The Mathematics of the Rubik's Cube

By Daniel Bump

Chapter 1
The Group of the Cube

In this chapter, we will explain how the operations of the Rubik's cube comprise an algebraic structure known as a *group*. The theory of groups is the natural domain for studying the Rubik's cube.

Definition 1.1. *A* group *is a set G with a multiplication law that associates to every pair of elements x and y of G an element xy (also denoted $x \cdot y$) such that the following properties are true. This multiplication is called the* group law*.*

(i) The associative law is satisfied:

$$x(yz) = (xy)z;$$

(ii) There is a particular element $1 \in G$ such that $1x = x1 = x$;
(iii) If $x \in G$ then there is an element x^{-1} such that $x \cdot x^{-1} = x^{-1} \cdot x = 1$.

If the *commutative law*

$$xy = yx$$

is also satisfied, the group is called *abelian*.

Example 1.2. The set $\mathbb{R}^{\times}$ of nonzero real numbers forms a group. The group law is ordinary multiplication. Notice that 0 is *not* an element of this group.

The group law does not have to be written multiplicatively. Sometimes it is more natural to write the group additively. In this modification, we write $x + y$ instead of xy, 0 instead of 1 and $-x$ instead of x^{-1}. Axioms (i), (ii) and (iii) in the definition of a group are written this way in the additive notation:

$$x + (y + z) = (x + y) + z;$$

$$0 + x = x + 0 = x;$$

and

$$x + (-x) = (-x) + x = 0.$$

In practice the additive notation is used *only* for abelian groups; this if we use the additive notation in a group it is understood that the commutative law is true, which in additive notation reads

$$x + y = y + x.$$

Example 1.3. The set $\mathbb{R}$ of all real numbers is a group. The group law is ordinary addition.

Both these examples are of infinite groups, and both are abelian. The next example is of a finite group that is not abelian.

Example 1.4. Let $G = \{1,\ a,\ b,\ c,\ d,\ e\}$ with the multiplication table in Table 1.1.

$\times$	1	t	u	v	w	x
1	1	t	u	v	w	x
t	t	u	1	w	x	v
u	u	1	t	x	v	w
v	v	x	w	1	u	t
w	w	v	x	t	1	u
x	x	w	v	u	t	1

Table 1.1. A finite group of order six. The product is left $\times$ top, so $tv = w$, not x.

To check that the group axioms (i)–(iii) are satisfied, we will give two concrete realizations of this group.

Example 1.5. Let Ω be a set with n elements, and let S_n be the set of all bijective maps $\sigma\colon \Omega \longrightarrow \Omega$. For definiteness, we may take

$$S = \{1, 2, 3, \cdots, n\}.$$

If σ and τ are two elements of G, then $\sigma\tau$ is the composition map from Ω to Ω. Thus

$$(\sigma\tau)(x) = \sigma(\tau(x)).$$

Note that $\sigma\tau$ is the map *first* τ, *then* σ, so we perform the operations in S_n *from right to left*. The group S_n is called the *symmetric group of degree* n, and its elements are called *permutations*. It is clear that S_n is a group.

Example 1.6. Let us label the elements of S_3 as follows. With $\Omega = \{1, 2, 3\}$, we will denote by

$$\begin{pmatrix} 1 & 2 & 3 \\ a & b & c \end{pmatrix}$$

the map $\sigma\colon \Omega \longrightarrow \Omega$ such that $\sigma(1) = a$, $\sigma(2) = b$ and $\sigma(3) = c$. Let

$$1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \qquad t = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \qquad u = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$
$$v = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \qquad w = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \qquad x = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

Then one may check that the multiplication table of Table 1.1 is satisfied.

Exercise 1.1. Check with this labeling that Table 1.1 is the multiplication table of S_3.

Example 1.7. Let T be an equilateral triangle. Let $\mathfrak{T}$ be the following group. It has six elements, each of which is an operation on T consisting of a rotation or reflection. We consider the triangle as "movable," that is, something that can be physically reoriented in space, just like the pieces of the Rubik's cube. By an *operation* on T we mean a transformation of the underlying space that takes T to itself. For example, $\mathfrak{T}$ has an element, that we call t, that rotates the triangle clockwise in an angle of $\frac{2\pi}{3} = 120°$, and is shown in Figure 1.1.

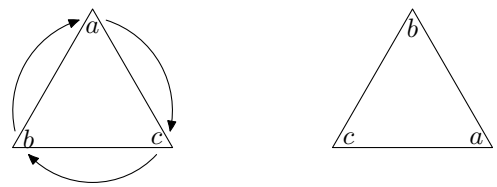

Figure 1.1. The operation t. Left: before. Right: after.

Also, let x be the operation that is a flip in the vertical axis, as in Figure 1.2.

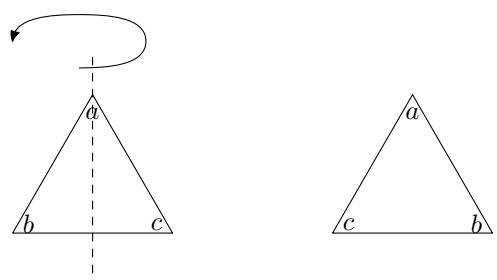

Figure 1.2. The operation x. Left: before. Right: after.

One might want to think of these operations of mappings of the triangle to itself, but we prefer not to do so, for reasons we will now explain. If one tries to interpret x as a mapping of T to itself, Figure 1.1 suggests that it should be interpreted as the permutation that sends a to itself and interchanging b and c. That is, when T is in the configuration of Figure 1.1, the effect of x is the same as that of the permutation

$$\begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}$$

of $\{a, b, c\}$.

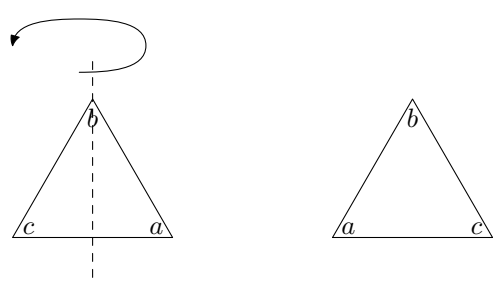

Figure 1.3. Left: initial position. Right: after the operation x.

But what if we apply x to the triangle in the position on the left in Figure 1.3? In this case, clearly we should arrive at the rightmost position in Figure 1.3. The effect is that a and c have been switched. Thus when applied to T in this configuration, it has the same effect as the permutation

$$\begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix}.$$

This is not the same transformation as before! Since the permutation that x causes on the three vertices $\{a, b, c\}$ of the cube depends on the orientation of the cube, we prefer not to be too quick to identify $\mathfrak{T}$ with the group of permutations of this set.

There is another difference between this group and the permutation group S_3: we have explained that in S_3 we parse $\sigma\tau$ as the permutation obtained by doing first τ, then σ, so that we apply the mappings in order from right to left. By contrast, in $\mathfrak{T}$, we will do operations from left to right. Thus tx means *first t, then x*. (It will turn out this is the most natural way.)

Let us compute tx. Applying first t, then x to a labeled triangle, we get the sequence of triangles in Figure 1.4.

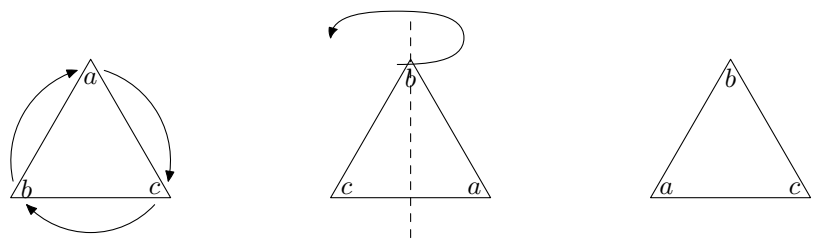

Figure 1.4. Computing tx in the group $\mathfrak{T}$.

We see that tx coincides with a reflection in the axis shown in Figure 1.5.

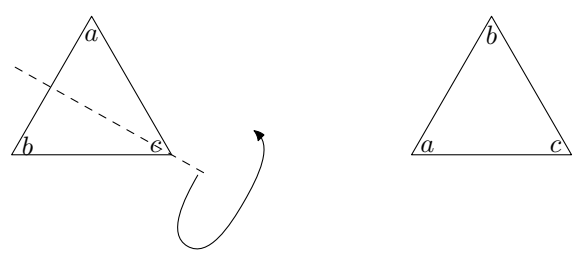

Figure 1.5. The operation v.

Exercise 1.2. List the six operations in the group $\mathfrak{T}$, and show that they can be labeled as $1, t, u, v, w, x$ in such a way that the multiplication table Table 1.1 is correct.

Exercise 1.3. Check the formula $vtv^{-1} = t^{-2}$ in both S_3 and $\mathfrak{T}$, with the elements labeled as above.

We will next consider the Rubik's cube, and show that there is associated with it a group that is (like Example 1.4) finite and nonabelian.

Rubik has always insisted on from the manufacturers is a coloring scheme is followed to this day. Red is opposite orange, blue opposite green and yellow opposite white. Your cube should look like that in Figure 1.6 when solved, though it might be a mirror image.

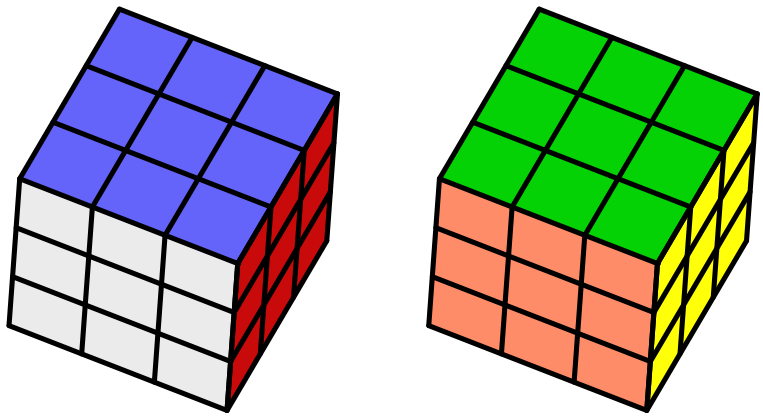

Figure 1.6. Top and bottom views of a solved cube.

Figure 1.6 shows the whole cube in two views. The cube is viewed from the top in the left figure, and from the bottom in the right figure.

It is also useful to give a single "stereographic" image of the cube showing *most* of the cube in a single view, as in Figure 1.7. Everything except the bottom (green) face is visible.

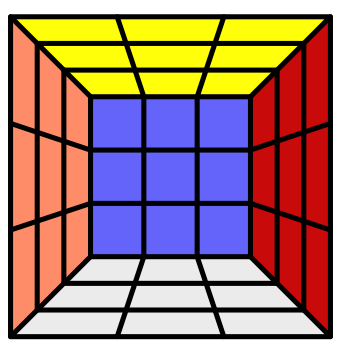

Figure 1.7. Stereographic view of the solved cube.

Following cube pioneer David Singmaster, we label the six sides of the cube with the names "up," "down," "left," "right," "front," "back," and "down," with a 1-letter mnemonic as in Table 1.2. The names "up" and "down" are used instead of "top" and "bottom" (or "truth" and "beauty") so that the letter 'B' is not overloaded (it already stands for "back").

Face	Mnemonic	Color in Figure 1.6 or 1.7
Up	U	Blue
Down	D	Green
Right	R	Red
Left	L	Orange
Front	F	White
Back	B	Yellow

Table 1.2.

Singmaster's notion extends to operations on the cube, such as turning one of the faces. If X is one of the faces of the cube, then X denotes the operation of rotating the face through an angle of $\frac{\pi}{2} = 90°$ in the *clockwise* direction, while X^{-1} denotes the operation of rotating the X face through an angle of 90° in the counterclockwise direction. Thus, starting with the solved cube as in Figure 1.6, after R^{-1} the cube looks as in Figure 1.8. Following Singmaster, we will use the notation R' interchangeably with R^{-1}.

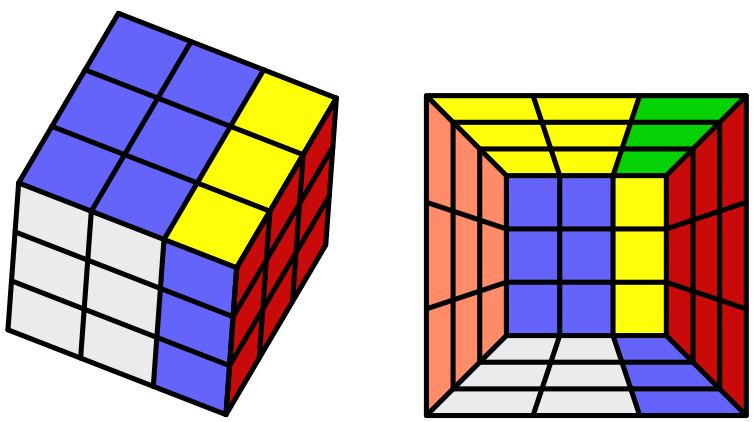

Figure 1.8. After $R^{-1} = R'$ is applied to a solved cube.

If g is any operation of the cube we will denote by g^n the operation g done n times, and 1 will denote the operation which doesn't change anything, so if X is the rotation of a face, $X^4 = 1$ while $X^3 = X^{-1}$.

In addition to the operations U, D, R, L, F and B, it is useful to introduce operations U_0, D_0, R_0, L_0, F_0 and B_0 that turn the *whole cube*. Thus if X denotes a face, X_0 is the operation that turns that face clockwise, and turns the whole cube. These operations are frequently omitted in defining the group of the cube, since obviously turning the whole cube does not affect its configuration in any essential way. Nevertheless they are very important. We note that $U_0 = D_0^{-1}$, $R_0 = L_0^{-1}$ and $F_0 = B_0^{-1}$ since (for example) turning the whole cube clockwise while looking at the front is the same as turning it counterclockwase while looking at the back.

Next introduce the *middle layer moves*. If X is a face, and Y is the opposite face, then X_m will denote the operation that rotates just the middle layer *between* the X and Y faces clockwise (looking at X face) in an angle of $\frac{\pi}{2} = 90°$. Thus Figure 1.9 shows the operation U_m. It is clear that X_m and Y_m are inverses.

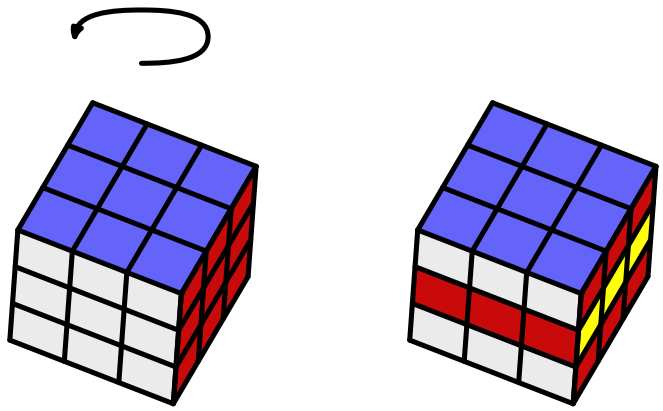

Figure 1.9. Left: initial state. Right: After the middle layer move U_m.

We can concatenate operations of the cube. Thus if X and Y are operations of the cube, then XY is the operation consisting of first doing X, then doing Y. For example, Figure 1.10 shows the effect of RF. Just as in algebra we might write the product a times b as, alternatively, ab, $a \cdot b$ or $a \times b$, we will similarly feel free to denote the result of concatenating X and Y by XY, $X \cdot Y$ or $X \times Y$.

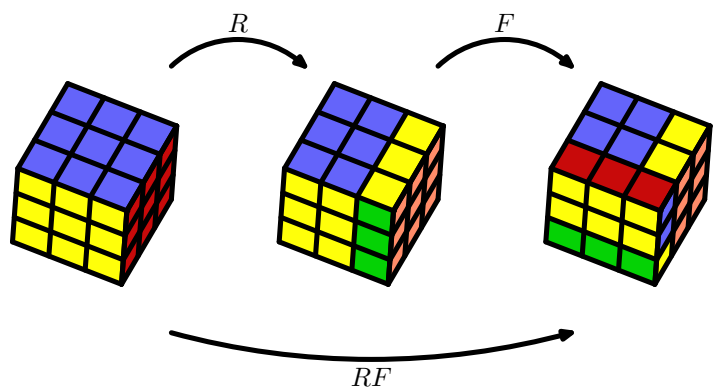

Figure 1.10. RF is the operation "first R then F"

We think of concatenation as a sort of multiplication. Let $\mathfrak{G}_0$ denote the set of all possible operations of the cube that can be constructed out of the ones we have already defined: U, D, F, B, L, R, U_0, D_0, F_0, B_0, L_0, R_0, U_m, D_m, F_m, B_m, R_m and L_m.

Remark. A case can be made for omitting U_0, D_0, R_0, L_0, F_0, U_m, D_m, F_m, B_m, R_m and L_m from the group of the cube, and working only with U, D, F, B, L and R (which do not move the centers). After all, the operations U_0, D_0, F_0, B_0, R_0 and L_0 don't really affect the configuration of the cube, they just rotate the whole thing, so in some sense they are superfluous. Nevertheless we include them, and will give a reason later.

Remark. Once one has the operations U, D, F, B, L, R, U_0, D_0, F_0, B_0, L_0, R_0 one can construct the operations U_m, D_m, F_m, B_m, L_m and R_m. For example,

$$U_m = U_0 U^{-1} D,$$

since if we turn the whole cube, then turn back the up and down faces, the net effect is just to turn the middle layer.

Theorem 1.8. *With the operation of concatenation as its multiplication, $\mathfrak{G}_0$ is a group.*

Proof. First we check that the "associative law"

$$(XY)Z = X(YZ)$$

is satisfied. Indeed $(XY)Z$ means first doing the operation XY, then the operation Z, while $X(YZ)$ means first do the operation X, then the operation YZ. In either case, the net effect is to do X first, then Y, and finally Z. We have checked Axiom (i) of Definition 1.1.

There is one particular operation which has no effect: this is the operation I which stands for "do nothing." It is a sort of a unit in the group $\mathfrak{G}_0$ since if X is any operation, we clearly have

$$I \cdot X = X \cdot I = X.$$

This confirms Axiom (ii) of Definition 1.1.

Finally, if X is an operation of the cube, then X^{-1} denotes the operation that undoes whatever X does. This is logical, since

$$X \cdot X^{-1} = X^{-1} \cdot X = I.$$

Indeed, if we do the operation X, then undo it, this has the same effect as doing nothing. □

Proposition 1.9. *If X and Y are elements of a group G, then*

$$(XY)^{-1} = Y^{-1}X^{-1}. \tag{1.1}$$

Proof. This is easily checked by multiplying XY and $Y^{-1}X^{-1}$ together. We get

$$XY \cdot Y^{-1}X^{-1} = X(YY^{-1})X^{-1} = XIX^{-1} = XX^{-1} = I,$$

so XY and $Y^{-1}X^{-1}$ are inverses of each other, and (1.1) follows. □

Exercise 1.4. Let G be the group of transformations that take an equilateral triangle into itself. There are six elements of G: the identity, three reflections and two rotations. Give names to these elements and compute the multiplication table of G.

Exercise 1.5. Repeat the last exercise for the square. This time there are eight transformations.

Exercise 1.6. Let G be a group and $u \in G$ a fixed element. Define a map $f: G \longrightarrow G$ by $f(g) = ugu^{-1}$. Prove that $f(gh) = f(g)f(h)$ and that $f(g^{-1}) = f(g)^{-1}$.

Chapter 2

A minimal repertoire

Solving the cube means taking a scrambled cube and restoring it. As one approaches completion, one needs to be able to move pieces that are out-of-place without disturbing ones that are already correctly positioned. One therefore needs to know operations that only move a few pieces.

Fortunately there are operations that only move a few pieces at a time. The most important ones are *3-cycles* that only move three pieces – either three edges or three corners.

In order to solve the cube, it is sufficient to memorize about 4 or 5 operations, and their mirror images. We will give a short list consisting of 3 edge 3-cycles, one corner 3-cycle and one other operation that affects the orientation of the corners but not their position. One also needs to know a trick called "conjugation" that vastly expands the usefulness of an operation.

We will describe a few operations in this Chapter that can be used to solve the cube. In the next Chapter, only 4 of these will be required: $\alpha_1, \alpha_3, \beta$ and γ; we will also assume that the reader can do the mirror image operations of the first two and last of these moves, which will be denoted $\alpha_1^\dagger$, $\alpha_3^\dagger$, and $\gamma^\dagger$. Two other operations, called α_2 and ϕ will also be described. These other operations can sometimes be used to shorten the process.

There are many other useful operation that can be used. We will encounter others in the course of the book.

2.1 Edge 3-cycles

First, three edge 3-cycles. We show the effect of each operation by demonstrating what happens to a pristine cube when it is applied. In Figure 2.1, we see the effect of the operation $\alpha_1 = RU^{-1}R^{-1}\,U_mRUR^{-1}U_m^{-1}$. Note that three edge pieces are permuted cyclicly.

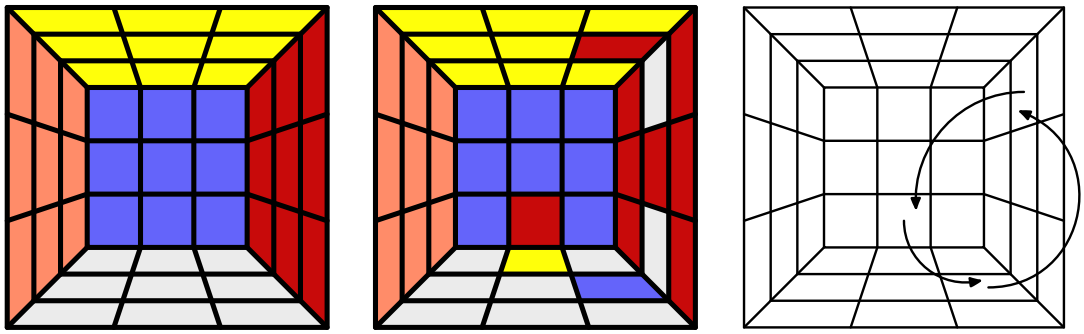

Figure 2.1. Left: Pristine cube. Middle: after $\alpha_1 = RU^{-1}R^{-1}U_mRUR^{-1}U_m^{-1}$. Right: the effect is to permute three edges cyclicly. This is an *edge 3-cycle*.

Similarly in Figure 2.2 and Figure 2.3 we have two further edge 3-cycles. The three operations are:

- $\alpha_1 = RU^{-1}R^{-1}U_mRUR^{-1}U_m^{-1}$,
- $\alpha_2 = RU^{-1}R^{-1}U_m^2RUR^{-1}U_m^2$,
- $\alpha_3 = RU^{-1}R^{-1}U_m^{-1}RUR^{-1}U_m$.

These three operations are quite similar to each other, and each has a "rhythm" that makes it easy to remember. Each puts the up-front edge piece (which we will denote UF into the front right position (denoted FR). The FR piece goes to one of three possible locations, either RB (right-back) or BL (back-left) or RF (right-front).

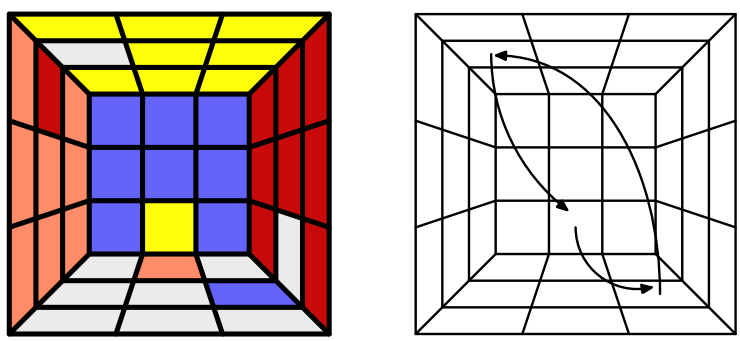

Figure 2.2. Left: after $\alpha_2 = RU^{-1}R^{-1}U_m^2RUR^{-1}U_m^2$. Right: the effect of this edge 3-cycle.

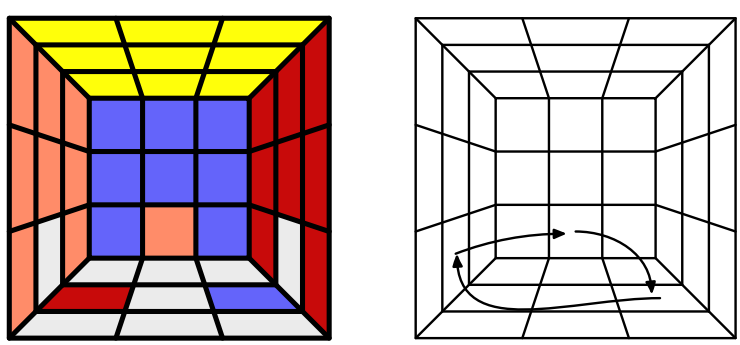

Figure 2.3. Left: after $\alpha_3 = RU^{-1}R^{-1}U_m^{-1}RUR^{-1}U_m$. Right: the effect of this edge 3-cycle.

A good way to practice these operations is to start with a pristine cube, then do the operation *3-times*. This will return the cube to its pristine state.

In addition to α_1, α_2 and α_3, it is a good idea to have command of their mirror image operations. If one knows a cube operation it is a small matter to perform a mental adjustment and do the mirror image operation. This is a curious point of psychology since this reversal does not work well with handwriting. For the record, the mirror image operations are:

- $\alpha_1^\dagger = L^{-1}ULU_m^{-1}L^{-1}U^{-1}LU_m$,
- $\alpha_2^\dagger = L^{-1}ULU_m^2L^{-1}U^{-1}LU_m^2$,
- $\alpha_3^\dagger = L^{-1}ULU_mL^{-1}U^{-1}LU_m^{-1}$.

Their effects are shown in Figure 2.4.

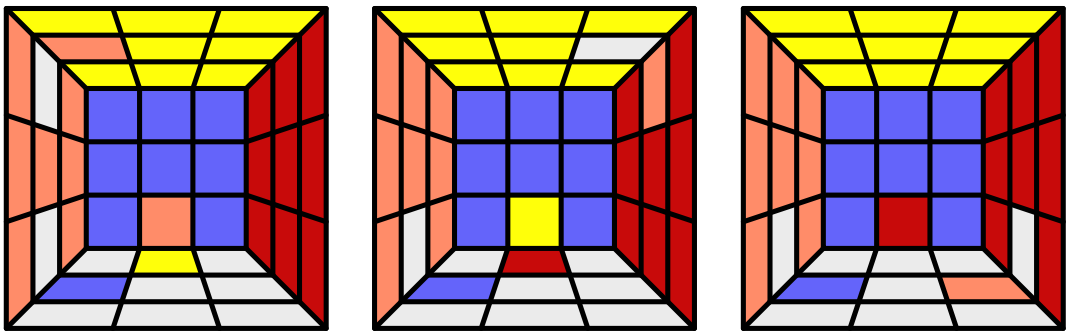

Figure 2.4. The mirror image operations. Left: $\alpha_1^\dagger = L^{-1}ULU_m^{-1}L^{-1}U^{-1}LU_m$; Middle: $\alpha_2^\dagger = L^{-1}ULU_m^2L^{-1}U^{-1}LU_m^2$; Right: $\alpha_3^\dagger = L^{-1}ULU_mL^{-1}U^{-1}LU_m^{-1}$.

2.2 A corner 3-cycle

Next we come to the corner 3-cycle $\beta = FRF^{-1}LFR^{-1}F^{-1}L^{-1}$. Its effect is shown in Figure 2.5. There are many corner 3-cycles; the method that we will describe of solving the cube only requires one, and this one will do. You will not need the mirror image operation.

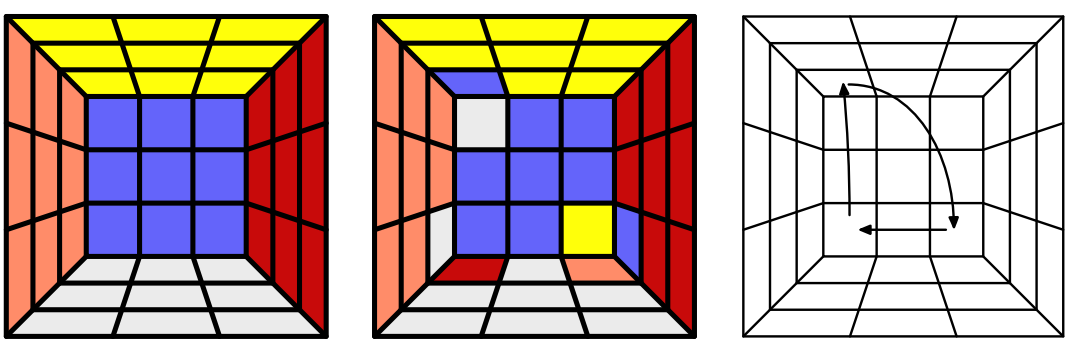

Figure 2.5. The corner 3-cycle $\beta = FRF^{-1}LFR^{-1}F^{-1}L^{-1}$. Left: before. Middle: after. Right: three corners are permuted.

2.3 A supplementary corner operation

Another operation that is sometimes useful in putting the top corners into place is $\phi = FRUR^{-1}U^{-1}F^{-1}$. *This operation is not required for the algorithm that we will describe for solving the cube.* The reader may therefore skip this operation. However, it is easy to remember and can shorten one of the steps (Section 4.5).

The effect of ϕ is shown in Figure 2.6. It will be noted that the top corners are interchanged in pairs, and an edge three-cycle is also effected.

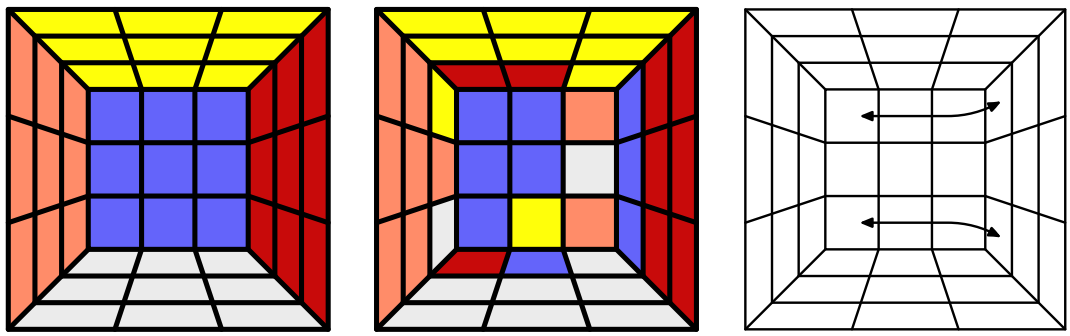

Figure 2.6. The operation $FRUR^{-1}U^{-1}F^{-1}$. Left: before. Middle: after. Right: this affects both top corners and top edges. Here we are interested only in the effect on the corners.

If the edge 3-cycle is a defect, one wishes to have an operation that affects the top corners by interchanging them in pairs (as in Figure 2.6, right) but that has no effect on the edges, one may repeat $FRUR^{-1}U^{-1}F^{-1}$ three times. This gives us the operation

$$(FRUR^{-1}U^{-1}F^{-1})^3 = F(RUR^{-1}U^{-1})^3F^{-1}. \tag{2.1}$$

This is an easy operation to remember and to perform quickly.

Exercise 2.1. Explain why the two operations in (2.1) are the same.

2.4 Corner twists

Finally, we have the operation $\gamma = RUR^{-1}URU^2\,RU^2$, whose effect is shown in Figure 2.7 (left). It is valuable for its effect on the corners. These are not moved, but three of the corners are twisted, each by an angle of $120° = \frac{2\pi}{3}$ (clockwise). See Figure 2.7 (middle).

In addition to twisting the three corners, γ also permutes three edges in a 3-cycle. This may be regarded as a defect. It is sometimes useful to know that if one omits the final U^2 and follows the operation by its mirror image, one obtains

$$RUR^{-1}URU^2\,R \cdot L^{-1}U^{-1}LU^{-1}L^{-1}U^2L.$$

This operation has the effect of twisting two corner pieces, one clockwise and counterclockwise, and the edges are untouched. See Figure 2.7 (right).

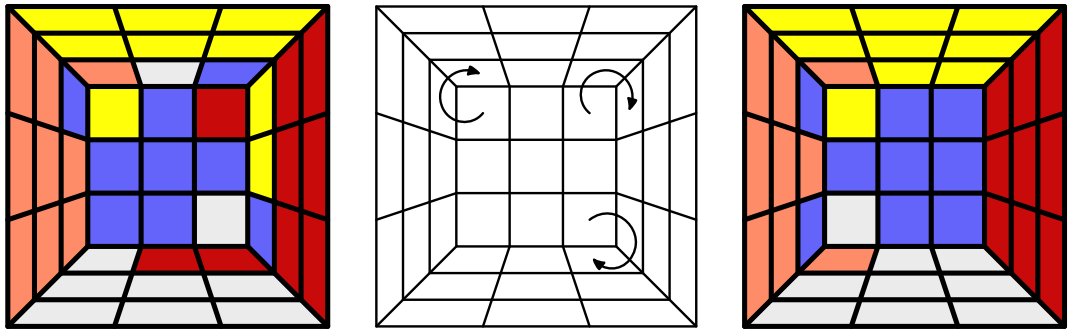

Figure 2.7. Left: after $\gamma = RUR^{-1}URU^2R^{-1}U^2$ is applied to a solved cube. Middle: effect of γ. Right: the effect of $RUR^{-1}URU^2R^{-1} \cdot L^{-1}U^{-1}LU^{-1}L^{-1}U^2L$.

Chapter 3
Practical Conjugation

In group theory, if g and x are elements of a group G, the element $h = xgx^{-1}$ is called the *conjugate* of g by x. Since we have $g = x^{-1}hx$, we may also say that g is the conjugate of h by x^{-1}.

Conjugation has great theoretical importance in group theory, and we will return to it from a more theoretical viewpoint later. The purpose of this chapter is to explain conjugation from a *practical* point of view. We will see that this simple idea greatly expands the applicability of the operations that we have already introduced.

The examples that we give are chosen with *practical* goals in mind. Let us start with the goal of finding operations that only affect the up face. This is an eminently practical thing, since one way to solve the cube is to put all the pieces in the bottom to rows right first, then fix the top.

We begin with an example involving $\alpha_3 = RU^{-1}R^{-1}U_m^{-1}RUR^{-1}U_m$. From Figure 2.3 we see that this only affects the pieces of the front face. Now suppose that we want an operation that only affects the pieces of the *up* face? Naturally we begin by turning the up face to where the front face is now. Thus we preceed the operation with the operation L_0; then we perform α_3; then we perform L_0^{-1} to move the blue face back to the up position, where it should be. In short, the operation we want is $L_0\alpha_3L_0^{-1}$, the *conjugate* of α_3 by L_0. The three steps are shown in Figure 3.1.

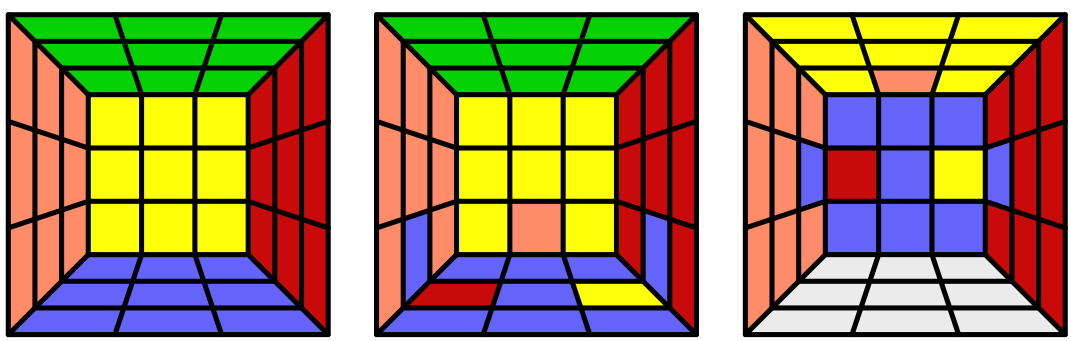

Figure 3.1. A simple conjugation: $L_0\alpha_3L_0^{-1}$. Left: L_0 rolls the top face down.
Middle: α_3 affects the front face only.
Right: L_0^{-1} rolls the affected face back into its proper location.

Now let us consider a more complex example. Unlike α_3, the pieces that are moved by α_1 are not confined to a single face. So if we want an operation that only affects one face, we will have to do a more complicated operation. Let us conjugate α_1 by F_0U (Figure 3.2). As you can see, F_0U puts the blue-orange, blue-white and blue-yellow into the three locations that will be affected by α_1.

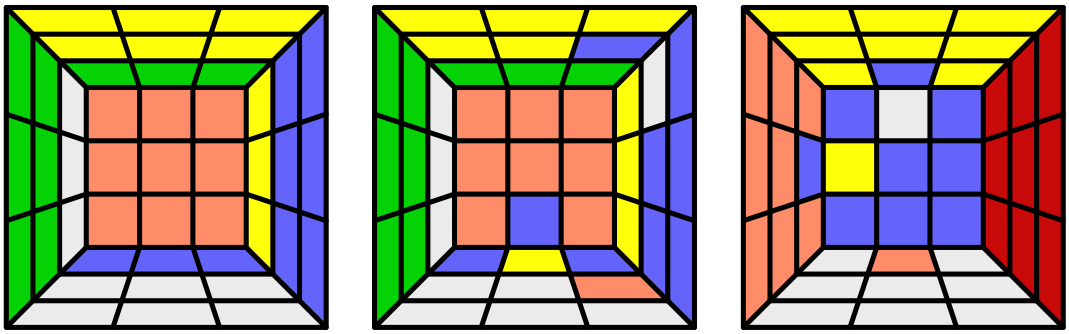

Figure 3.2. A more complicated conjugation: $(F_0U)\alpha_1(F_0U)^{-1}$.
Left: F_0U moves the blue-orange, blue-white and blue-yellow faces into position ...
Middle: α_1 permutes the three blue faces ... Right: $(F_0U)^{-1}$ puts everything back in place!

Exercise 3.1. Prove that if g is an edge 3-cycle then so is hgh^{-1} for any h. Why is this interesting?

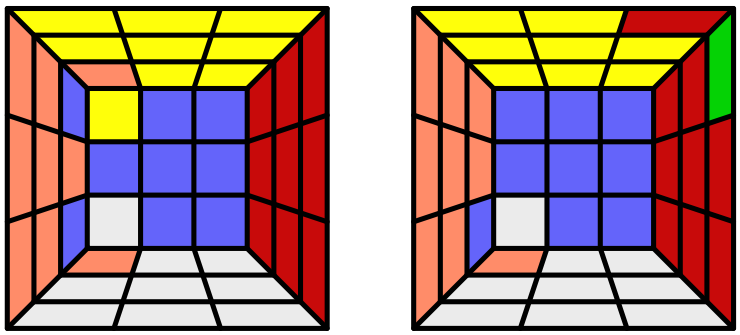

Figure 3.3. Left: effect of $RUR^{-1}URU^2R^{-1} \cdot L^{-1}U^{-1}LU^{-1}L^{-1}U^2L$.
Right: Can you obtain this effect by conjugating?

Exercise 3.2. We saw in the last Chapter that the effect of the operation $RUR^{-1}URU^2R^{-1} \cdot L^{-1}U^{-1}LU^{-1}L^{-1}U^2L$ is to twist two corners, as in Figure 3.3 (left). Knowing this, can you obtain the effect in Figure 3.3 (right) by conjugation?

Chapter 4
How To Solve It

In this chapter we will describe an algorithm for solving the cube. There are two reasons you might not want to read this chapter.

- You already know how to solve the cube.
- You do not already know how to solve the cube.

If either of these pertains to you, you should skip this chapter. For if you already know how to solve the cube, you can skip directly to the next chapter, while if you do not know how to solve it, reading someone else's solution can spoil the pleasure of figuring out your own algorithm.

There are many different algorithms for solving the cube. The process we will describe does first the bottom layer, then the middle layer, then the top layer (corners first, edges last). Using the same set of tricks, you can just as easily do the eight corners first, then the edges.

It should be observed that in order for the green face to be considered solved, it is not really sufficient to make the face all one color. The pieces must be in the correct position.

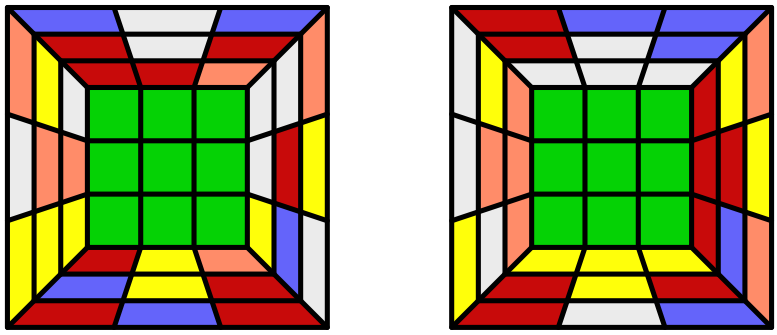

Figure 4.1. Left: the green layer is *not* solved. Right: correct.

Thus in Figure 4.1, the green layer may look solved in the cube at the left, but in fact it is not. A glance at the sides of the nine green faces will show that some of them have to be moved, because the colors are not all lined up. The cube on the right is better – the green face is solved.

In most of this book, the top face will be blue. *However we'll start by solving the green face, then later turn the cube upside down.* So for the time being the green face will be top, but in fact, we are actually solving the bottom layer.

4.1 Stage 1: The centers are always solved!

In discussing the solution of the cube, we will label faces that we don't care about in gray. In Figure 4.2 (left), we label the unsolved pieces of a scrambled in gray. The *center pieces are always solved*, so they are colored in. Indeed, the six center pieces can rotate, but their spatial relationship to each other never changes. (If one takes the cube apart and examines the mechanism, one sees that the center pieces are mechanically linked.) So we can regard the subconfiguration of these six pieces as being "solved" and try to orient the other pieces with respect to them.

4.2 Stage 2: The bottom corners

In Figure 4.2 (right), one more piece is solved. The remaining pieces are kept gray to indicate that we do not care what they are. The first question is – how to attain the configuration in Figure 2.2?

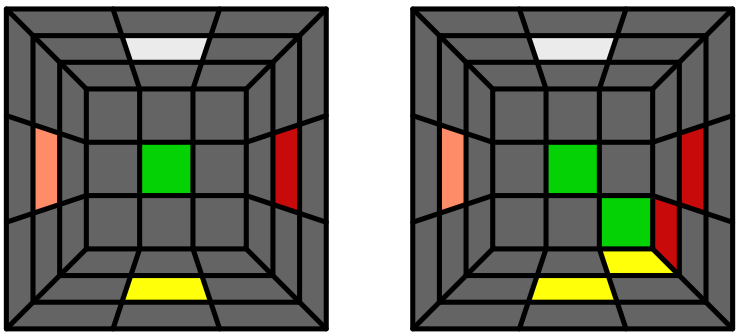

Figure 4.2. Left: the centers are *always* solved. Right: One more piece solved.

We will call the piece in question RYG, since its colors are Red, Yellow and Green. We discuss now how to move it into position. We first assume that the piece is in the *bottom row*, and later we will consider what to do if it is not. Rotating the bottom row, we may assume that it is in one of the three locations in Figure 4.3.

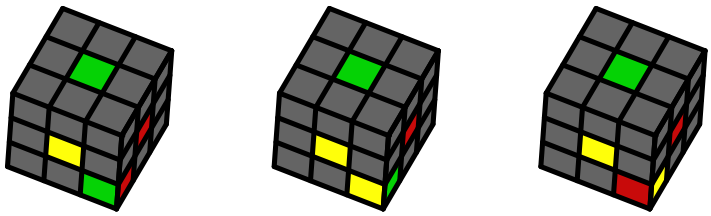

Figure 4.3. Three possible orientations of the RYG piece.

In the first case, that is, when the RYG piece is oriented as in the first diagram in Figure 4.3, it may be brought into position (achieving the right diagram in Figure 4.2) by applying R, or alternatively, by applying FDF^{-1}. See Figure 4.4, where the operation FDF^{-1} is worked out.

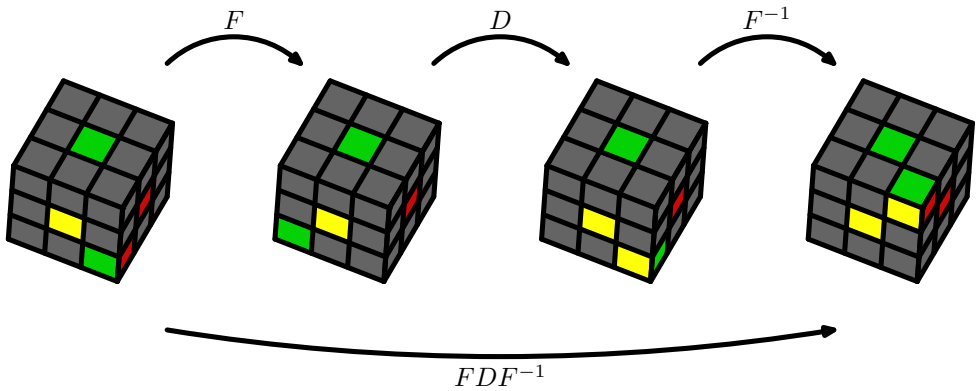

Figure 4.4.

The reader may be puzzled that we have mentioned two different ways of moving RYG into place when it is oriented as in the first diagram in Figure 4.3. Surely it is simpler to use R than to use FDF^{-1}! Yet the latter, seemingly harder way has an important advantage. That is, that *it does not disturb the three remaining top pieces*.

So imagine that RYG is the last of the top pieces to be out of place, in other words that the configuration is as in the left diagram of Figure 4.5. Then after FDF^{-1} we find that RYG is correctly positioned and the other three top corners are not disturbed, as in the right diagram of Figure 4.5.

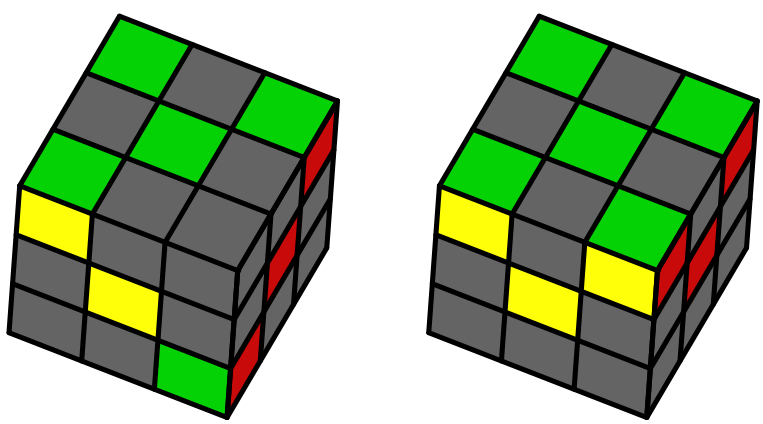

Figure 4.5. The operation FBF^{-1} does not disturb the remaining three top corners.

Similarly if the cube is arranged as in the second position of Figure 4.3, then the operation F^{-1} or (better) $R^{-1}D^{-1}R$ will move RYG into position; and $R^{-1}D^{-1}R$ has the advantage of doing so without disturbing the remaining top corners.

Finally, if the cube is arranged as in the third diagram of Figure 4.3, the operation $R^{-1}DRFB^2F^{-1}$ will put the piece in place without disturbing the remaining top corners.

In the above discussion, we assumed that RYG is in the bottom row. If instead it is in the top row, we may move it to the bottom row using operations such as FDF^{-1}. In short, by using the three operations FDF^{-1}, $R^{-1}D^{-1}R$ and $R^{-1}DRFD^2F^{-1}$, we may put the top corners in place, achieving the right configuration in Figure 4.5.

4.3 Stage 3: The bottom edges

Now let us consider how to restore the green edges. We suppose at first that the green-and-yellow edge piece (which we naturally call GY) is in the bottom row. By rotating the bottom row, we may assume that it is in one of the two positions in Figure 4.6.

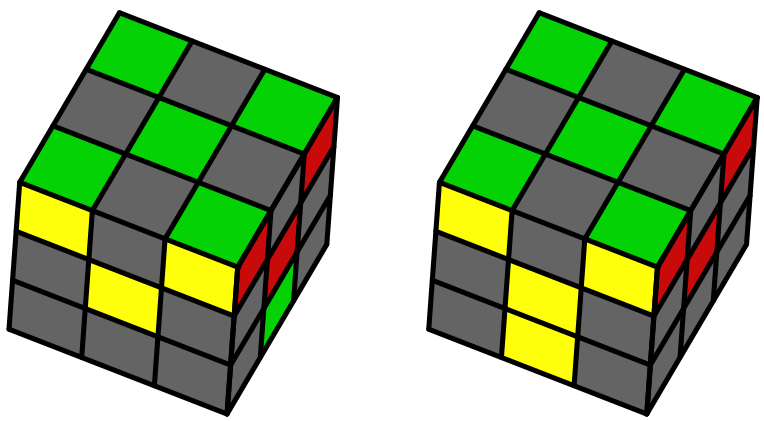

Figure 4.6. Two possible GY positions on the bottom row.

If the cube is in the first position in Figure 4.6, then $R_m^{-1}D^{-1}R_m$ puts it into place. This is shown in Figure 4.7. In Figure 4.7 we assume that the remaining top pieces are all in place, to demonstrate that this operation does not disturb any of the top pieces that might already be in place.

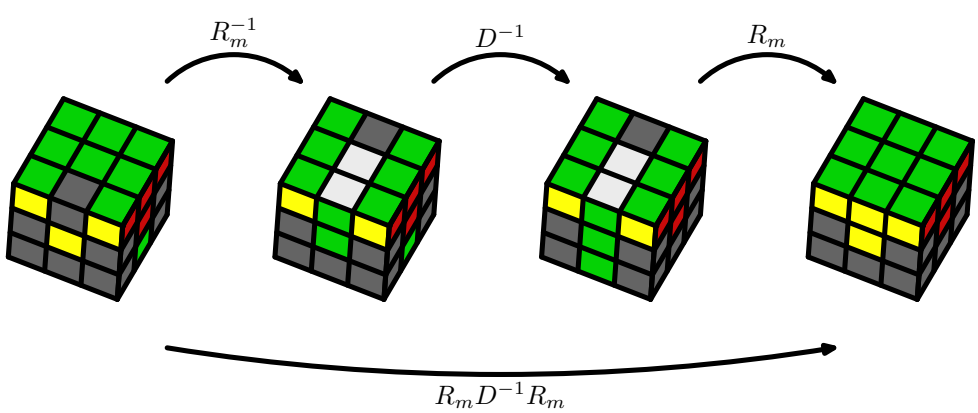

Figure 4.7. Putting GY into place (first possibility)

If the cube is in the second position in Figure 4.6, then $R_m^{-1}D^2R_m$ does the job (not shown).

We have seen what to do if GY is in the bottom row. Suppose next it is in the middle layer. Rotating the middle layer we may put it into one of the two positions in Figure 4.8. *Note:* since we have rotated the middle layer, the center faces in that layer may no longer be in position, so we have colored them dark. This is unimportant since they may be rotated back to where they belong after the green layer is complete.

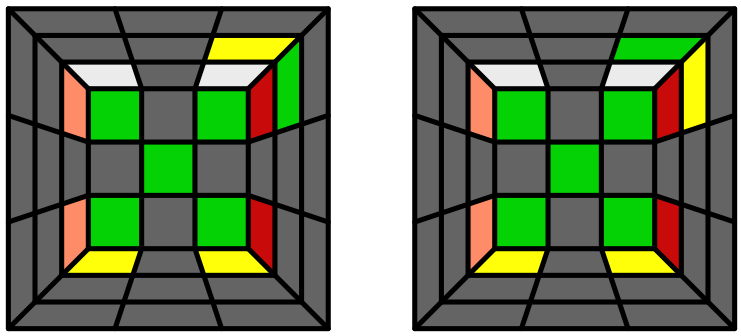

Figure 4.8. Two possible middle-layer positions for GY.

In the first case, $F^{-1}U_m^2F$ will restore GY to its proper position; and in the second case FU_mF^{-1} will do the job.

We now know how to put the green edge pieces in place, using operations that don't destroy the progress we've already made. There is only one case we haven't explained, which is that GY might already be in the top row, but in the wrong position – or in the correct position, but flipped. But operations that we have already discussed are sufficient to handle this case, too. We may rotate the top face until GY is in the front, then apply $F^{-1}U_m^2F$, which will leave it in the middle layer; then rotate the top face until it is correctly positioned. One of the two positions in Figure 4.8 will be attained, and we already know how to solve that.

4.4 Stage 4: The middle layer edges

We now know how to solve the green layer. We will assume it to be solved, and turn the cube over. From now on, the up side of the cube will be blue, and the down side is green.

Next we assemble the middle layer, though we could, alternatively, do the top layer next.

We assume first that the red-and-white edge piece, known to its friends as RW, is in the upper layer, and we show how to position it. There are two cases, depending on how RW is oriented. After rotating the upper face, we may

assume that it is in one of the first two positions in Figure 4.9. The goal is to move it into its correct location,, as in the third position in Figure 4.9.

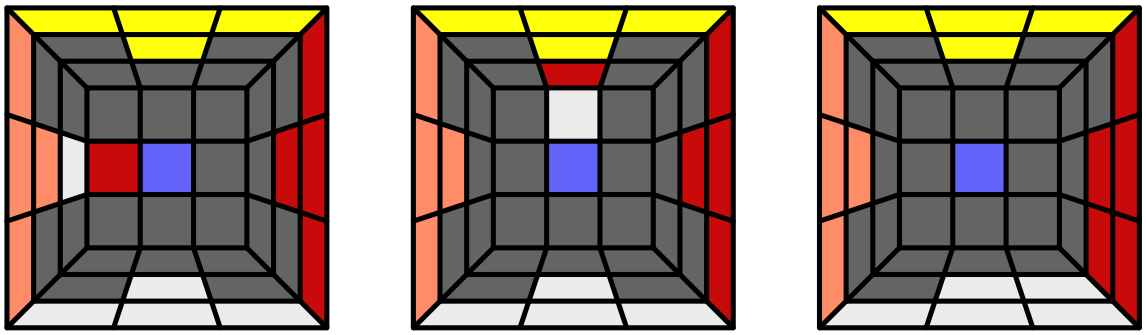

Figure 4.9. Left and middle: Possible top layer positions for RW. Right: Correct position.

We will describe a way of doing this that *does not disturb any pieces in the first two layers* so that if some middle layer pieces are already positioned, they will not be affected. Thus if the cube is in the left position in either of the two positions in Figure 4.10, the method will put it correct as in Figure 4.10 (right). If you don't care about not disturbing the other pieces of the middle layer, it may be possible to get to Figure 4.9 (right) more efficiently.

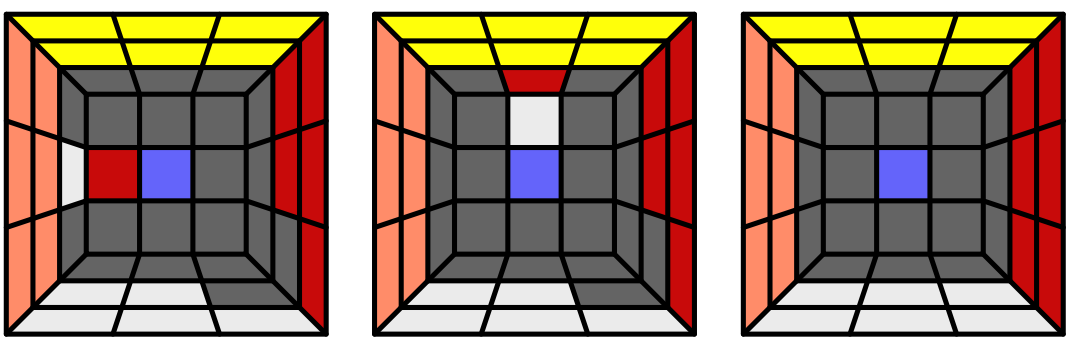

Figure 4.10. Left and middle: Possible top layer positions for RW (middle layer nearly solved). Right: Correct position.

First, if we are in the left position of Figure 4.9 or Figure 4.10, we will use a conjugate of $\alpha_1^\dagger = L^{-1}ULU_m^{-1}L^{\ -1}U^{-1}LU_m$. Specifically, we will conjugate by $F_0^{-1}L$, which rotates the entire cube so that the down face (green in the figures) is on the right, then rotates the left face so that the RW piece is in position for $\alpha_1^\dagger$. The effect is shown in Figure 4.11 (left). A comparison with Figure 2.4 (left) shows that applying $\alpha_1^\dagger$ now will move the RW piece into position, as in Figure 4.11 (middle). Finally, applying $(F_0^{-1}L)^{-1} = L^{-1}F_0$ will roll the cube back into position.

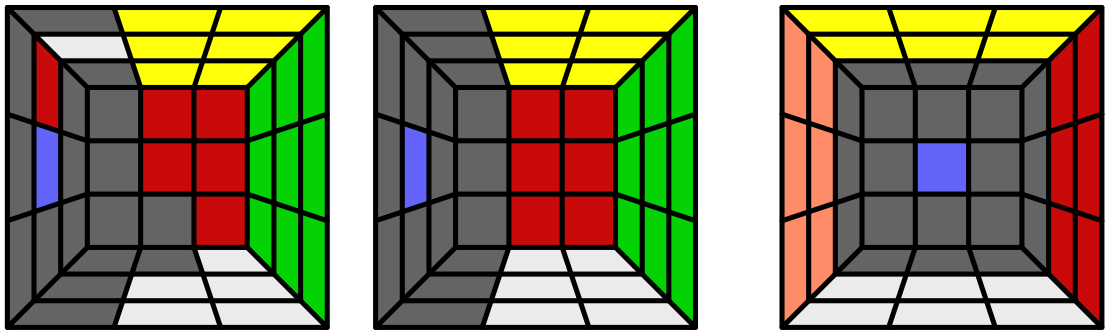

Figure 4.11. Stages of the conjugated operation $(F_0^{-1}L)\alpha_1^\dagger(F_0^{-1}L)^{-1} = F_0^{-1}L\alpha_1^\dagger L^{-1}F_0L$, applied to the first position in Figure 4.10.
Left: after $F_0^{-1}L$. Middle: now applying $\alpha_1^\dagger$. Right: after $(F_0^{-1}L)^{-1} = L^{-1}F_0$.

The operation $(F_0^{-1}L)\alpha_1^\dagger(F_0^{-1}L)^{-1}$ can be simplified. Written out in full (remembering that $(F_0^{-1}L)^{-1} = L^{-1}F_0$) this is:

$$F_0^{-1}LL^{-1}ULU_m^{-1}L^{-1}U^{-1}LU_mL^{-1}F_0$$

Observe that the LL^{-1} at the beginning cancel, and that the last L^{-1} is rather superfluous since it only serves to rotate the gray face. What the cubist should actually do is therefore:

$$F_0^{-1}ULU_m^{-1}L^{-1}U^{-1}LU_mF_0.$$

All this will be obvious as soon as you put the move into operation.

A similar treatment will handle the middle position in Figure 4.9 or (more specifically) Figure 4.10. One uses the operation α_1, conjugated by $U_0F_0R^{-1}$. This is illustrated in Figure 4.12. As with the other case, there is a minor simplification to be noted (which we leave to the reader).

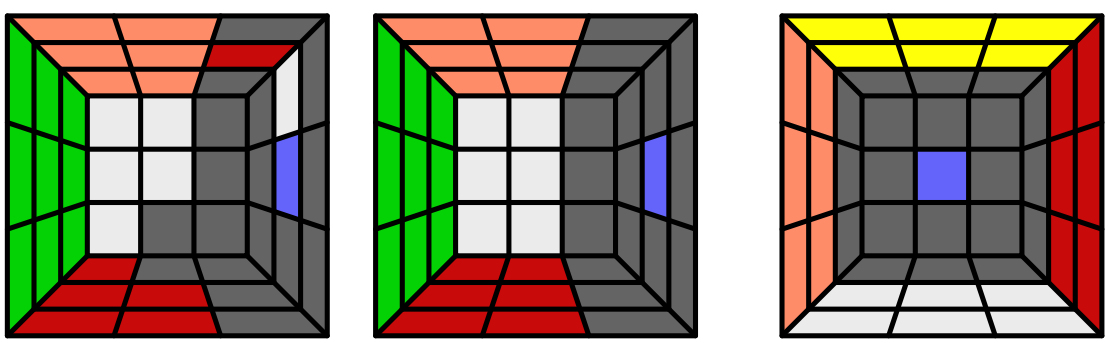

Figure 4.12. Stages of the conjugated operation $(U_0F_0R^{-1})\alpha_1(U_0F_0R^{-1})^{-1}$, applied to the second position in Figure 4.10.
Left: after $U_0F_0R^{-1}$. Middle: now applying α_1. Right: after $(U_0F_0R^{-1})^{-1} = RF_0^{-1}U_0^{-1}$.

4.5 Stage 5: Positioning the top corners

The operations that we have already discussed are sufficient to solve the first two layers, and we consider that done. We now turn to the solution of the top face. Our first goal is to get the top four corners into their correct position, though not necessarily in their correct orientation. For example, the two positions in Figure 4.13 are "solved" by this criterion.

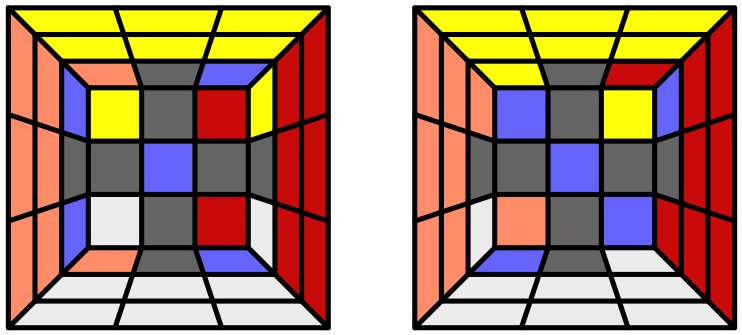

Figure 4.13. The next goal is to get the corners correctly positioned, though not necessarily correctly oriented.

We recall that in Chapter 2 we had two operations β (a corner 3-cycle) and ϕ (swapping two pairs of corners). These operations have the following effects (summarized from Figure 2.5 and Figure 2.6):

$$\boxed{\begin{array}{ccc} A & & B \\ \uparrow & \searrow & \\ C & \longleftarrow & D \end{array}} \qquad\qquad \boxed{\begin{array}{ccc} A & \longleftrightarrow & B \\ & & \\ C & \longleftrightarrow & D \end{array}}$$

Label the top four corners by A, B, C, D. Assume that the cube is labeled so that the solved configuration is $\begin{array}{|c|c|}\hline A & B \\ \hline C & D \\ \hline\end{array}$. Rotate the top using U so that A is in the right place. There are six possibilities.

1. $\begin{array}{|c|c|}\hline A & B \\ \hline C & D \\ \hline\end{array}$. In this case it is already solved.

2. $\begin{array}{|c|c|}\hline A & B \\ \hline D & C \\ \hline\end{array}$. Solve it as follows: $\xrightarrow{U^2} \begin{array}{|c|c|}\hline C & D \\ \hline B & A \\ \hline\end{array} \xrightarrow{\beta} \begin{array}{|c|c|}\hline B & D \\ \hline A & C \\ \hline\end{array} \xrightarrow{U} \begin{array}{|c|c|}\hline A & B \\ \hline C & D \\ \hline\end{array}$.

3. $\begin{array}{|c|c|}\hline A & C \\ \hline B & D \\ \hline\end{array}$. Solve it as follows: $\xrightarrow{\phi} \begin{array}{|c|c|}\hline C & A \\ \hline D & B \\ \hline\end{array} \xrightarrow{U^{-1}} \begin{array}{|c|c|}\hline A & B \\ \hline C & D \\ \hline\end{array}$.

   Alternatively (without using ϕ):

   $\xrightarrow{\beta} \begin{array}{|c|c|}\hline B & C \\ \hline D & A \\ \hline\end{array} \xrightarrow{U^2} \begin{array}{|c|c|}\hline A & D \\ \hline C & B \\ \hline\end{array} \xrightarrow{\beta} \begin{array}{|c|c|}\hline C & D \\ \hline B & A \\ \hline\end{array} \xrightarrow{U^2} \begin{array}{|c|c|}\hline A & B \\ \hline C & D \\ \hline\end{array}$

4. $\begin{array}{|c|c|}\hline A & C \\ \hline D & B \\ \hline\end{array}$. Solve it as follows: $\xrightarrow{\beta}$ $\begin{array}{|c|c|}\hline D & C \\ \hline B & A \\ \hline\end{array}$ $\xrightarrow{U^2}$ $\begin{array}{|c|c|}\hline A & B \\ \hline C & D \\ \hline\end{array}$.

5. $\begin{array}{|c|c|}\hline A & D \\ \hline B & C \\ \hline\end{array}$. Solve it as follows: $\xrightarrow{U^{-1}}$ $\begin{array}{|c|c|}\hline C & D \\ \hline B & A \\ \hline\end{array}$ $\xrightarrow{\beta}$ $\begin{array}{|c|c|}\hline B & D \\ \hline A & C \\ \hline\end{array}$ $\xrightarrow{U}$ $\begin{array}{|c|c|}\hline A & B \\ \hline C & D \\ \hline\end{array}$.

6. $\begin{array}{|c|c|}\hline A & D \\ \hline C & B \\ \hline\end{array}$. Solve it as follows: $\xrightarrow{\beta}$ $\begin{array}{|c|c|}\hline C & D \\ \hline B & A \\ \hline\end{array}$ $\xrightarrow{U^2}$ $\begin{array}{|c|c|}\hline A & B \\ \hline C & D \\ \hline\end{array}$.

It will be noted that in every case but one, a single application of β is sufficient to solve the cube. In the anomalous case 3, one may either employ two applications of β or (more efficiently) a single application of ϕ. Thus ϕ is not needed to solve the cube, but one time in six, its use is most efficient.

4.6 Stage 6: Orienting the top corners

Now we have enough operations to achieve the goal of positioning the top corners (as in Figure 4.13) but they may be oriented incorrectly at this stage. We have an operation $\gamma = RUR^{-1}URU^2R^{-1}U^2$ that twists three top faces each in an angle of $120° = \frac{2\pi}{3}$ counterclockwise. The configuration resulting from the application of this operation to the pristine cube is shown in Figure 4.14 (left). We represent this operation symbolically by Figure 4.14 (right), with a $+$ denoting a counterclockwise twist, and a $-$ representing a clockwise one.

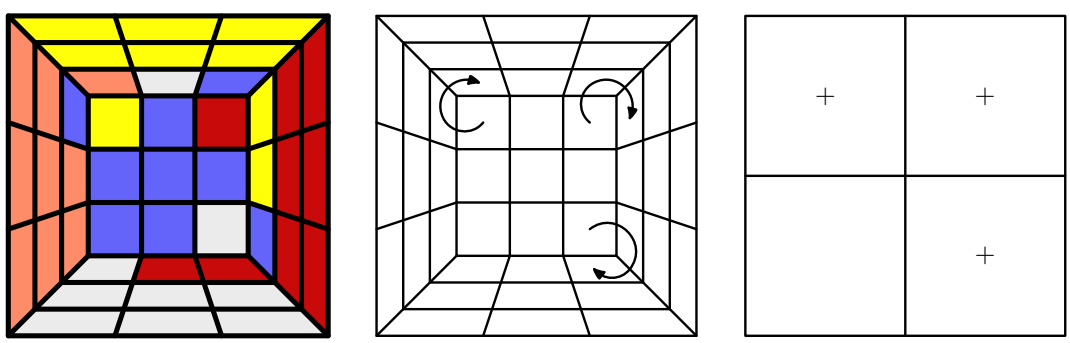

Figure 4.14. Left: result of $\gamma = RUR^{-1}URU^2R^{-1}U^2$ applied to a pristine cube. Note: at this stage we do not care what happens to the center edge pieces. Middle: effect of γ. Right: symbolic representation of the three corner twists.

We will prove later that not every possible twisting of the corners can be obtained. It is not possible to twist a single corner—the configuration in Figure 4.15 (right) cannot be achieved (except by taking the cube apart and reassembling it). The possible twists that can occur are three $+$'s, three $-$'s, a single $+$ and a single $-$, or two $+$'s and two $-$'s. Each such configuration can be solved using one or two applications of γ or of its mirror image operation $\gamma^\dagger = L^{-1}U^{-1}LU^{-1}L^{-1}U^2LU^2$.

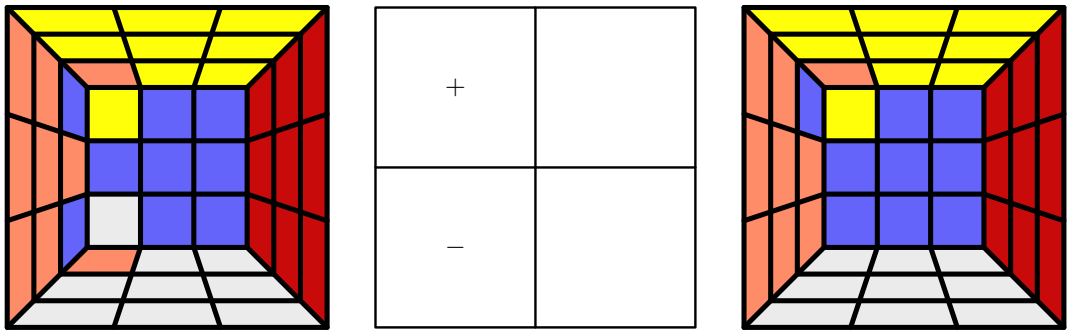

Figure 4.15. Left: the effect of $RUR^{-1}URU^2R^{-1} \cdot L^{-1}U^{-1}LU^{-1}L^{-1}U^2L$
Middle: symbolic representation of this operation. Right: *An impossible configuration!*

Here is a table of the possible twisted configurations and their solutions.

$$\begin{array}{c}\begin{array}{|c|c|}\hline + & + \\ \hline + & \\ \hline\end{array}\end{array} \xrightarrow{\gamma^\dagger} \begin{array}{c}\begin{array}{|c|c|}\hline & \\ \hline & \\ \hline\end{array}\end{array} \qquad \text{(solved!)}$$

$$\begin{array}{c}\begin{array}{|c|c|}\hline - & - \\ \hline & - \\ \hline\end{array}\end{array} \xrightarrow{\gamma} \begin{array}{c}\begin{array}{|c|c|}\hline & \\ \hline & \\ \hline\end{array}\end{array}$$

$$\begin{array}{c}\begin{array}{|c|c|}\hline - & \\ \hline + & \\ \hline\end{array}\end{array} \xrightarrow{\gamma} \begin{array}{c}\begin{array}{|c|c|}\hline & + \\ \hline + & + \\ \hline\end{array}\end{array} \xrightarrow{U^2} \begin{array}{c}\begin{array}{|c|c|}\hline + & + \\ \hline + & \\ \hline\end{array}\end{array} \xrightarrow{\gamma^\dagger} \begin{array}{c}\begin{array}{|c|c|}\hline & \\ \hline & \\ \hline\end{array}\end{array}$$

$$\begin{array}{c}\begin{array}{|c|c|}\hline & + \\ \hline & - \\ \hline\end{array}\end{array} \xrightarrow{\gamma^\dagger} \begin{array}{c}\begin{array}{|c|c|}\hline - & \\ \hline - & - \\ \hline\end{array}\end{array} \xrightarrow{U^2} \begin{array}{c}\begin{array}{|c|c|}\hline - & - \\ \hline & - \\ \hline\end{array}\end{array} \xrightarrow{\gamma} \begin{array}{c}\begin{array}{|c|c|}\hline & \\ \hline & \\ \hline\end{array}\end{array}$$

$$\begin{array}{c}\begin{array}{|c|c|}\hline + & - \\ \hline - & + \\ \hline\end{array}\end{array} \xrightarrow{\gamma^\dagger} \begin{array}{c}\begin{array}{|c|c|}\hline & + \\ \hline + & + \\ \hline\end{array}\end{array} \xrightarrow{U^2} \begin{array}{c}\begin{array}{|c|c|}\hline + & + \\ \hline + & \\ \hline\end{array}\end{array} \xrightarrow{\gamma} \begin{array}{c}\begin{array}{|c|c|}\hline & \\ \hline & \\ \hline\end{array}\end{array}$$

$$\begin{array}{c}\begin{array}{|c|c|}\hline - & + \\ \hline - & + \\ \hline\end{array}\end{array} \xrightarrow{\gamma^\dagger} \begin{array}{c}\begin{array}{|c|c|}\hline + & \\ \hline + & + \\ \hline\end{array}\end{array} \xrightarrow{U} \begin{array}{c}\begin{array}{|c|c|}\hline + & + \\ \hline + & \\ \hline\end{array}\end{array} \xrightarrow{\gamma} \begin{array}{c}\begin{array}{|c|c|}\hline & \\ \hline & \\ \hline\end{array}\end{array}$$

After rotating the top, that is, applying a power of U, any possible configuration can be made to agree with one of the above, and the above chart shows how to fix the corner twistings. In practice it is better not to memorize this table since the method will be clear with just a little practice.

4.7 Stage 7: Up edges into place

At this stage, the cube is finished except the up edges. The last step in finishing the cube is to put the top into place.

- A simple way of doing this is use the edge 3-cycles to first put the edges into their correct positions, then as a second step, to fix their orientations. This way there are two steps – after the first step, all pieces will be

in position, but two of four up edges might be flipped.

- A better way is to try to get the orientations correct as you move them into place. This requires more care in the use of edge 3-cycles.

We will describe the first method first.

We recall that α_3 only affects the edges of one face, which it permutes in a 3-cycle. That face is the front face, but as we saw in Figure 3.1 it is a simple matter to obtain a 3-cycle of the up face by first turning the whole cube before doing the operation. (The operation is reviewed in Figure 4.16.) Using either α_3 or its mirror image $\alpha_3^\dagger$, then every possible 3-cycle of the top edges can be obtained in this way. (In making this statement, we are concerned at this point with the *positions* of the four pieces, rather than their orientations.)

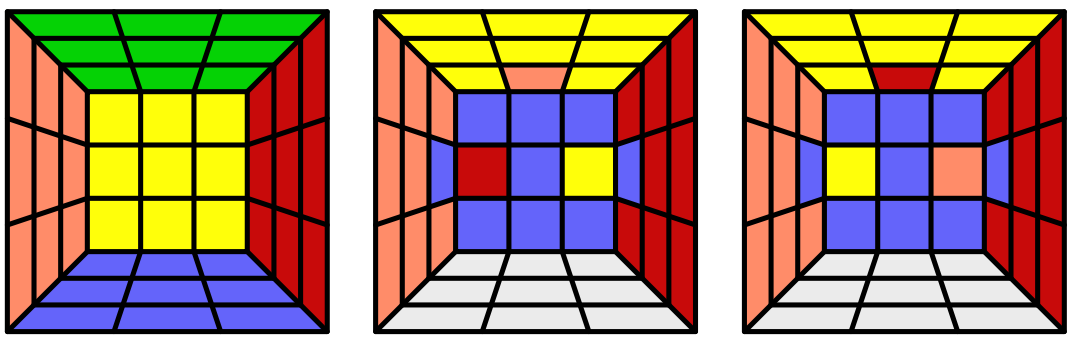

Figure 4.16. Recall $\alpha_3 = R\,U^{-1}R^{-1}U_m^{-1}R\,U\,R^{-1}U_m$ and $\alpha_3^\dagger = L^{-1}ULU_m\,L^{-1}U^{-1}LU_m^{-1}$.
Left: Before doing α_3 or $\alpha_3^\dagger$, first apply L_0 to turn the cube so the up face (blue) is in front.
Afterwards, apply L_0^{-1} to turn it back with the up face up again.
Middle: after $L_0\alpha_3L_0^{-1}$. Right: after $L_0\alpha_3^\dagger L_0^{-1}$. This and other conjugates of α_3 and $\alpha_3^\dagger$ produce every possible 3-cycle of the up edges.

Not every possible configuration of the up edges can occur. We will prove later in the book that if two top edges are in position, then the remaining two will also be in place. Thus the first configuration in Figure 4.17 (left) can't happen. With this in mind, we can easily put the top faces into position as follows:

- If no up edges are in place, position any up edge using a conjugate of α_3 or $\tilde{\alpha}_3$. Otherwise (if at least one edge is already in place), skip this step.

- Now at least one up edge is in place. The remaining up edges are either all in place, or none are in place. In the second case, another application of a conjugate of α_3 or $\tilde{\alpha}_3$ will finish this stage.

It is clear that this procedure will put two of the edges into position, and as we have just noted this will position the remaining ones, also.

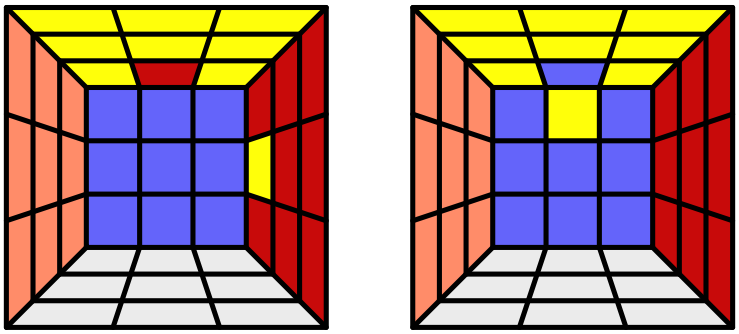

Figure 4.17. Two more impossible configurations.
Left: two pieces switched. *This can't happen!* Right: one edge flipped. *Neither can this!*

4.8 Stage 8: Final flips

At this stage, all pieces are in place, and all pieces are correctly oriented except that some of the four up edges may be flipped. Only an *even* number of edges may be flipped – we'll prove this later. Thus the configuration of Figure 4.17 (right) can't happen. If some edges are flipped, either two or four will be, never just one.

There are many ways to flip two edges. One way is to just to α_3, then its mirror image $\alpha_3^\dagger$. This gives the result in the left figure of Figure 4.18. By turning the cube before doing the operation, that is, conjugating, one may flip two adjacent top edges Figure 4.18 (middle or right).

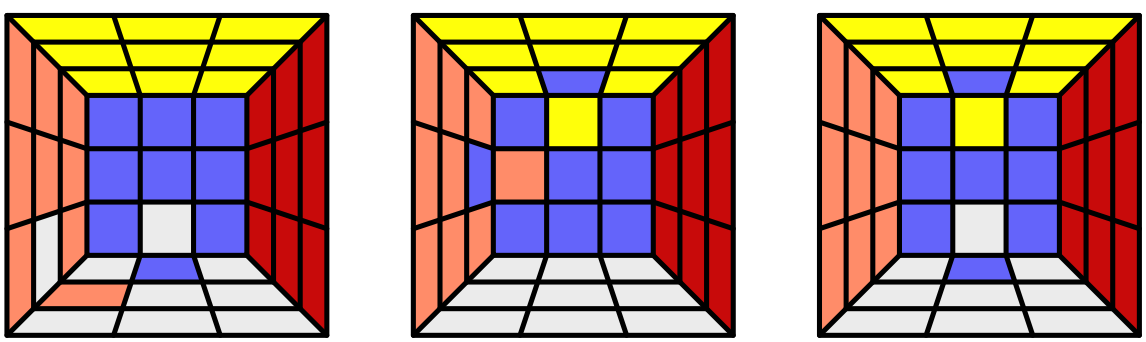

Figure 4.18. Left: result of $\alpha_3\alpha_3^\dagger$. To get top edge flips, conjugate. Middle: $L_0\alpha_3\alpha_3^\dagger L_0^{-1}$.
Right: $(BL^2)\alpha_3\alpha_3^\dagger(BL^2)^{-1}$

Chapter 5
Planning Edge 3-Cycles

The last Chapter described one method of solving the cube. We have used just the operations α_1, α_3, β, γ and the mirror images $\alpha_1^\dagger$, $\alpha_3^\dagger$ and $\gamma^\dagger$. We also saw that the solution could occasionally be made more efficient by using ϕ.

In practice, a great improvement in efficiency can be made by proper use of the edge 3-cycles. If one uses the correct 3-cycle, one can usually combine Stages 7 and 8 of the solution; that is, by using the right 3-cycles at Stage 7, one can usually avoid having flipped edges at the end, obtaining a faster solution.

The exercises in this section are intended to improve the reader's grasp of α_1, α_2, α_3 and $\alpha_1^\dagger$, $\alpha_2^\dagger$, $\alpha_3^\dagger$.

For each of the positions in Figure 5.1, you are asked to do the following.

- Give a conjugate of α_1, α_2, α_3 and $\alpha_1^\dagger$, $\alpha_2^\dagger$, $\alpha_3^\dagger$ that creates the position from the pristine cube.
- Give a conjugate of α_1, α_2, α_3 and $\alpha_1^\dagger$, $\alpha_2^\dagger$, $\alpha_3^\dagger$ that solves it.

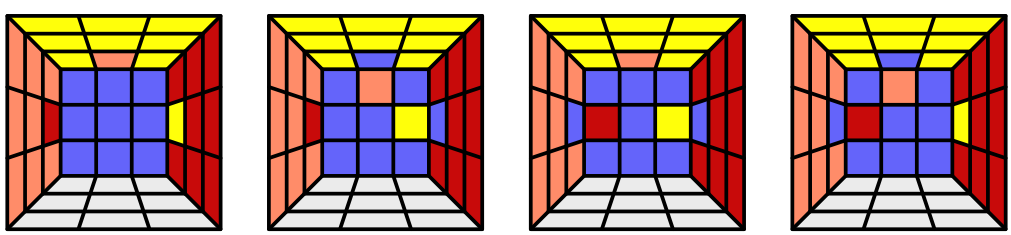

Figure 5.1. Edge 3-cycle practice problems.

The mirror image problems are contained in Figure 5.2.

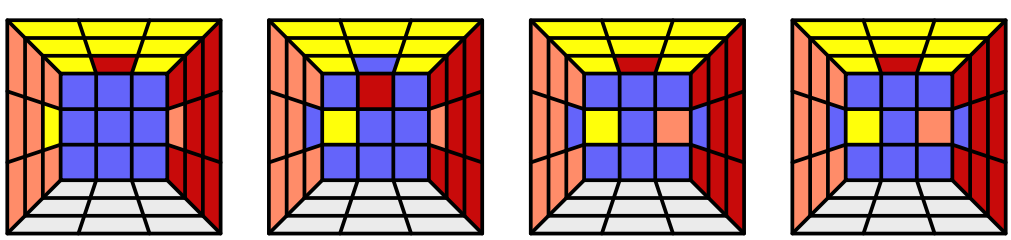

Figure 5.2. Mirror image 3-cycle practice problems.

We will explain in detain the solution to one of these problems, the first. We begin with the pristine cube, and try to permute the three edges so that the configuration in Figure 5.1 is obtained.

Our aim is to convey the *logic* of setting up an edge 3-cycle with a desired effect. The solutions to all of the exercises will follow the description that we now give.

5.1 Step 1: move BY into position

For these particular problems, the first step is always to apply L_0, rolling the cube to prepare for one of the α_i. To see why this is the right way to begin, consider the following. From Figures 2.1, 2.2, 2.3 and 2.4, we may summarize the effect of the α_i and $\alpha_i^\dagger$ as follows. *The three permuted pieces are the up-front edge, and two pieces from the middle layer, one of which is the right-front edge (for the α_i) or the left-front edge (for the $\alpha_i^\dagger$).* Now L_0 will put the blue-yellow piece (known as BY) into the up-front position, and the up-left and up-front pieces into the middle layer. From our description of the α_i and $\alpha_i^\dagger$, this is exactly where we want these three pieces. After L_0, the position in the left diagram of Figure 5.3 results.

5.2 Step 2: decide whether to use an α_i or $\alpha_i^\dagger$

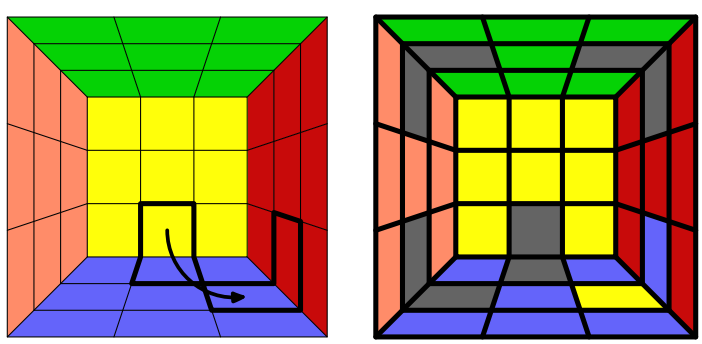

Figure 5.3. First possibility to move BY down: L_0 followed by α_1, α_2 or α_3.

There are now two possibilities: we can use an α_i or an $\alpha_i^\dagger$. Which is correct depends on the orientation that we want for the BY face. Bearing in mind that we want to move it into the location currently occupied by the BR face there are two ways.

- We can do an α_i. In this case BY will end up in the orientation shown in Figure 5.3.

- We can do an $\alpha_i^\dagger$. Since we want BY in the position currently occupied by BR, we must first turn the bottom two layers. The operation that does this is $D^{-1}D_m^{-1}$. This means that we must add $D^{-1}D_m^{-1}$ to the conjugating operation. After this, $\alpha_i^\dagger$ will cause BY to end up in the orientation shown in the Figure 5.4.

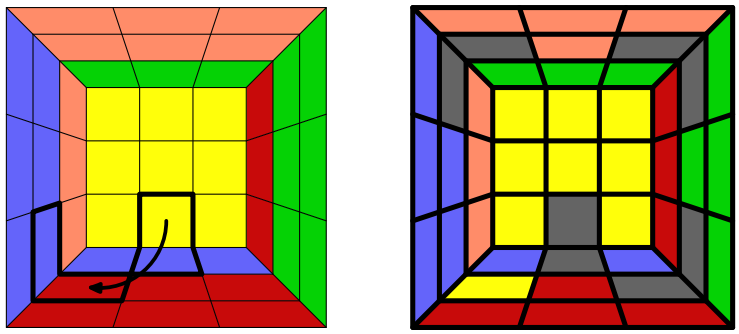

Figure 5.4. Second possibility to move BY down: use $\alpha_1^\dagger$, $\alpha_2^\dagger$ or $\alpha_3^\dagger$. First we must turn the bottom two layers so that BY will end up in its intended location. Thus we preceed the operation by $L_0U_mD^{-1}$.

In the case at hand, the orientation of BY should be with the B face next to the B center, as we can see from the goal configuration in Figure 5.1 (left). Thus we proceed as in Figure 5.4.

5.3 Step 3: Decide which α_i or $\alpha_i^\dagger$ to use.

So far, we have done L_0 and $D^{-1}D_m^{-1}$, which are the first two constituents of the conjugating operation, and we have decided that we will use an $\alpha_i^\dagger$, but we have not decided which one. Given that we want the blue-red piece (BR) to move into the location of the blue-orange piece (BO), there are two possibilities.

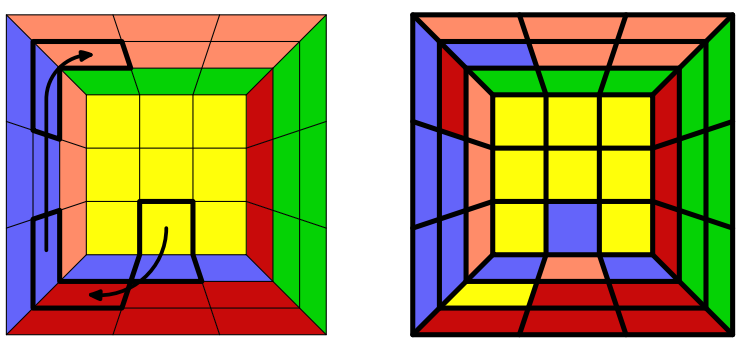

Figure 5.5. The effect of $\alpha_1^\dagger$.

- We can do $\alpha_1^\dagger$. The effect is shown in Figure 5.5.
- We can do $\alpha_2^\dagger$. Since we want BR to end up in the location currently occupied by BO, we must first turn the back face so that BO is in the back right position. This means adding B^2 to the conjugation. The effect is shown in Figure 5.6.

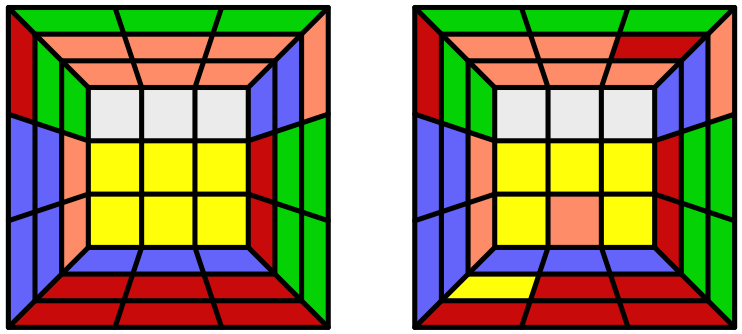

Figure 5.6. The effect of $\alpha_2^\dagger$.

In the case at hand, the desired orientation of BO dictates which course is correct: we must use $\alpha_2^\dagger$, and we must add B^2 to the conjugating operation.

5.4 Step 4: Do the operation

We have so far determined that $\alpha_2^\dagger$ is the correct operation to solve the exercise, and at each step we added something to the conjugating operation; the conjugating operation is $L_0 D^{-1} D_m^{-1} B^2$. Happily, we did each element of the conjugating operation as we figured out that $\alpha_2^\dagger$ is the correct operation, so we are now ready to do it. After $\alpha_2^\dagger$, the cube is as in Figure 5.6 (right).

5.5 Step 5: Undo the conjugating operation

So far we have done $L_0 D^{-1} D_m^{-1} B^2$ and $\alpha_2^\dagger$. It remains to undo the conjugating operation, so we now do $(L_0 D^{-1} D_m^{-1} B^2)^{-1} = B^2 D_m D L_0^{-1}$ and the operation is finished. Thus the operation to produce the first configuration of Figure 5.1 is

$$(L_0 D^{-1} D_m^{-1} B^2)\alpha_2^\dagger (L_0 D^{-1} D_m^{-1} B^2)^{-1}.$$

Chapter 6
Basic Group Theory

6.1 Subgroups and generators

If X is a subset of a group G, we may consider what elements of G can be built up from the elements of G by the operations in X. The set of such elements turns out to be a group itself, though it might not be all of G. This group will be the subject of this section.

If G is a group and H is a subset such that for all $x, y \in H$ we have $xy \in H$ and $x^{-1} \in H$. Then H is itself naturally a group. We call H a *subgroup* of G.

Proposition 6.1. *Let G be a group and X a subset of G. Then there is a unique smallest subgroup H of G containing X.*

Concretely, the conclusion means that H is a subgroup of G, H contains X and if K is any subgroup of G containing X then $H \subseteq K$. We call H the *subgroup of G generated by X* and denote $H = \langle X \rangle$.

Proof. First let us observe that H, if it exists, is unique. Indeed, suppose that H' is another subgroup of G with the property that H' contains X and that if K is any subgroup of G containing X then $H' \subseteq K$. Since H' contains X we have $H \subseteq H'$ (by the property that H is assumed to have) and similarly since H contains X we have $H' \subseteq H$ (by the property that H is assumed to have). So $H' = H$.

It remains for existence to be proved, and we give two proofs of this, since both are instructive.

The first proof is as follows. Let Σ be the set of all subgroups of G containing X. Then Σ is nonempty since $G \in \Sigma$. Let

$$H = \bigcup_{K \in S} K.$$

It is clear that H is a subgroup of G containing X, and if K is any subgroup of G containing X then $K \in S$ so $H \subseteq K$. This completes the first existence proof.

The second existence proof is constructive. Let

$$\tilde{X} = \{x \in G \,|\, x \text{ or } x^{-1} \in X\}.$$

Let H be the set consisting of 1 together with all elements of G of the form $x_1 \cdots x_n$ where each x_i is either an element of $\tilde{X}$. It is clear that $1 \in H$ and that if $x, y \in H$ then $xy \in H$ and $x^{-1} \in H$. So H is a subgroup of G containing X. Moreover if K is a group and K contains X, then K contains $\tilde{X}$ and so K contains all products of elements of $\tilde{X}$, that is, K contains H. This completes the second existence proof. □

As an example, $\mathfrak{G}_0$ was defined in Chapter 1 to be "the set of all possible operations of the cube that can be constructed out of the ones we have already defined: $U, D, F, B, L, R, U_0, D_0, F_0, B_0, L_0, R_0, U_m, D_m, F_m, B_m, L_m$ and R_m." This means that $\mathfrak{G}_0$ is the group generated by these elements.

Proposition 6.2. *The group $\mathfrak{G}_0$ is generated by $U, D, F, B, L, R, U_0, F_0, R_0$.*

Proof. It is enough to show that a subgroup H of $\mathfrak{G}_0$ that contains $U, D, F, B, L, R, U_0, F_0, R_0$ also contains D_0, B_0, L_0, U_m, D_m, F_m, B_m, L_m and R_m; indeed, if we know this, then it is clear that the smallest group containing

$$U, D, F, B, L, R, U_0, F_0, R_0, D_0, B_0, L_0, U_m, D_m, F_m, B_m, L_m, R_m$$

is identical with the smallest group containing $U, D, F, B, L, R, U_0, F_0, R_0$.

Since $D_0 = U_0^{-1}$, $B_0 = F_0^{-1}$ and $L_0 = R_0^{-1}$, the group H contains D_0, B_0 and R_0. Now since

$$\begin{aligned} U_m &= U_0 U^{-1} D, & F_m &= F_0 F^{-1} B, & R_m &= R_0 R^{-1} L, \\ D_m &= D_0 D^{-1} U, & B_m &= B_0 B^{-1} F, & L_m &= L_0 L^{-1} R, \end{aligned}$$

the group H also contains U_m, F_m, R_m, D_m, B_m and L_m. □

In fact, $\mathfrak{G}_0$ is generated by just $U, D, F, B, L, R, U_0, F_0, R_0$.

6.2 Equivalence relations

Suppose that X is a set. A *relation* on X is a rule $x \sim y$ that is either true or false for x and y in X. The relation is called an *equivalence relation* if the following three axioms are satisfied.

1. Reflexive property: $x \sim x$ for all $x \in X$.
2. Symmetric property: if $x \sim y$ then $y \sim x$.
3. Transitive property: if $x \sim y$ and $y \sim z$ then $x \sim z$.

For example, if $X = \mathbb{Z}$ then define $x \sim y$ to be true if $x - y$ is even. Thus, $x \sim y$ if and only if x and y are either both even or both odd.

Proposition 6.3. *Let X be a set with an equivalence relation $\sim$. If $x \in X$ define*

$$C(x) = \{z \in X \mid z \sim x\}.$$

Then

$$X = \bigcup_{x \in X} C(x), \tag{6.1}$$

and any two sets $C(x)$ and $C(y)$ are either disjoint or equal.

The set $C(x)$ is called the *equivalence class* of X.

Proof. By the reflexive property, $x \in C(x)$, so every element of X is an element of an equivalence class, whence (6.1).

Suppose that $C(x)$ and $C(y)$ are not disjoint. Then there is a $z \in C(x) \cap C(y)$. Thus $z \sim x$ and $z \sim y$. Using the symmetric and transitive properties, $x \sim z$ and so $x \sim y$. Now we can show that $C(x) = C(y)$. If $w \in C(x)$ then $w \sim x$ and $x \sim y$ so $w \sim y$ and so $w \in C(y)$. We have proved that $C(x) \subseteq C(y)$ and $C(y) \subseteq C(x)$ is proved the same way. Thus if $C(x)$ and $C(y)$ are not disjoint they are equal. □

We see that X is partitioned into disjoint equivalence classes.

Exercise 6.1. Let $X = \mathbb{Z}$, and let m be a positive integer. Define $x \sim y$ if $x - y$ is a multiple of m. Prove that this is an equivalence relation. How many equivalence classes are there?

6.3 Orders of elements and subgroups

Proposition 6.4. *Let G be a finite group, and let $g \in G$. There exists an integer n such that $g^k = 1$ in G if and only if n divides k. We have*

$$\{g^n \mid n \in \mathbb{Z}\} = \{1, g, g^2, \cdots, g^{k-1}\}. \tag{6.2}$$

The number k is called the *order* of g, and we sometimes denote it $|g|$. We denote the group (1.2) with the notation $\langle g \rangle$, and call it the *cyclic subgroup of G generated by g*. (In the notation of the last section, this would have been denoted $\langle \{g\} \rangle$ as the subgroup generated by a set $\{g\}$ consisting of the single element g.) The term *cyclic* here refers to the fact that the sequence $1, g, g^2, \cdots, g^{k-1}, 1, g, g^2, \cdots$ repeats, that is, $g^{n+k} = g^k$ for all n.

Proof. We first prove that there exists an integer $l > 0$ such that $g^l = 1$. Since G is finite, the set of elements

$$1, g, g^2, \cdots$$

is not infinite, so $g^n = g^m$ for some $n > m$. Let $l = n - m$. Then $g^l = g^{n-m} = g^n (g^m)^{-1} = 1$ since g^n and g^m are equal.

Now let k be the *smallest* positive integer such that $g^k = 1$. We must show that $g^n = 1$ if and only if k divides n. Divide k into n, with quotient q and remainder r. Thus $n = qk + r$ where $0 \leqslant r < k$. We observe that

$$g^n = g^{kq+r} = (g^k)^q \cdot g^r = 1^q \cdot g^r = g^r.$$

Now if k divides n, then $r = 0$, so $g^n = 1$. On the other hand, if $g^n = 1$, then $g^r = 1$, and since $0 \leqslant r < k$ and k is the smallest *positive* integer such that $g^k = 1$, r is not positive, that is, it is zero and $n = qk$. We have proved that $g^n = 1$ if and only if k divides n. □

If G is a group, the number of elements of G is called the *order* of G; we denote it $|G|$; more generally if X is a finite set, we denote the number of elements of X by $|X|$, but we prefer the term *cardinality* for $|X|$ if X is not a group. We will mostly consider finite groups, so $|G|$ is a finite number; if it isn't, we use the same notation but write $|G| = \infty$.

Proposition 6.5. *Let G be a group and $g \in G$. Then the order of $\langle g \rangle$ equals the order of g.*

Proof. It follows from Proposition 6.4 that if k is the order of g, then $1, g, \cdots, g^{k-1}$ are all distinct, and that these are exactly the elements of $\langle g \rangle$, so the order of $\langle g \rangle$ is also k. □

If G is a group (finite or infinite) and H a subgroup, and if $x \in G$ we denote

$$xH = \{xh \mid h \in H\}.$$

This set is called a *left coset* of H. Similarly $Hx = \{hx \mid h \in H\}$ is called a *right coset*.

Proposition 6.6. *Let G be a finite group and let H be a subgroup. Define a relation $x \sim y$ on G by $x \sim y$ if $x^{-1}y \in H$. Then $\sim$ is an equivalence relation, and if $x \in G$, the equivalence class of x is the left coset xH. The cardinality of xH is $|H|$.*

Proof. If $x, y \in G$ write $x \sim y$ if $x^{-1}y \in H$. Let us check that this is an equivalence relation. Clearly $x^{-1}x = 1 \in H$ so $x \sim x$. If $x \sim y$ then $x^{-1}y \in H$ so $y^{-1}x = (x^{-1}y)^{-1} \in H$. Finally, if $x \sim y$ and $y \sim z$ then $x^{-1}y$ and $y^{-1}z$ are in H so

$$x^{-1}z = (x^{-1}y)(y^{-1}z) \in H.$$

Now we show that $x \sim y$ if and only if $y \in xH$. Indeed, let us write $h = x^{-1}y$. Then

$$x \sim y \quad \Leftrightarrow \quad h \in H \quad \Leftrightarrow \quad y = xh \text{ with } h \in H \quad \Leftrightarrow \quad y \in xH.$$

This means that the equivalence class $C(x)$ of x is xH, since

$$y \in C(x) \quad \Leftrightarrow \quad y \sim x \quad \Leftrightarrow \quad y \in xH$$

means that $C(x)$ and xH are identical.

To show that H and xH have the same cardinality, define a map $f\colon H \longrightarrow xH$ by $f(h) = xh$. It is by definition surjective, and it is injective since if $xh = yh$ then right multiplying by h^{-1} shows that $x = y$. Thus f is a bijection and so H and xH have the same number of elements. □

Theorem 6.7. *Let G be a finite group and H a subgroup. Then the order of H divides the order of G.*

Proof. We see from Proposition 6.6 that G is partitioned into disjoint cosets xH, all of which have the same cardinality $|H|$ and so $|G|/|H|$ is the number of cosets; in particular, it is an integer, which means that $|H|$ divides $|G|$. □

Proposition 6.8. *Let G be a finite group, and let $g \in G$. Then $|g|$ divides $|G|$.*

Proof. This follows from Theorem 6.7 on taking $H = \langle g \rangle$. □

If G is a group and H a subgroup, the number of left cosets xH is called the *index* of H in G, and it is denoted $[G: H]$.

6.4 Isomorphisms and homomorphisms

Let G and H be groups. When are two groups the "same"? They should be considered equivalent or *isomorphic* if they have the "same" multiplication table. This means that there is a bijection $f: G \longrightarrow H$ that takes the multiplication of G into the multiplication of H. Explicitly, $f(gg') = f(g)f(g')$ for $g, g' \in G$. The map f is called an *isomorphism*.

For example, here are the multiplication tables of two groups:

$\times$	1_G	t	u
1_G	1_G	t	u
t	t	u	1_G
u	u	1_G	t

$\times$	1_H	a	b
1_H	1_H	a	b
a	a	b	1_H
b	b	1_H	a

Table 6.1. Two isomorphic groups. Left: $G = \{1_G, t, h\}$. Right: $H = \{1_H, a, b\}$.

These two tables describe the isomorphic groups, and indeed the map $f: G \longrightarrow H$ such that $f(1_G) = 1_H$, $f(t) = a$ and $f(u) = b$ is an isomorphism.

A *homomorphism* is a map $f: G \longrightarrow H$ that is not assumed to be a bijection, but that satisfies $f(gg') = f(g)f(g')$. There are two groups that we may associate with a homomorphism. The *kernel* of f is

$$\ker(f) = \{g \in G \mid f(g) = 1\}.$$

The *image* of f is

$$\mathrm{im}(f) = \{f(g) \in H \mid g \in G\}.$$

Thus the image of f is a subgroup of H and the kernel is a subgroup of G.

As an example of a group homomorphism, let $\mathfrak{G}$ be (as before) the group of the usual $3 \times 3 \times 3$ Rubik's cube generated by U, D, L, R, F and B, and let $\mathfrak{H}$ be the corresponding group of the smaller $2 \times 2 \times 2$ Rubik's cube. We will denote the standard generators (consisting of rotations of the six faces) of the group $\mathfrak{H}$ by u, d, l, r, f and b, in an obvious notation.

Proposition 6.9. *There is a homomorphism* $\phi\colon \mathfrak{G} \longrightarrow \mathfrak{H}$ *such that* $\phi(U) = u$, $\phi(D) = d$, $\phi(L) = l$, $\phi(R) = r$, $\phi(F) = f$ *and* $\phi(B) = b$.

Proof. To see this, let us write any element of $g \in \mathfrak{G}$ as a product $X_1 \cdots X_n$, where each X_i is one of U, D, L, R, F and B. We would like to define $\phi(g) = x_1 \cdots x_n$, where each x_i is the element of $\mathfrak{H}$ corresponding to X_i; thus if $X_i = U$ then $x_i = u$, and so forth. However to make this definition, we must show that $\phi(g)$ is well-define. Thus if $X_1 \cdots X_n = Y_1 \cdots Y_m$, and if $y_1, \cdots, y_m$ are the elements of $\mathfrak{H}$ corresponding to $Y_1, \cdots, Y_m$, we must show that

$$x_1 \cdots x_n = y_1 \cdots y_m. \tag{6.3}$$

The proof of (6.3) is based on the observation that the configuration of the $2 \times 2 \times 2$ cube after $x_1 \cdots x_n$ can be read off from the configuration of the $3 \times 3 \times 3$ cube after $X_1 \cdots X_n$. The reason is that the eight corner pieces of the $3 \times 3 \times 3$ correspond to the eight pieces of the smaller cube, and will be in the same location and orientation. This is obvious, but to clarify the point we consider an example. We will consider $X_1 = R$ and $X_2 = U$. In Figure 6.1 (left) we see the effect of $X_1 X_2 = RU$. Ignoring all but the corner pieces as in Figure 6.1 (middle) we see that the configuration of the corners is the same as the configuration of the corners in the small cube (Figure 6.1, middle) after $x_1 x_2 = ru$.

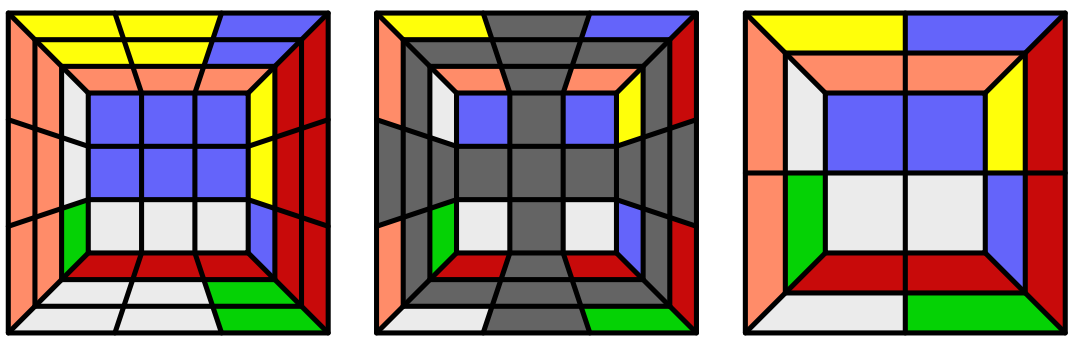

Figure 6.1. Left: after RU. Middle: Ignoring all but corners. Right: The small cube after ru.

Now, since $X_1 \cdots X_n$ and $Y_1 \cdots Y_m$ leave the corners (indeed the entire cube) in the same configuration, it follows that $x_1 \cdots x_n$ and $y_1 \cdots y_m$ leave the small cube in the same configuration, which proves (6.3). Thus we may define

$$\phi(X_1 \cdots X_n) = x_1 \cdots x_n,$$

and this map is well-defined. It is easy to see that it is a homomorphism. □

Let us exhibit some non-trivial elements of the kernel of ϕ. An interesting and often useful operation is $(R^2U^2)^3 = R^2U^2R^2U^2R^2U^2$. Its utility is that it can be done very quickly, and it only affects edges, as we can see from Figure 6.2. Its effect is to switch two pairs of edges. Now it is clear from the principle explained in the proof of Proposition 6.9 that *any operation that only effects edges is in the kernel of* ϕ.

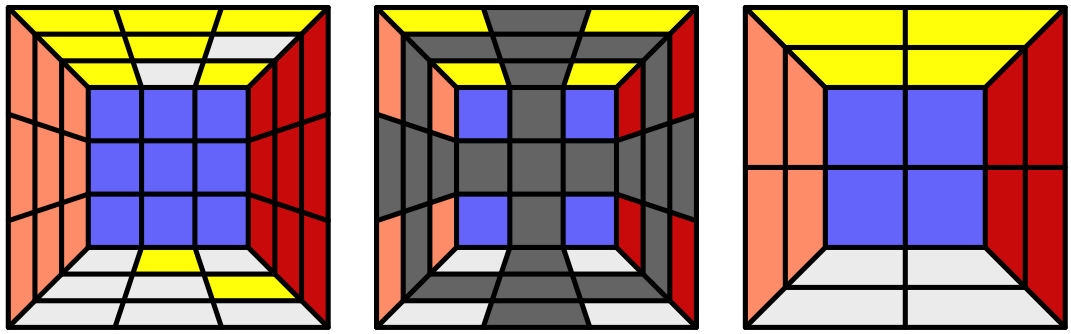

Figure 6.2. Left: after $(R^2 U^2)^3$. Middle: It has no effect on the corners! Right: So the small cube is unchanged after $(r^2 u^2)^3$.

Exercise 6.2. Show that the homomorphism ϕ can be extended to a homomorphism ϕ_0: $\mathfrak{G}_0 \longrightarrow \mathfrak{H}$ such that $\phi(U_m) = \phi(D_m) = \phi(R_m) = \phi(L_m) = \phi(F_m) = \phi(B_m) = 1$.

6.5 Group Actions

The fundamental importance of groups is closely connected with the concept of a *group acting on a set*. Let G be a group and X a set. A *group action* is map $m: G \times X \longrightarrow X$ satisfying certain assumptions that we will next describe. Since this map is thought of as a sort of multiplication we may write $g \cdot x$ or simply gx for $m(g,x)$. It is assumed that $1 \cdot x = x$ for all $x \in X$, and if $g, h \in G$, $x \in X$ it is assumed that $g \cdot (h \cdot x) = (gh) \cdot x$.

Group actions abound in mathematics and we will encounter more than a few. As a first example, let $G = \mathrm{GL}(n, \mathbb{R})$ be the group of $n \times n$ invertible real matrices, and let $X = \mathbb{R}^n$ be the n-dimensional vector space of column vectors

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

The action of G on X is by matrix multiplication: if $g \in G$ and $x \in X$ then gx is the usual product of a matrix with a column vector.

As a second example, let H be a subgroup of a group G, and let G/H be the space of left cosets:

$$G/H = \{xH \,|\, x \in G\}.$$

The group G acts on G/H by left multiplication:

$$g \cdot xH = (gx)H.$$

Note that this multiplication is well defined: if $xH = yH$ then $(gx)H = (gy)H$, so the definition of $g \cdot xH$ does not depend on the choice of representative x for the coset xH.

Proposition 6.10. *Let G be a group and X a set with an action of G. Define a relation $\sim$ on X by $x \sim y$ if and only if $x = gy$ for some $g \in G$. Then $\sim$ is an equivalence relation.*

Proof. Since $1 \cdot x = x$ we have $x \sim x$. If $x = gy$ then $y = g^{-1}x$, so $x \sim y$ implies $y \sim x$. Finally, if $x \sim y$ and $y \sim z$, we can find g and h so that $x = gy$ and $y = hz$; then $x = gh \cdot z$ so $x \sim z$. □

If G acts on X and $x_0 \in X$ then $H = \{g \in G \mid gx_0 = x_0\}$ is easily checked to be a group, called the *isotropy subgroup* or *stabilizer* of x_0.

The equivalence classes for this equivalence relation are called *orbits*. The action is called transitive if there exists a single orbit. The following fact is rather important.

Theorem 6.11. *Let X be a group with a transitive action of the group G. Let x_0 be an element of X, and let H be the isotropy group of x_0. Then there is a bijection $f: X \longrightarrow G/H$ such that $f(gx_0) = gH$ for all $g \in G$.*

Proof. First note that if g_1 and g_2 are in G then

$$g_1x_0 = g_2x_0 \quad \Leftrightarrow \quad g_2^{-1}g_1x_0 = x_0 \quad \Leftrightarrow \quad g_2^{-1}g_1 \in H \quad \Leftrightarrow \quad g_1H = g_2H. \tag{6.4}$$

Since the action of G on X is transitive, the orbit of x_0 is all of X, which means that every element of X can be written as gx_0. Thus we can define a map $f: X \longrightarrow G/H$ by $f(gx_0) = gH$ if we check that this is well defined, that is, that the definiton $f(gx_0) = gH$ does not depend on the choice of g. This however follows from (6.4).

With the map f defined, (6.4) implies that $f(x) = f(y)$ if and only if $x = y$, as we can see by writing $x = g_1x_0$ and $y = g_2x_0$ for suitable g_1 and $g_2 \in G$, again by the assumed transitivity of the action. Thus f is injective.

Finally, f is surjective since by definition every element of G/H is of the form $gH = f(gx_0)$ for some $g \in G$. □

Proposition 6.12. *Let G be a finite group acting on a set X. Then each orbit of X has cardinality dividing the order of G; indeed, the order of the orbit of $x_0 \in X$ is the index $[G: H]$, where H is the stabilizer of x_0.*

Proof. Let C be the orbit of $x_0 \in X$. Then G acts on C, and this action is transitive. Thus if H is the isotropy group of x_0, the order of C is the index of H since by Theorem 6.11 there is a bijection of G/H with C. □

6.6 The Theory of Conjugation

So far, we have experience conjugation in its practical aspect. But conjugation is a fundamental tool in group theory. We look at it now from a more theoretical point of view.

If g and h are elements of a group G we say they g is a *conjugate* of h there exists an $x \in G$ such that $g = xhx^{-1}$. The relation of being conjugate is called *conjugacy*.

Proposition 6.13. *The relation of conjugacy is an equivalence relation.*

In view of the fact that the relation is symmetric, we will also say that g and h are *conjugates* (of each other) if g is a conjugate of h.

Proof. If $x = 1$ we have $xgx^{-1} = g$ so g is conjugate to itself, and the reflexive property is satisfied.

If g is conjugate to h write $g = xhx^{-1}$. Then $h = x^{-1}gx = x^{-1}g(x^{-1})^{-1}$ so h is conjugate to g and the symmetric property is satisfied.

Finally if g is conjugate to h and h is conjugate to k we can find x and y so that $g = xhx^{-1}$ and $h = yky^{-1}$. Then $g = xyky^{-1}x^{-1} = zkz^{-1}$ where $z = xy$, and so g is conjugate to k. □

Since conjugacy is an equivalence relation, *group G is partitioned into disjoint equivalence classes under the operation of conjugacy.* The equivalence classes are called *conjugacy classes.*

Exercise 6.3. Consider the group of order 6 with the multiplication table Table 1.1. Show that there are three conjugacy classes, and they are:

$$\{1\}, \qquad \{t, u\}, \qquad \{v, w, x\}.$$

If $x \in G$ let

$$Z(x) = \{g \in G \mid xg = gx\}.$$

It is called the *centralizer of x*. It is straightforward to check that $Z(x)$ is a subgroup of G, consisting of the set of elements of G that commute with x.

Theorem 6.14. *Let G be a finite group, and let $x \in G$. Then the order of the conjugacy class of x is the index $[G: Z(x)]$.*

Proof. We can define an action of G on itself by defining

$$g * x = gxg^{-1}.$$

For notational reasons we will *not* use the notation gx for this group action. It satisfies the definition of a group action. In particular

$$g * (h * x) = ghxh^{-1}g^{-1} = (gh)x(gh)^{-1} = (gh) * x.$$

Now the stabilizer of x in this action is the set of g such that $x = gxg^{-1}$, that is, $gx = xg$; that is, the stabilizer of x is $Z(x)$. The statement now follows from Proposition 6.12. □