$ in Section 5.

*Exact sequence, short exact sequence.* An exact sequence is a sequence of group homomorphisms such that the image of each is the kernel of the next. A short exact sequence (the only kind considered in this paper) is 5 terms long, beginning and ending with trivial groups.

$$1 \to A \xrightarrow{\alpha} G \xrightarrow{\beta} B \to 1.$$

If all groups in the sequence are abelian, denote the trivial group by 0: otherwise 1.

*Split short exact sequence.* A splitting of the exact sequence above is a map $\psi$: $B \to G$ such that $\beta \circ \psi(b) = b$. If $G$ is abelian, the existence of a splitting says that $G$ is the direct sum of $A$ and $B$: this follows from the Proposition of §4.

*Tree.* A graph is a tree if it is connected and contains no cycles. This is the same (for finite graphs) as saying that the number of vertices is one more than the number of edges. An important property of a tree is that there is exactly one way to get from one vertex to another in the tree without retracing.

*Singmaster notation.* Singmaster's notation—which has become standard—denotes the basic moves on the Rubik's cube by letters indicating the face being rotated clockwise (see Fig. 10):

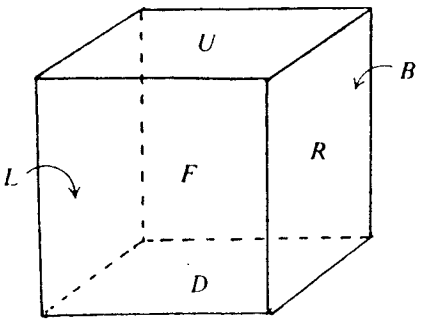



FIG. 10

| | | |
|---|---|---|
| $L$ = left | $U$ = up | $F$ = front |
| $R$ = right | $D$ = down | $B$ = back. |

(*Note*: $L$ and $R$ here should not be confused with $L$ and $R$ in The Method).

*Canonical.* A map or construction is canonical if it does not depend on arbitrary choices. In §3, $\varphi$ is canonical but $\psi$ is not, since $\psi$ depends on the trees chosen.

*Simple group.* A group is simple if it has no non-trivial normal subgroups, or equivalently, no non-trivial quotients.