On Rubik's Cube

Olof Bergvall, olofberg@kth.se
Elin Hynning, ehynning@kth.se
Mikael Hedberg, mihed@kth.se
Joel Mickelin, joelmi@kth.se
Patrick Masawe, masawe@kth.se

Supervisors: Sandra Di Rocco and Carel Faber

May 16, 2010

Abstract

Rubik's Cube is a three dimensional mechanical puzzle. In this report Rubik's Cube is considered from a mathematical perspective. We see that Rubik's Cube can be given the structure of a group and we define this group and deduce some of its properties. For the reader unfamiliar with group theory, a short introduction to elementary group theory is provided.

Contents

Chapter 1

On Rubik's Cube

1.1 Introduction

The aim of this report is to describe Rubik's Cube in a mathematical way. The mathematical structure describing Rubik's Cube is a group structure, and we will therefore use abstract algebra and group theory to classify Rubik's Cube as a mathematical object.

The first section of the first chapter is devoted to elementary group theory and may be skipped by readers familiar with these concepts. However, references will be made to this chapter in subsequent chapters.

In the second section of the first chapter we discuss the mathematical properties of Rubik's Cube. We start by considering sequences of rotations of the faces of the cube, and let them act on the set of facets of the cube. We thus obtain one infinite group of concatenations of rotations and one finite group of scramblings of facets. Through observations of Rubik's Cube and group theoretic arguments we describe the latter group and determine its cardinality. Since the cube has 54 facets, the latter group is a subgroup of S_{54}. Since this is an enormous group we choose to divide the cubies of the cube into two subsets, corners and edges, and define a concept of orientation of the cubies. We shall see that the permutation of the corner cubies must have the same sign as the permutation of the edge cubies. We shall also see that we cannot change the orientation of a single cubie without changing the orientation of another cubie of the same kind.

The last five chapters are devoted to various subjects related to Rubik's Cube.

1.2 Introductory Group Theory

In this section we will introduce and prove notions concerning introductory group theory. People who are familiar with basic concepts concerning groups may skip ahead to the next section.

1.2.1 Groups

This subsection will define and prove some basic properties of groups.

Definition 1.2.1. A **binary operator** on a set S is a function $* : S \times S \mapsto S$ where $S \times S$ is the set of ordered pairs of elements in S.

It is important to note that if $(s_1, s_2) \in S \times S$ then $*(s_1, s_2) \neq *(s_2, s_1)$ in general. If $*(s_1, s_2) = *(s_2, s_1)$ then s_1 and s_2 are said to *commute*. If $*(s_1, s_2) = *(s_2, s_1)$ for all $(s_1, s_2) \in S \times S$ then the binary operator $*$ is said to be *Abelian* or *commutative*.

Remark 1.2.2. If $(s_1, s_2) \in S \times S$ we denote $*(s_1, s_2)$ as $s_1 * s_2$ or simply as $s_1 s_2$.

Definition 1.2.3. A **group** is a set G with an associated binary operator $*$, satisfying:

(1)**Associativity:**

$$g_1 * (g_2 * g_3) = (g_1 * g_2) * g_3, \forall g_1, g_2, g_3 \in G.$$

(2)**Identity:**

$$\exists id \in G \text{ such that } \forall g \in G, g * id = id * g = g.$$

(3)**Inverse:**

$$\forall g \in G \text{ there is a } g^{-1} \in G \text{ such that } g * g^{-1} = g^{-1} * g = id.$$

Remark 1.2.4. A group G under the operation $*$ is denoted by $(G, *)$, (or simply by G if the binary operator is clear from the context).

Example 1. The set of continuous, bijective functions, F, on $\mathbb{R}$ is a group under the operation of composition. We check that this is true by verifying the group axioms.

We know from Calculus that $f_1, f_2, f_3 \in F \Rightarrow f_1 \circ (f_2 \circ f_3) = (f_1 \circ f_2) \circ f_3$, so F is associative under composition. The identity element in this case is $f_0(x) = x$, since $f \in F \Rightarrow f_0 \circ f = f \circ f_0 = f$. It is also clear that $f \in F \Rightarrow \exists\ f^{-1} \in F$ such that $f \circ f^{-1} = f^{-1} \circ f = x = f_0$. We have thus shown that F is a group under the operation of composition.

Below follow some simple, but important, facts about groups.

Proposition 1.2.5. *If G is a group then the following is true:*

(1) The identity, id, of G is unique.

(2) If $g \in G$ then the inverse of g, g^{-1}, is unique.

(3) The inverse of $g_1 g_2$, $g_1, g_2 \in G$, is $g_2^{-1} g_1^{-1}$.

(4) The inverse of the identity, id, is the identity itself.

(5) If $g \in G$, then $(g^{-1})^{-1} = g$.

Proof. (1) Let id_1 and id_2 be identities of G. Then $id_1 * g = g * id_1 = g, \forall g \in G$ and $id_2 * g = g * id_2 = g$, for all $g \in G$. In particular $id_1 * id_2 = id_2 * id_1 = id_2$ and $id_2 * id_1 = id_1 * id_2 = id_1$. Hence $id_1 = id_1 * id_2 = id_2 * id_1 = id_2$, so the identity is unique.

(2) Let g be an element of G and let $g_1 \in G$ and $g_2 \in G$ be elements such that $gg_1 = g_1 g = id$ and $gg_2 = g_2 g = id$. If we multiply the latter equation from the left by g_1 we get

$$g_1 * (g * g_2) = g_1 * id,$$

$$(g_1 * g) * g_2 = g_1,$$

$$(id) * g_2 = g_1,$$

$$g_2 = g_1.$$

Hence, the inverse of every element $g \in G$ is unique.

(3) Multiply $g_1 g_2$ from the right by $g_2^{-1} g_1^{-1}$. This gives

$$(g_1 g_2)(g_2^{-1} g_1^{-1}) = g_1 (g_2 g_2^{-1}) g_1^{-1} = g_1 (id) g_1^{-1} = g_1 g_1^{-1} = id.$$

$g_2^{-1} g_1^{-1}$ is therefore a right inverse of $g_1 g_2$.

Now multiply $g_1 g_2$ from the left by $g_2^{-1} g_1^{-1}$.

$$(g_2^{-1} g_1^{-1})(g_1 g_2) = g_2^{-1} (g_1^{-1} g_1) g_2 = id$$

Hence, the inverse of $g_1 g_2$ is $g_2^{-1} g_1^{-1}$.

(4) $id * id = id \Rightarrow id^{-1} = id$

(5) Consider the equation $g^{-1}(g^{-1})^{-1} = id$. Multiplying from the left by g gives $(g^{-1})^{-1} = g$. □

Proposition 1.2.6 (Generalised Associative Law)**.** *Let G be a group. For any $g_1, g_2, \ldots, g_n \in G$ the value of the expression $g_1 g_2 \ldots g_n$ is independent of how the expression is bracketed.*

Proof. Let $\prod_{i=1}^{1} g_i = g_1$ and define $\prod_{i=1}^{n+1} g_i$ recursively by

$$\prod_{i=1}^{n+1} g_i = \left(\prod_{i=1}^{n} g_i \right) g_{n+1}.$$

Now, let n be a fixed, nonnegative integer and consider the expression

$$\left(\prod_{i=1}^{n} g_i\right)\left(\prod_{j=1}^{m} g_{n+j}\right).$$

We want to prove that the above is equal to $\prod_{i=1}^{n+m} g_i$.

By definition, this is the case for $m = 1$. Now assume that the above holds for $m = k \geq 1$ and consider the case $m = k + 1$. We have

$$\left(\prod_{i=1}^{n} g_i\right)\left(\prod_{j=1}^{k+1} g_{n+j}\right) = \left(\prod_{i=1}^{n} g_i\right)\left(\left(\prod_{j=1}^{k} g_{n+j}\right) g_{n+k+1}\right) =$$

$$= \left(\left(\prod_{i=1}^{n} g_i\right)\left(\prod_{j=1}^{k} g_{n+j}\right)\right) g_{n+k+1} = \left(\prod_{i=1}^{n+k} g_i\right) g_{n+k+1} = \prod_{i=1}^{n+k+1} g_i,$$

which proves the claim. □

Definition 1.2.7. If G is a group and $g \in G$ we will denote the expression $\underbrace{gg\ldots g}_{n \text{ times}}$ by g^n.

Note that, because of the generalised associative law, g^n is well defined.

Proposition 1.2.8. *Let G be a group and let $g_1, g_2 \in G$. Then the equations $g_1 x = g_2$ and $x g_1 = g_2$ have unique solutions in G.*

Proof. Consider the equation $g_1 x = g_2$. Multiply both sides from the left by g_1^{-1}. This gives $x = g_1^{-1} g_2$. By Proposition 1.2.5 g_1^{-1} is unique. Hence x is unique.

Now consider the equation $x g_1 = g_2$. Multiply both sides of the equation from the right by g_1^{-1}. This gives $x = g_2 g_1^{-1}$. Since g_1^{-1} is unique, so is x. □

Corollary 1.2.9. *The left and right cancellation laws hold in groups, (i.e. $gx = gy$ implies $x = y$ and $xg = yg$ implies $x = y$).*

Proof. This follows immediately from Proposition 2.1.8. □

1.2.2 The Symmetric Group

In this subsection we will introduce the symmetric group and concepts associated with this group.

Definition 1.2.10. For any set A, a bijection $\phi : A \longrightarrow A$ is called a **permutation** of A.

Proposition 1.2.11. *The set of all permutations on a set A, denoted S_A, is a group under the operation of composition of functions.*

Proof. (1) The associative condition holds since permutations are functions, thus being associative.
(2) The identity element is the permutation $id_A(a) = a$, $\forall a \in A$.
(3) Let $\phi \in S_A$. ϕ is bijective, hence ϕ has a bijective inverse, ϕ^{-1}. ϕ^{-1} is a bijective function from A to A and therefore an element of S_A. □

Note that A is not assumed to be finite in the above definitions. In the following however, this will be assumed.

Definition 1.2.12. A **cycle** is a permutation on a subset $\{a_i\} \subseteq A$ (A finite) defined by $a_1 \longrightarrow a_2, a_2 \longrightarrow a_3, \ldots, a_n \longrightarrow a_1$. A cycle is denoted $(a_1 a_2 \ldots a_n)$ and the number n is called the **length** of the cycle. A cycle of length n is called an **n-cycle**.

Note that there are several ways of writing the same cycle. For example the cycle $(a_1 a_2 \ldots a_n)$ is the same as the cycle $(a_n a_1 a_2 \ldots a_{n-1})$. This is however not a problem when the cycles are considered to be functions. We may also note that compositions of disjoint cycles commute.

When writing compositions of cycles, the singlet cycles, (a), will be omitted. Compositions of permutations will also be referred to as products of permutations.

There is a generalisation of the cycle concept to bijections on any set, not necessarily finite. Let σ be a function on the set A. If $a \in A$ the sequence

$$\ldots, \sigma^{-2}(a), \sigma^{-1}(a), \sigma^0(a), \sigma^1(a), \sigma^2(a), \ldots$$

is called the **orbit** of a under σ and is denoted $\mathcal{O}_{\sigma(a)}$. Note that if A is a finite set the orbit of a is just the cycle $(a\ \sigma(a)\ \sigma^2(a) \ldots \sigma^n(a))$ where n is the largest integer such that $\sigma^n(a) \neq \sigma^m(a)$ for all $m < n$, $m \geq 0$.

Proposition 1.2.13. *Any permutation σ on a set A can be written as a product of disjoint cycles.*

Proof. Take $\sigma \in S_A$. The orbits of the elements of A under σ define an equivalence relation, $\sim$, on A, by $a \sim b$ precisely if $a = \sigma^i(b)$ for some $i \in \mathbb{Z}$. This can be verified by checking the axioms for equivalence relations, namely

(1) $a \sim a$ (Reflexivity)
(2) $a \sim b \Leftrightarrow b \sim a$ (Symmetry)
(3) $a \sim b$ and $b \sim c \Rightarrow a \sim c$ (Transitivity)

(1) If $a \in A$ then $\sigma^0(a) = a$ so $a \sim a$.
(2) If $a, b \in A$ and $a \sim b$ then there is an $i \in \mathbb{Z}$ such that $a = \sigma^i(b)$. But then $b = \sigma^{-i}(a)$ so $b \sim a$.
(3) If $a, b, c \in A$, $a \sim b$ and $b \sim c$ there are integers $i, j \in \mathbb{Z}$ such that $a = \sigma^i(b)$ and $b = \sigma^j(c)$. Hence $a = \sigma^{i+j}(c)$ so $a \sim c$.

Hence $\sim$ is an equivalence relation on A. It is well known that an equivalence relation induces a partition on the underlying set. Hence each element $a \in A$ lies in precisely one orbit. This proves the claim. □

Theorem 1.2.14. *Assume that $|A| = n$. Then, $|S_A| = n!$.*

Proof. Take $a_1 \in A$. This element can be mapped by $\sigma \in S_A$ in n different ways. Pick one of them. Take a new element $a_2 \in A$ such that $a_1 \neq a_2$. The bijectivity of σ gives that a_2 can be mapped in $n - 1$ ways. Iterating over the elements of A, we see that the number of possible permutations is $n \cdot (n-1) \dots \cdot 2 \cdot 1 = n!$. □

Proposition 1.2.15. *Every permutation may be expressed as a product of 2-cycles.*

Proof. Consider the cycle $(a_1 a_2 \dots a_n)$. This cycle can be expressed as $(a_1 a_2 \dots a_n) = (a_1 a_n)(a_1 a_{n-1}) \dots (a_1 a_3)(a_1 a_2)$. Thus every cycle can be expressed as a product of 2-cycles. But every permutation can be expressed as a product of disjoint cycles, of which each can be expressed as a product of 2-cycles. Hence, every permutation can be expressed as a product of 2-cycles. □

Remark 1.2.16. 2-cycles are also called transpositions.

Definition 1.2.17. Let σ be a permutation. If σ can be written as an even number of transpositions we say that the permutation σ is **even**. Similarly, if σ can be written as an odd number of transpositions we say that σ is **odd**.

Theorem 1.2.18. *No permutation may be written as a product of both an even number of transpositions and an odd number of transpositions.*

Proof. Note that S_A, for $|A| = n$, is isomorphic to the permutations of the rows in the identity matrix I_n. We know from linear algebra that this matrix has determinant 1, and that interchanging two rows of any matrix will change the sign of the determinant. Thus, if any matrix could be obtained by both a sequence of even and a sequence of odd permutations, it would have both determinant 1 and -1. This is impossible and the claim follows. □

Remark 1.2.19. The proof above suggests the definition of a sign function on permutations. We define the **signature** of the permutation $\sigma \in S_A$ to be 1 if the determinant of the matrix of the proof corresponding to σ is 1 and -1 if the determinant is -1. We see that this is just another way of saying that a permutation is even or odd, but nonetheless sometimes useful.

Definition 1.2.20. For a permutation S_X on a finite set X, we call the set of even permutations on X the **alternating group** on X, and we denote this set A_X.

Theorem 1.2.21. *A_X, as defined above, is a group.*

Proof. (1) **Closure** Take $x, y \in A_X$. x can be written as a product of $2n$ transpositions, while y can be written as a product of $2m$ transpositions, $m, n \in \mathbb{Z}$. The product can be written as $2(m+n)$ transpositions, and is therefore in A_X.

(2) **Identity** The identity, id, of S_X is a product of 0 transpositions. This is clearly an even number of transpositions so id is also an element of A_X.

(3) **Inverse** The inverse of any permutation can be obtained by reversing the order of its transpositions. The inverse of an even permutation must therefore be even and thus an element of A_X. □

Theorem 1.2.22. *The cardinality of A_X is $\frac{n!}{2}$ if $|X| = n \geq 2$.*

Proof. Let us denote the odd permutations of X as B_X. If we can find a bijection between A_X and B_X, we have proven the theorem, since the two sets must then have the same cardinality.

Let us define a bijection ϕ as such: Take any transposition (which must exist, since $|X| \geq 2$) $\sigma \in S_X$, and define $\phi(x) = \sigma \circ x, x \in A_X$. x being even gives that $\phi(x)$ is odd, therefore $\phi(x) \in B_X$. Note that $\forall x, y \in A_X, \phi(x) = \phi(y)$ implies $\sigma \circ x = \sigma \circ y$, and left cancellation gives $x = y$. Therefore, ϕ is one-to-one. The cancellation law also gives that for any $\gamma \in B_X$, $\phi^{-1}(\gamma) = \sigma^{-1}\gamma \in A_X$. Therefore, ϕ is onto, and we have that ϕ is a bijection. Therefore,
$|A_X| = |B_X|$
$|A_X| + |B_X| = n!$
which gives that $|A_X| = \frac{n!}{2}$. □

Lemma 1.2.23. *The set $S = \{(1,2), (2,3), \ldots, (n-1, n)\}$ for $n \geq 2$ generates S_n.*

Proof. Let $(x, x+k)$ be a transposition in S_n. Then, $(x, x+k) = (x, x+1)(x+1, x+2)\cdots(x+k-2, x+k-1)(x+k-1, x+k)(x+k-2, x+k-1\cdots)\cdots(x, x+1)(x+1, x+2)$. So by conjugation of the transpositions in the set S we can obtain any transposition in S_n. It then follows from Proposition 1.2.15 that S generates S_n. □

Theorem 1.2.24. *The alternating group, A_n, is generated by the 3-cycles* $(1,2,3),(2,3,4),...(n-2,n-1,n)$.

Proof. A_n is generated by all products of two transpositions. Thus it suffices to prove that we can get all the products of two transpositions. Clearly we can get all the products of transpositions two "adjacent" numbers:

$$\begin{aligned}
(1,2,3) = \quad & (1,2)(2,3) \\
& (2,3,4) = \quad (2,3)(3,4) \\
& \qquad\qquad (3,4,5) = \quad (3,4)(4,5) \\
& \qquad\qquad\qquad\qquad \ddots \\
& \qquad\qquad\qquad\qquad (n-2,n-1,n) = \quad (n-2,n-1)(n-1,n).
\end{aligned}$$

and if one would like to obtain the pair $(x,x+1)(x+k,x+k+1)$ this can be done by successively multiplying the 3-cycle $(x,x+1,x+2)$ by the elements of the rows between $(x,x+1,x+2)$ and $(x+k,x+k+1,x+k+2)$, i.e.

$$(x,x+1)(x+k,x+k+1) = (x,x+1,x+2)\cdots(x+k,x+k+1,x+k+2).$$

(This corresponds to "taking a walk down the stairs", starting at $(x,x+1)(x+1,x+2)$, and multiplying all the elements on the way down to $(x+k-1,x+k)(x+k,x+k+1)$). It then follows from Lemma 1.2.23 that A_n can be generated by the 3-cycles mentioned above. □

1.2.3 Subgroups

This section will deal with the notion of subgroups and associated concepts.

Definition 1.2.25. For a group $(G, *)$, a **subgroup** $(H, *)$ of $(G, *)$ is a set $H \subseteq G$ which is a group under $*$.

Theorem 1.2.26. *A nonempty subset $H \subseteq G$ is a subgroup of G precisely if*

(1) $x, y \in H \Rightarrow xy \in H$ *and*
(2) $x \in H \Rightarrow x^{-1} \in H$.

Proof. If $(H, *)$ is a subgroup of G, (1) and (2) will hold by definition. Conversely (for $x \in H$), if (1) and (2) hold, $xx^{-1} \in H$. But $xx^{-1} = id$, so $id \in H$. The associativity holds, since the operation in H is the same as for G. Thus, $(H, *)$ is a group, and therefore a subgroup of G. □

Corollary 1.2.27. *For a finite nonempty set H, (1) is sufficient.*

Proof. If $a \in H \Rightarrow \forall n \in \mathbb{N}, a^n \in H$. But H is finite, so $\exists m > n \in \mathbb{N} : a^m = a^n$. Canceling, $a^{m-n} = id$, so $a^{-1} = a^{m-n-1} \in H$. Note that if $m = n + 1$, $a = id$. □

Theorem 1.2.28. *Let G be a group and let A be a nonempty collection of subgroups of G. Then $H = \bigcap_{H_k \in A} H_k$ is a subgroup of G.*

Proof. Let $a, b \in H$. Then $a \in H_k$ for all $H_k \in A$ and $b \in H_k$ for all $H_k \in A$. Since H_k is a subgroup for every $H_k \in A$ and $a, b \in H_k$ we must have $ab \in H_k$ for all $H_k \in A$. Moreover, a^{-1} and b^{-1} are also elements of H_k for all $H_k \in A$. Thus, $ab \in H$ for all $a, b \in H$, so H is closed under the group operation, and every element of H has an inverse in H. Hence, H is a subgroup of G. □

Definition 1.2.29. Let G be a group and let S be a subset of G. We define **the subgroup generated by** S, denoted $< S >$, as the intersection of all subgroups H_i of G containing S, i.e. $< S >= \bigcap H_i$.

Definition 1.2.30. Let G be a group and let S be a subset of G. If $< S >= G$ we say that G is **generated** by the subset S and the elements of S are called generators of G. If S consists of a single element then G is said to be **cyclic**.

Remark 1.2.31. The term "cyclic" comes from the fact that in the finite case a cyclic group, generated by s, may be written

$$\{s^0, s^1, s^2, \ldots, s^n\}$$

where n is the smallest integer such that $s^{n+1} = id$.

We see that cyclic groups, both finite and infinite, must be abelian since if G is a cyclic group generated by g and $g_1, g_2 \in G$ we must have $g_1 = g^i$ and $g_2 = g^j$, for some $i, j \in \mathbb{Z}$, so $g_1 g_2 = g^i g^j = g^{i+j} = g^{j+i} = g^j g^i = g_2 g_1$.

1.2.4 Homomorphisms and Isomorphisms

This subsection will introduce the concepts of homomorphisms and isomorphisms.

Definition 1.2.32. Let $(G, *)$ and $(H, \circ)$ be groups. A function $\phi : G \to H$ is a **homomorphism** if, for all $a, b \in G$, $\phi(a * b) = \phi(a) \circ \phi(b)$.

Definition 1.2.33. A homomorphism which is also bijective is called an **isomorphism**. If G and H are groups and there exists an isomorphism between G and H we say that G and H are **isomorphic** and write $G \cong H$.

Every group is, of course, isomorphic to itself since the identity map clearly is an isomorphism from the group to itself. However, this may not be the only isomorphism from the group to itself. Such an isomorphism is called an *automorphism* and the set of all automorphisms of a group G is denoted $Aut(G)$.

Definition 1.2.34. For a homomorphism $\phi : G \longrightarrow H$, the set

$$Ker(\phi) = \{g \in G | \phi(g) = id_H\}$$

is called the **kernel** of ϕ. The set

$$Im(\phi) = \{\phi(g) \in H | g \in G\}$$

is called the **image** of ϕ.

Note that $Ker(\phi)$ is a subset of G and that $Im(\phi)$ is a subset of H.

Proposition 1.2.35. *Let ϕ be a homomorphism between groups G and H, let g be an element of G and let id_G and id_H be the identities of G and H respectively. Then the following is true:*

(1) $\phi(id_G) = id_H$.
(2) $\phi(g^{-1}) = \phi(g)^{-1}$.
(3) $\phi(g^n) = \phi(g)^n$.
(4) $Ker(\phi)$ *is a subgroup of* G *and* $Im(\phi)$ *is a subgroup of* H.

Proof. (1) $\phi(id_G id_G) = \phi(id_G)\phi(id_G)$. But $id_G id_G = id_G$ so $\phi(id_G id_G) = \phi(id_G)$. Hence, $\phi(id_G)\phi(id_G) = \phi(id_G)$. Cancellation implies $\phi(id_G) = id_H$.

(2) $\phi(g^{-1}g) = \phi(g^{-1})\phi(g)$. But $\phi(g^{-1}g) = \phi(id_G) = id_H$ so $\phi(g^{-1})\phi(g) = id_H$. Cancellation gives $\phi(g^{-1}) = \phi(g)^{-1}$.

(3) $\phi(g^n) = \phi(g)\phi(g^{n-1}) = \ldots = \prod_{i=1}^{n} \phi(g) = \phi(g)^n$.

(4) We note that $Ker(\phi)$ is nonempty, since $id_G \in Ker(\phi)$. Let g_1 and g_2 be elements of $Ker(\phi)$. $\phi(g_1 g_2) = \phi(g_1)\phi(g_2) = id_H id_H = id_H$. Hence $g_1 g_2 \in Ker(\phi)$.

We now need to show that if $g \in Ker(\phi)$ then $g^{-1} \in Ker(\phi)$. Take $g \in Ker(\phi)$ and $g^{-1} \in G$. $\phi(gg^{-1}) = \phi(g)\phi(g^{-1}) = id_H$. But $g \in Ker(\phi)$ so $\phi(g)\phi(g^{-1}) = id_H\phi(g^{-1}) = \phi(g^{-1})$. Hence $\phi(g^{-1}) = id_H$ so $g^{-1} \in Ker(\phi)$.

We note that $Im(\phi)$ is nonempty, since $id_H = \phi(id_G) \in Im(\phi)$. Take $h_1, h_2 \in Im(\phi)$. Then there is $g_1, g_2 \in G$ such that $\phi(g_1) = h_1$ and $\phi(g_2) = h_2$. But $\phi(g_1g_2) \in H$ and $\phi(g_1g_2) = \phi(g_1)\phi(g_2) = h_1h_2$ so $h_1h_2 \in H$.

Now take $h \in Im(\phi)$. Hence, there is a $g \in G : \phi(g) = h$. $g^{-1} \in G$ so $\phi(g^{-1}) \in Im(\phi)$. But $\phi(gg^{-1}) = \phi(g)\phi(g)^{-1} = id_H$ so $h^{-1} = \phi(g)^{-1} \in Im(\phi)$. By Theorem 1.2.26, $Ker(\phi)$ and $Im(\phi)$ are subgroups of G and H, respectively. □

1.2.5 Group Actions

In this section the notion of group actions will be defined.

Definition 1.2.36. Let G be a group and let A be a set. A **group action** of G on A is a map $f : G \times A \to A$ that satisfies:

(1) $f(g_1, f(g_2, a)) = f(g_1 g_2, a)$, for all $g_1, g_2 \in G$ and $a \in A$.
(2) $f(id, a) = a$ for all $a \in A$.

Given a group action $f : G \times A \to A$ one says that *the group G acts on the set A*. It is customary to write $g.a$, instead of $f(g, a)$, and say that the element $g \in G$ acts on the element $a \in A$.

Proposition 1.2.37. *For fixed $g \in G$ the map $\sigma_g : A \to A$ defined by $\sigma_g(a) = g.a$ defines a permutation of the set A.*

Proof. A permutation of a set A is a bijective map from A to A. Hence, σ_g is a permutation iff it has a left and a right inverse.

Left inverse: Let $a \in A$. Consider the map $\sigma_{g^{-1}}$. Now consider the composition $\sigma_{g^{-1}} \circ \sigma_g(a) = f(g^{-1}, f(g, a)) = g^{-1}.(g.a) = id.a = a$. Hence, $\sigma_{g^{-1}}$ is a left inverse of σ_g.

Right inverse: Let $a \in A$. Again, consider the map $\sigma_{g^{-1}}$. Now consider the composition $\sigma_g \circ \sigma_{g^{-1}}(a) = g.(g^{-1}.a) = (gg^{-1}).a = id.a = a$. Hence, $\sigma_{g^{-1}}$ is a right inverse of σ_g.

Thus, $\sigma_g \in S_A$. □

Proposition 1.2.38. *Define a map $\pi : G \to S_A$ by $\pi(g) = \sigma_g$. This map is a homomorphism.*

Proof. Let $g, h \in G$ and let $a \in A$. Then

$$\pi(gh)(a) = \sigma_{gh}(a) = gh.a = g.(h.a) = \sigma_g(h.a) = \sigma_g \circ \sigma_h(a) = \pi(g)\pi(h)(a).$$

Hence π is a homomorphism. □

1.2.6 Quotient Groups

In this section we will introduce the notion of **Quotient Groups**.

Proposition 1.2.39. *Let G and H be groups and let $\phi : G \to H$ be a homomorphism. We define a relation, $\sim$, on G by saying that if $a, b \in G$ then $a \sim b$ precisely if $\phi(a) = \phi(b)$. The relation, $\sim$, is an equivalence relation.*

Proof. We need to check the three equivalence axioms.
(1) $\sim$ is reflexive since $\phi(a) = \phi(a)$.
(2) $\phi(a) = \phi(b) \Leftrightarrow \phi(b) = \phi(a)$. Thus, $\sim$ is symmetric.
(3) If $\phi(a) = \phi(b)$ and $\phi(b) = \phi(c)$ this implies that $\phi(a) = \phi(c)$. Thus, $\sim$ is transitive.
Hence, $\sim$ is an equivalence relation. □

Definition 1.2.40. If $\overline{a}$ and $\overline{b}$ are equivalence classes under $\sim$ we define the product $\overline{a}\overline{b}$ as the set $\{g \in G | \phi(g) = \phi(ab)\}$ (i.e. $\overline{a}\overline{b}$ is the equivalence class of ab, $\overline{ab}$).

Proposition 1.2.41. *Let G, H, ϕ and $\sim$ be defined as in Proposition 1.2.39. The set of equivalence classes under $\sim$ forms a group under the operation defined in Definition 1.2.40. This group is called a* ***quotient group*** *and is denoted $G/Ker(\phi)$.*

Proof. Let the equivalence class of an element $g \in G$ be denoted by $\bar{g}$.
(1) $\overline{a}(\overline{b}\overline{c}) = \overline{a}\overline{bc} = \overline{abc} = (\overline{ab})\overline{c} = (\overline{a}\overline{b})\overline{c}$. Hence, associativity holds.
(2) The identity is $\overline{id}$ (i.e. $Ker(\phi)$).
(3) If $g \in G$ is of equivalence class $\overline{g}$ and g^{-1} of equivalence class $\overline{g^{-1}}$ we see that $\phi(g)\phi(g^{-1}) = \phi(g)\phi(g)^{-1} = id_H$. Hence, $\overline{g}\overline{g^{-1}} = \overline{id}$.
This shows that $G/ker(\phi)$ is a group. □

Theorem 1.2.42. *Let G and H be groups and let ϕ be a homomorphism from G to H. Then $G/Ker(\phi) \cong Im(\phi)$.*

Proof. Define $\varphi : G/Ker(\phi) \to Im(\phi)$ by $\varphi(\overline{g}) = \phi(g)$. If g_1 and g_2 both lies in the equivalence class $\overline{g}$ then, by definition, $\phi(g_1) = \phi(g_2)$ so $\varphi(\overline{g})$ is well defined (i.e. it does not depend on the choice of representative of $\overline{g}$).

We claim that φ is an isomorphism.

φ is a homomorphism because $\varphi(\overline{g_1}\ \overline{g_2}) = \varphi(\overline{g_1 g_2}) = \phi(g_1 g_2) = \phi(g_1)\phi(g_2) = \varphi(\overline{g_1})\varphi(\overline{g_2})$.

If $h \in Im(\phi)$ then there is a $g \in G$ such that $\phi(g) = h$. But then $\varphi(\overline{g}) = h$ so φ is surjective.

Assume φ is not injective. Then there is $\overline{g_1} \neq \overline{g_2}$ such that $\varphi(\overline{g_1}) = \varphi(\overline{g_2})$. But then $\phi(g_1) = \phi(g_2)$ which leads us to conclude that $\overline{g_1} = \overline{g_2}$. This is a contradiction so φ must be injective.

We have thus shown that φ is a homomorphism that is surjective and injective, and thus bijective. Hence, $G/Ker(\phi)$ is isomorphic to $Im(\phi)$. □

Definition 1.2.43. Let N be a subgroup of a group G. N is said to be a **normal subgroup** if $gNg^{-1} = N$ for all $g \in G$. If N is a normal subgroup of G we write $N \trianglelefteq G$.

Definition 1.2.44. The **left coset**, gH, of a subgroup H in a group G, where g is an element of G, is defined as $gH = \{a \in G | a = gh, h \in H\}$, i.e. all elements in G that can be written as a product of the element g and an element in H.

It is possible to define quotient groups using the notion of normal subgroups. The following proposition clarifies why.

Proposition 1.2.45. *A subgroup N of a group G is normal precisely if it is the kernel of a homomorphism.*

Proof. First assume that N is the kernel of a homomorphism $\phi : G \to H$ where H is some group. If $n \in N$, then $\phi(gng^{-1}) = \phi(g)\phi(n)\phi(g^{-1}) = \phi(g)id_H\phi(g)^{-1} = id_H$. Hence, $gng^{-1} \in ker(\phi) = N$ for all $g \in G$ so N is a normal subgroup of G.

Now assume that N is a normal subgroup of G. We may define a binary operation on the cosets of N by $g_1N\dot{g}_2N = (g_1g_2)N$. This operation is well defined because if $a_1, a \in aN$ and $b_1, b \in bN$ we may write $a_1 = an$ and $b_1 = bn'$ for some $n, n' \in N$ (since if $c_1 \in cN$ we have $c_1n_1 = cn$ for some $n_1, n \in N$). What we want to show is that $a_1b_1 \in abN$:

$$a_1b_1 = (an)(bn') = a(bb^{-1})nbn' =$$
$$= ab(b^{-1}nb)n' = ab(n''n')$$

where $n'' = b^{-1}nb$. Hence, $a_1b_1 \in abN$.

We now claim that the set of all cosets of N form a group, G_N, under the operation defined above.

(1) Associativity holds because $aN(bNcN) = aNbcN = abcN = abNcN = (aNbN)cN$. (2) The identity is idN since $gNidN = g * idN = gN = id*gN = idNgN$. (3) The inverse of gN is $g^{-1}N$ since $gNg^{-1}N = gg^{-1}N = idN$.

We now define a function $\varphi : G \to G_N$ by $\varphi(g) = gN$ for all $g \in G$. φ is a homomorphism because if $g_1, g_2 \in G$ then $\varphi(g_1g_2) = g_1g_2N = g_1Ng_2N = \varphi(g_1)\varphi(g_2)$. We now note that $N \subseteq ker(\varphi)$ because if $n \in N$ then $\varphi(n) = nN = N$. Conversely, if $g \in ker(\varphi)$ then $gN = idN$ so $g = id * n$ for some $n \in N$. Hence, $g \in N$ so $ker(\varphi) \subseteq N$. This shows that $ker(\varphi) = N$ and the proof is complete. □

The above proposition shows that the notion of a normal subgroup is "the same" as the notion of a kernel of a homomorphism. Hence, it makes sence to talk about the quotient group G/N as well as the quotient group $G/ker(\varphi)$. Note that G/N is precisely the group G_N in the proof above.

Remark 1.2.46. One may ask whether it is possible to make the construction of G_N of the proof for subgroups that are not normal. It turns out that this is not possible. This is because if H is a subgroup of G and the operation $g_1Hg_2H = g_1g_2H$ is well defined then $a_1, a \in aH$ and $b_1, b \in bH$ implies $a_1b_1H = abH$. Now let g be any element of G and h be any element of H. Let $a_1 = h$, $a = id$ and let $b_1 = b = g^{-1}$. This gives $id * g^{-1}H = hg^{-1}H$ and $g^{-1}H = hg^{-1}H$. Hence, $hg^{-1} \in g^{-1}H$ so $hg^{-1} = g^{-1}h'$ for some $h' \in H$. Hence, $ghg^{-1} = h' \in H$. This shows that it is only possible to define the binary operation of the proof for normal subgroups.

1.2.7 Direct and Semi-Direct Products

In this section, we will introduce the concept of direct products and show some results associated with this notion.

Definition 1.2.47. Let $G_1, G_2, \ldots, G_n$ be groups. Define the **direct product** $G_1 \times G_2 \times \ldots \times G_n$ as the set consisting of all n-tuples $(g_1, g_2, \ldots, g_n)$, where $g_1 \in G_1, g_2 \in G_2, \ldots, g_n \in G_n$.

Definition 1.2.48. Let $G_1, G_2, \ldots, G_n$ be groups with operations $*_1, *_2, \ldots, *_n$. We define a binary operation $*$ on $G_1 \times G_2 \times \ldots G_n$ by $(g_1, g_2, \ldots, g_n) * (g_1', g_2', \ldots, g_n') = (g_1 *_1 g_1', g_2 *_2 g_2', \ldots, g_n *_n g_n')$.

Proposition 1.2.49. *The direct product defined in Definition 1.2.47 together with the binary operation defined in Definition 1.2.48 forms a group G.*

Proof. Let $g = (g_1, \ldots, g_n), h = (h_1, \ldots, h_n), k = (k_1, \ldots, k_n) \in G$.

$$g(hk) = (g_1, g_2, \ldots, g_n)[(h_1, h_2, \ldots, h_n)(k_1, k_2, \ldots, k_n)] =$$

$$= (g_1, g_2, \ldots, g_n)(h_1k_1, \ldots, h_nk_n) = (g_1h_1k_1, \ldots, g_nh_nk_n) =$$

$$(g_1h_1, \ldots, g_nh_n)(k_1, \ldots, k_n) = [(g_1, \ldots, g_n)(h_1, \ldots, h_n)](k_1, \ldots, k_n) =$$

Consider the element $e = (id_1, \ldots, id_n) \in G$ and let $g = (g_1, \ldots, g_n) \in G$.

$$eg = (id_1, id_2, \ldots, id_n)(g_1, g_2, \ldots, g_n) =$$

$$= (id_1g_1, \ldots, id_ng_n) = (g_1, \ldots, g_n) = g$$

Hence, e is the identity of G.

Let $g = (g_1, \ldots, g_n) \in G$ and consider the element $l = (g_1^{-1}, \ldots, g_n^{-1}) \in G$.

$$gl = (g_1, g_2, \ldots, g_n)(g_1^{-1}, g_2^{-1}, \ldots, g_n^{-1}) =$$

$$= (g_1g_1^{-1}, \ldots, g_ng_n^{-1}) = (id_1, \ldots, id_n) = id$$

Since g is an arbitrary element in G, every element in G has an inverse. Hence, G is a group. □

Proposition 1.2.50. *The subgroup, G_i', of $G = G_1 \times G_2 \times \ldots \times G_n$ consisting of the elements $(id_1, \ldots, id_{i-1}, g_i, id_{i+1}, \ldots, id_n)$ is an isomorphic copy of G_i. This subgroup is normal.*

Proof. This is a subgroup because if $g_1', g_2' \in G_i'$ then

$$(id_1, \ldots, g_1', \ldots, id_n)(id_1, \ldots, g_2', \ldots, id_n) = (id_1, \ldots, g_1'g_2', \ldots, id_n) \in G_i'$$

and

$$(id_1, \ldots, g', \ldots, id_n)(id_1, \ldots, g'^{-1}, \ldots, id_n) = (id_1, \ldots, id_i, \ldots, id_n).$$

We now define a function $\phi : G_i \to G_i'$ by $\phi(g) = (id_1, \ldots, g, \ldots, id_n)$. That ϕ is an isomorphism is obvious.

Let $g \in G$ and $g' \in G_i'$.

$$gg'g^{-1} = (g_1, \ldots, g_i, \ldots, g_n)(id_1, \ldots, g', \ldots, id_n)(g_1^{-1}, \ldots, g_i^{-1}, \ldots, g_n^{-1}) =$$

$$= (id_1, \ldots, g_i g' g_i^{-1}, \ldots, id_n).$$

This is again an element of G_i' which shows that G_i' is an normal subgroup of G. □

Proposition 1.2.51. *The cardinality, $|G|$, of $G = G_1 \times G_2 \times \ldots G_n$ is equal to $|G_1||G_2| \ldots |G_n|$.*

Proof. Each element $g \in G$ is an n-tuple of the form $(g_1, g_2, \ldots, g_n)$ where $g_i \in G_i$. We may choose g_1 in $|G_1|$ ways, g_2 in $|G_2|$ ways and so on. Each of these choises are independent. Hence, $|G| = |G_1||G_2| \ldots |G_n|$. □

Note that, by the above proposition, the quotient group $G_1 \times \ldots \times G_n / G_i$ makes sense. Quite naturally the quotient group $G_1 \times \ldots \times G_n / G_i$ is isomorphic to the group $G_1 \times \ldots \times G_{i-1} \times G_{i+1} \times \ldots \times G_n$ (note the striking resemblance to multiplication and division of numbers).

One of the reasons for introducing the notions of quotient groups and direct products of groups is the prospect of decomposing large and seemingly complex groups into simpler parts (the factor groups of a product) or to unravel hidden similarities of the elements of a group through the equivalence classes in a quotient group. However, both concepts either require normality of the subgroup (in the case of quotient groups) or impose normality on the subgroup (in the case of direct products of groups). This is a quite strong requirement that in general prevents us from decomposing a group into a product. We therefore wish to extend the concept of products of groups.

Proposition 1.2.52. *Let N and H be groups and let $\varphi : H \to Aut(N)$ be a homomorphism where $\varphi(h)$ is denoted φ_h. The set $S = \{(n, h) | n \in N, h \in H\}$ with the operation $(n, h) * (n', h') = (n \cdot \varphi_h(n'), h \cdot h')$ is a group. This group is called a **semidirect product** of N and H and is denoted $N \rtimes_\varphi H$.*

Proof. Since $\varphi_h \in Aut(N)$ for all $h \in H$ the product $n \cdot \varphi_h(n') \in N$ so $*$ is a binary operation on S. We may therefore proceed to verify the group axioms.

(1) Associativity holds because:

$$(n, h) * ((n', h') * (n'', h'')) = (n, h) * (n' \cdot \varphi_{h'}(n''), h' \cdot h'') =$$

$$= (n \cdot \varphi_h(n' \cdot \varphi_{h'}(n'')), h \cdot h' \cdot h'') = (n \cdot \varphi_h(n') \cdot \varphi_h(\varphi_{h'}(n'')), h \cdot h' \cdot h'') =$$

$$= (n \cdot \varphi_h(n') \cdot \varphi_{h \cdot h'}(n''), h \cdot h' \cdot h'')) = (n \cdot \varphi_h(n'), h \cdot h') * (n'', h'') =$$

$$= ((n,h) * (n',h')) * (n'',h'').$$

$(\varphi(h)(\varphi(h')(n'')) = \varphi(h \cdot h')(n'')$ follows from the fact that $\varphi \in Aut(N)$ and hence is a homomorphism).

(2) The identity is (id_n, id_h) since:

$$(id_n, id_h) * (n,h) = (id_n \cdot \varphi(id_h)(n), id_h \cdot h),$$

and

$$(n,h) * (id_n, id_h) = (n \cdot \varphi_h(id_n), h \cdot id_h).$$

Since φ is a homomorphism we know that $\varphi id_h = id_{Aut(N)}$ and $id_{Aut(N)}(n) = n$ so $(id_n, id_h) * (n,h) = (n,h)$. Further, φ_h is also a homomorphism so $\varphi_h(id_n) = id_n$ which shows that $(n,h) * (id_n, id_h) = (n,h)$.

(3) The inverse of the element (n,h) is $(\varphi_{h^{-1}}(n^{-1}), h^{-1})$ since:

$$(n,h) * (\varphi_{h^{-1}}(n^{-1})) = (n \cdot \varphi_h(\varphi_{h^{-1}}(n^{-1})), h \cdot h^{-1}) =$$

$$= (n \cdot \varphi_{h \cdot h^{-1}}(n^{-1})), id_h) = (n \cdot id_{Aut(N)}(n^{-1})), id_h) =$$

$$= (n \cdot n^{-1}, id_h) = (id_n, id_h).$$

and

$$(\varphi_{h^{-1}}(n^{-1}), h^{-1}) * (n,h) = (\varphi_{h^{-1}}(n^{-1}) \cdot \varphi_{h^{-1}}(n), h^{-1} \cdot h) =$$

$$(\varphi_{h^{-1}}(n^{-1} \cdot n), id_h) = (\varphi_{h^{-1}}(id_n), id_h) = (id_n, id_h).$$

□

Proposition 1.2.53. *The cardinality of $N \ltimes_\varphi H$ is $|N||H|$.*

Proof. The proof is completely the same as for direct products. □

One may note that if $\varphi_h = id_{Aut(N)}$ for all $h \in H$ then $N \ltimes_\varphi H$ is just $N \times H$.

1.3 The Cube Group

Rubik's Cube is a three dimensional mechanical puzzle. The goal of the puzzle is to rotate the faces of the cube in a sequence such that at the end of the sequence each face is coloured in a single, distinct colour.

When discussing the cube it is convenient to have some terminology. The cube consists of 26 smaller cubes which we will refer to as **cubies**. The cubies are grouped in sets of 8 or 9 that can be rotated together. These sets will be refered to as **layers**. Each face of the cube consists of nine small, coloured squares. We will refer to these squares as **facets**.

Instead of referring to the faces of the cube by their colours we choose to fix the cube in space, with one face facing us, and call that side **the front face**. The other sides are then called the **back face, up face, down face, right face** and **left face**. A 90° clockwise rotation, as seen from the face, of the front face is denoted by F. Rotations of the other faces are similarly denoted B, U, D, R and L as seen from the respective faces. A 90° counter-clockwise rotation will be denoted by a -1 superscript. For instance, a 90° counter-clockwise rotation of the front face is denoted F^{-1}.

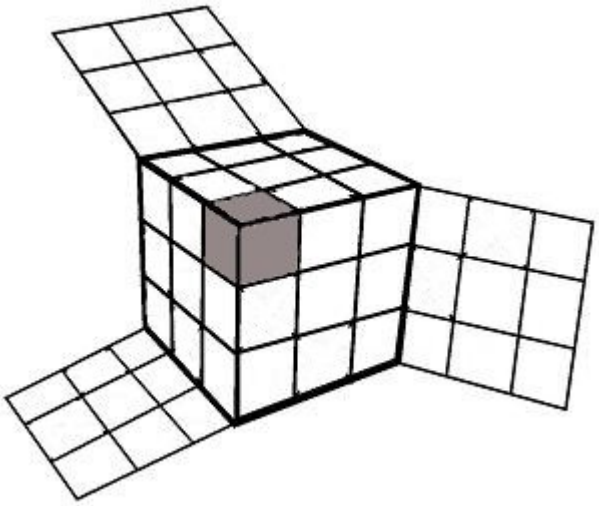


Figure 1.1: A cubie of the Cube

Remark 1.3.1. One might think that rotations of the center layers are also useful to define. These are however superfluous, as each rotation of a center layer is equivalent to rotating the two adjacent face layers.

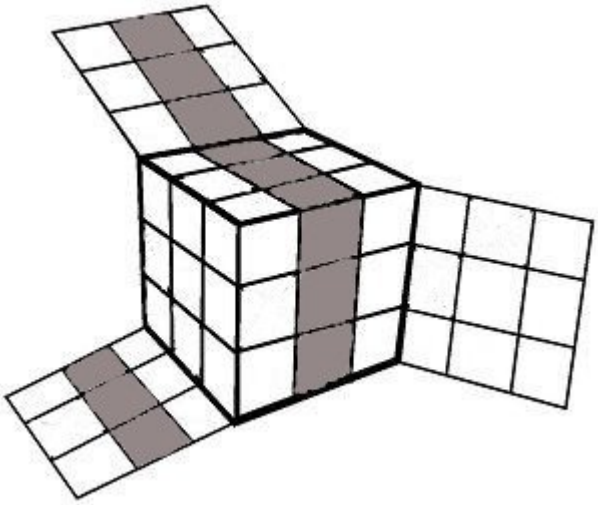


Figure 1.2: A layer of the Cube.

Remark 1.3.2. The relative configuration of the center facets of each face cannot be altered by any rotation of the layers.

1.3.1 The free group

A natural way to start when one wants to determine the group structure of Rubik's Cube is to consider a free group consisting of the concatenations of rotations of the faces of the cube.

Definition 1.3.3. We define the **concatenation operator** of two rotations by saying that AB denotes the sequence of rotations of first rotating B then A.

We can form sequences of rotations of arbitrary length with the concatenation operator.

A natural way to define a group is to consider sequences of the above rotations. Such sequences will correspond to scrambling the Cube, (or solving it). In order to form a group, we also have to introduce the concept of reducing sequences.

Definition 1.3.4. If $x = a_1 a_2 \dots a_n$ is a sequence of rotations the corresponding reduced sequence $\hat{x}$ is the sequence obtained from x by removing all partial sequences of two elements where an element is adjacent to its inverse.

Proposition 1.3.5. *The set S consisting of all finite, reduced sequences of rotations R, L, U, D, F, B and inverses $R^{-1}, L^{-1}, U^{-1}, D^{-1}, F^{-1}, B^{-1}$ is a group under the operation of concatenation. We denote this group by $\mathfrak{G}_R$ (read "frac-G-R") and call it the free Rubik's Group.*

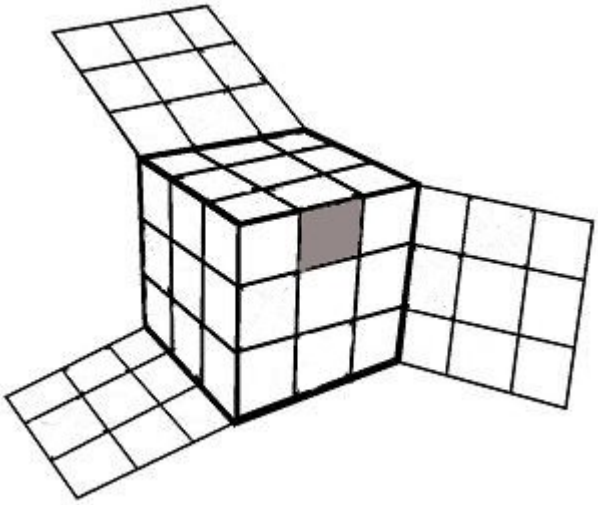


Figure 1.3: A facet of the Cube.

Proof. We check the group axioms.
1. Associativity: $\forall a, b, c \in \mathfrak{G}_R, a(bc) = (ab)c$ by the definition of the concatenation operator.
2. Identity: The empty sequence $\emptyset$ is the identity element, since $\forall x \in \mathfrak{G}_R, \emptyset x = x\emptyset = x$.
3. Inverse: Let $x = a_1 a_2 \dots a_n$ be an element of $\mathfrak{G}_R$. Then $x^{-1} = a_n^{-1} \dots a_2^{-1} a_1^{-1}$ since $xx^{-1} = x^{-1}x = \emptyset$. □

We note that this defines a group of infinite order. This is because it describes the rotations of the faces of the cube and not the scrambled state, or permutations, of the facets. The latter is however what we are most interested in and we therefore want $\mathfrak{G}_R$ to act on the set of facets of the cube.

We note that we have a total of 54 facets of the standard cube, since each face has nine facets, and there are a total of six faces. We can thus give each facet a unique index from 1 to 54 such as the one seen in Figure 1.4.

Definition 1.3.6. Given an indexation such as the one in Figure 1.4, we can define a group action $\phi : \mathfrak{G}_R \times [54] \to [54]$[1] by $\phi(g, x) = y, g \in \mathfrak{G}_R, x \in [54]$ where $y \in [54]$ is the index of the facet that x is brought to by the sequence g.

Note that by Proposition 1.2.38 the above group action defines a homomorphism from $\mathfrak{G}_R$ to S_{54}. However, S_{54} is rather cumbersome to work with,

[1] [54] is the set of all natural numbers 1 to 54

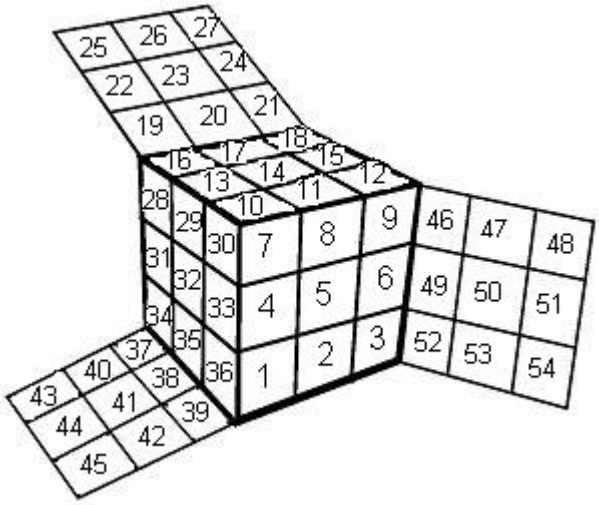


Figure 1.4: Each facet of the cube given a number $1, \ldots, 54$.

so a simplification of the current situation is desirable. We also note that the group obtained from this group action is only a subgroup of S_{54}, which will be seen below.

1.3.2 Positions of edge pieces and corner pieces

Consider the set of edge pieces, E, and the set of corner pieces, C, of the cube. We see that each sequence of rotations will map corner pieces to corner pieces, and edge pieces to edge pieces. Hence, all facet permutations of S_{54} are not allowed, since one cannot map a corner facet to an edge facet.

With this in mind, we can assign each edge piece an index between 1 and 12, and each corner piece an index between 1 and 8, i.e. $E = \{e_1, e_2, e_3 \ldots, e_{12}\}$, $C = \{c_1, c_2, \ldots, c_8\}$ as seen in Figure 1.5.

We let $\mathfrak{G}_R$ act on E by

$$g.x = y,\ g \in \mathfrak{G}_R,\ x \in E$$

where y is the index of the edge position that x is brought to by g. We may also let $\mathfrak{G}_R$ act on C by

$$g.x = y, g \in \mathfrak{G}_R, x \in C$$

where y is the index of the corner position that x is brought to by g. We thus obtain two homomorphisms, $\phi_E : \mathfrak{G}_R \to S_{12}$ and $\phi_C : \mathfrak{G}_R \to S_8$.

Given the indexation shown in Figure 1.5 the rotations generating $\mathfrak{G}_R$ are mapped to the following permutations in S_8 and S_{12}, respectively:

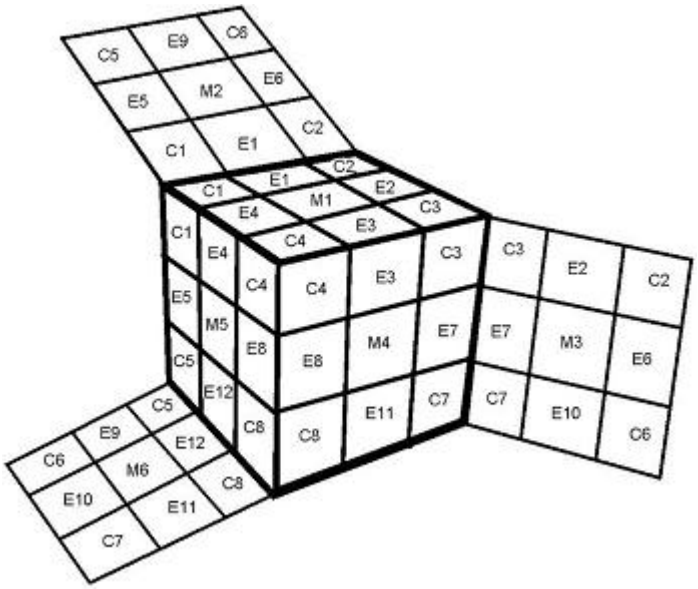


Figure 1.5: Each corner given a number $1, \ldots, 8$ and each edge given a number $1, \ldots, 12$.

$$S_8 : \begin{array}{ll} \phi_C(U) = (c_1c_2c_3c_4); & \phi_C(D) = (c_5c_8c_7c_6) \\ \phi_C(F) = (c_1c_4c_8c_5); & \phi_C(B) = (c_3c_2c_6c_7) \\ \phi_C(R) = (c_3c_7c_8c_4); & \phi_C(L) = (c_1c_5c_6c_2) \end{array}$$

$$S_{12} : \begin{array}{ll} \phi_E(U) = (e_1e_2e_3e_4); & \phi_E(D) = (e_9e_{12}e_{11}e_{10}) \\ \phi_E(F) = (e_4e_8e_{12}e_5); & \phi_E(B) = (e_2e_6e_{10}e_7) \\ \phi_E(R) = (e_3e_7e_{11}e_8); & \phi_E(L) = (e_1e_5e_9e_6) \end{array}$$

Remark 1.3.7. It's worth stressing that the edge pieces have two orientations, and the corner pieces have three, due to the fact that they consist of two and three facets, respectively. This observation is not contained in the description of the positions of the edges and corners, thereby making it incomplete for describing the different states of the cube. We will complete our description later in the text.

Theorem 1.3.8. *ϕ_C and ϕ_E are surjective mappings.*

Proof. We have to find a transposition of two adjacent corners in C. By the symmetry of the cube it follows that if we can transpose one pair of adjacent corners then we can transpose all pairs of adjacent corners. This will thus complete the proof for C, since any permutation thereof can be written as a product of transpositions of adjacent corners, since if $a, b, c \in C$ and a, b are adjacent and b, c are adjacent, then $(ab)(cb)(ab) = (ac)$. Further, if d is adjacent to c then $(ac)(cd)(ac) = (ad)$. A corner cannot possibly have more than two corners between itself and any other corner so this covers all cases.

But $\phi_C((LBU)^5) = ((c_1c_5c_6c_2)(c_3c_2c_6c_7)(c_1c_2c_3c_4))^5 = ((c_1c_2)(c_3c_4c_5c_6c_7))^5 = (c_1c_2)$, hence ϕ_C is surjective.

By the same reasoning, it is sufficient to find a transposition of two adjacent edge pieces in E. Consider:

$$\phi_E(UR^3U^3B^3UBR)$$

$$= (e_1e_2e_3e_4)(e_3e_8e_{11}e_7)(e_1e_4e_3e_2)(e_2e_7e_{10}e_6)(e_1e_2e_3e_4)(e_2e_6e_{10}e_7)(e_3e_7e_{11}e_8)$$

$$= (e_1e_4)$$

so both ϕ_C and ϕ_E are surjective. □

Remark 1.3.9. We note that, by Theorem 1.3.8, $Im(\phi_E) \cong S_{12}$, and $Im(\phi_C) \cong S_8$.

But ϕ_C and ϕ_E only consider the positions of corner pieces and edge pieces independent of each other. In order to determine the full structure, we need to consider the positions of corner pieces and edge pieces simultaneously.

Definition 1.3.10. We define $\phi_{C,E} : \mathfrak{G}_R \to S_8 \times S_{12}$ as $\phi_{C,E}(X) = (\phi_C(X), \phi_E(X))$.

Proposition 1.3.11. *$\phi_{C,E}$ is a homomorphism.*

Proof. This follows immediately from the fact that ϕ_C and ϕ_E are homomorphisms. □

One might think that $\phi_{C,E}$ is surjective since ϕ_C and ϕ_E are surjective. This is however not the case, as the following theorem shows.

Theorem 1.3.12. *$\phi_{C,E}$ is not surjective.*

Proof. Note that $\mathfrak{G}_R$ is generated by $S_{gen} = \{F, B, U, D, R, L\}$. For each generator $X \in S_{gen}$ $\phi_{C,E}(X) = (\phi_C(X), \phi_E(X))$ where both $\phi_C(X)$ and $\phi_E(X)$ are 4-cycles, i.e. $\phi_C(X)$ and $\phi_E(X)$ are both odd permutations. It follows from the fact that $\phi_{C,E}$ is a homomorphism that if $\phi_{C,E}(Y) = (\phi_C(Y), \phi_E(Y))$ is the image of an element $Y \in \mathfrak{G}_R$ then $\phi_C(Y)$ and $\phi_E(Y)$ are both odd or both even. $S_8 \times S_{12}$ contains elements (σ, π) where σ is odd and π is even (and the other way around). These elements are clearly not in the image of $\phi_{C,E}$. Hence, $\phi_{C,E}$ is not surjective. □

A natural question would be if all pairs of an even corner permutation and an even edge permutation can be achieved (and the analogue for odd permutations).

Lemma 1.3.13. *All pairs (σ_C, σ_E), $\sigma_C \in S_8, \sigma_E \in S_{12}$, where σ_C and σ_E are both even or both odd, lie in the image of $\phi_{C,E}$.*

Proof. Consider the set of all pairs, $(\sigma_C, \sigma_E) \in Im(\phi_{C,E})$, where both σ_C and σ_E are even. Given such an element, (σ'_C, σ'_E), we know that σ'_E is an even permutation in S_{12} and there are elements in $Im(\phi_{C,E})$ that fixes the edges while permuting three of the corners cyclically. Such an element is

$$\phi_{C,E}(FRF^{-1}LFR^{-1}F^{-1}L^{-1}) =$$

$$((c_1c_4c_8c_5)(c_3c_7c_8c_4)(c_1c_5c_8c_4)(c_1c_5c_6c_2)$$

$$(c_1c_4c_8c_5)(c_3c_4c_8c_7)(c_1c_5c_8c_4)(c_1c_2c_6c_5),$$

$$(e_4e_8e_{12}e_5)(e_3e_7e_{11}e_8)(e_4e_5e_{12}e_8)(e_1e_5e_9e_6)$$

$$(e_4e_8e_{12}e_5)(e_3e_8e_{11}e_7)(e_4e_5e_{12}e_8)(e_1e_6e_9e_5)) =$$

$$= ((c_1)(c_2)(c_3)(c_4)(c_5c_8c_6)(c_7), id) = ((c_5c_8c_6), id)$$

By the symmetry of the cube, every 3-cycle such that all three corners lie in the same face is an element of the image of $\phi_{C,E}$. From Theorem 1.2.24 we know that these cycles will generate A_8, and thus every even permutation of the corners lies in the image of $\phi_{C,E}$. But σ'_E is an arbitrary permutation in A_{12} and hence, every combination (σ_C, σ_E) such that both σ_C and σ_E are even lies in $Im(\phi_{C,E})$.

Now consider the pairs $(\sigma_C, \sigma_E) \in \phi_{C,E}$ such that both σ_C and σ_E are odd. Consider an odd element $\sigma''_E \in S_{12}$. This element will be paired with an odd element $\sigma''_C \in S_8$. σ_C is a representative of a coset of A_8. Hence we have, by the same reasoning as in the previous case, that all odd permutations of S_8 can be paired with σ''_E, and since σ''_E is an arbitrary element every pair (σ_C, σ_E) such that both σ_C and σ_E are odd lies in the image of $\phi_{C,E}$. This completes the proof. □

1.3.3 Orientation of edge pieces and corner pieces

Until now we have considered the positioning of the corners and edges. There is however no guarantee that the cube is solved even though all edges and corners are in their correct positions. This is because they may be "flipped". Therefore, as mentioned earlier, we also need to consider the orientation of the pieces to completely determine the structure of the cube group, and in particular the cardinality of the group.

In its correct position each edge piece can be flipped in two ways and each corner piece in three ways. However, we want to define the orientation of the pieces in such a way that it is possible to determine the orientation of a piece independently of whether it is in its correct position or not.

Definition 1.3.14. Consider a cube in its solved state on which a cross has been drawn on precisely one side of each edge and corner piece. These crosses determine the **map of the orientations** of the positions of the cube (see Figure 1.6 and Figure 1.7). An edge piece in an unsolved cube is said to

be correctly oriented if its cross coincides with the cross of that position in the orientation map, and incorrectly oriented otherwise. Similarly, a corner piece in an unsolved cube is said to be correctly oriented if its cross coincides with the cross of that position in the orientation map, if it is rotated 120° clockwise it is said to have incorrect orientation of the first type and if it is rotated 120° anti-clockwise it is said to have incorrect orientation of the second type.

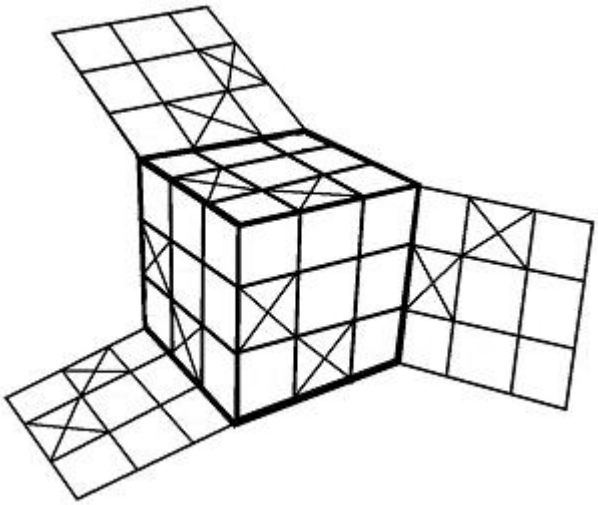


Figure 1.6: Orientations of the edges.

We may represent the orientation of the edges of the cube by a 12-tuple of zeros and ones where each coordinate represents an edge position. A coordinate is 0 if the edge piece in that position is correctly oriented and 1 otherwise. Similarly, the orientation of the corners can be represented by an 8-tuple of zeros, ones and twos where each coordinate represents a corner position. A coordinate is 0 if the corner piece in that position is correct, 1 if it is of incorrect orientation of the first type and 2 if it is of incorrect orientation of the second type.

Now consider how the orientations of the edges change when we perform a rotation of a single face, $X := \pi = (x_1x_2x_3x_4) \in S_{12}$. Before performing X we have performed some sequence Y that has permuted the edges to the state described by $\sigma \in S_{12}$ and changed the orientations to the state described by the 12-tuple $(\epsilon_1, \ldots, \epsilon_{12}), \epsilon_i \in \{0, 1\}$. If we perform X on a solved cube the change of orientations will be represented by the 12-tuple $(\omega_1, \ldots, \omega_{12})$. We now perform X on a cube with orientations $\epsilon = (\epsilon_1, \ldots, \epsilon_{12})$ and thus obtain

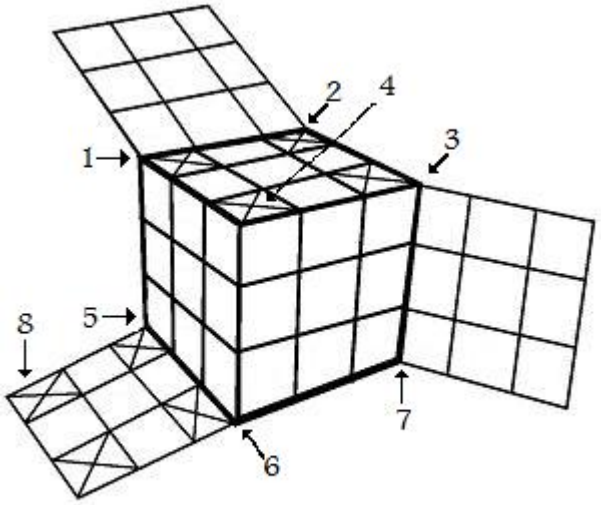


Figure 1.7: Orientations of the corners.

a representation for the orientations of the final state, $(\omega'_1, \ldots, \omega'_{12})$. We note that $\omega'_i = \omega_i$ whenever $\epsilon_{x_{i-1}} = 0$ ($\epsilon_{x_{1-1}} = \epsilon_{x_4}$) and that $\omega'_i = \omega_i + 1(mod 2)$ if $\epsilon_{x_{i-1}} = 1$ (if $\epsilon_{i-1} = 0$ there will be no difference to the case of performing X on a solved cube and if $\epsilon_{i-1} = 1$ the final state will be completely opposite to a solved cube. We note that this can be stated as

$$(\omega'_1, ..., \omega'_{12}) = (\epsilon_1, ..., \underbrace{\epsilon_{x_4}}_{\text{pos } x_1}, ..., \underbrace{\epsilon_{x_1}}_{\text{pos } x_2}, ..., \underbrace{\epsilon_{x_2}}_{\text{pos } x_3}, ..., \underbrace{\epsilon_{x_3}}_{\text{pos } x_4}, ..., \epsilon_{12}) + (\omega_1, ..., \omega_{12})$$

where the sum is reduced $mod 2$. We see that π^{-1} has permuted the indices of ϵ.

We now try to generalise the discussion above. Therefore let X be a finite sequence of rotations that permutes the edges of a solved cube in a way described by $\pi \in S_{12}$ and changes the orientations in a way described by the 12-tuple ω. We perform X on a solved cube after first performing a sequence Y that permutes the faces of a solved cube in way described by σ and the orientations in a way described by ϵ. Let the orientations after applying XY be described by ω'. We again see that $\omega'_i = \omega_i$ precisely if $\epsilon_{i-1} = 0$ and $\omega'_i = \omega_i + 1(mod 2)$ precisely if $\epsilon_{i-1} = 1$. This observation can be summarised

$$\omega' = \omega + \pi.\epsilon$$

where π acts by permuting the indices of ϵ according to π^{-1} and the sum is reduced $mod 2$. We have thus shown that the positions and orientations of the edges, and how they change, are described by (some subgroup of) the

group

$$S_{12} \ltimes_\varphi \left(\underbrace{Z_2 \times \ldots \times Z_2}_{12 \text{ times}} \right) = S_{12} \ltimes_\varphi Z_2^{12}$$

where $(\pi, \omega) *_\varphi (\sigma, \epsilon) = (\pi\sigma, \omega + \varphi_\pi(\epsilon))$, where $\varphi_\pi(\epsilon)$ is the element of Z_2^{12} obtained from ϵ by permuting its indices according to π^{-1}.

We now want to do something similar with the orientations of the corners. Therefore let X be a finite sequence of rotations that permutes the corners of a solved cube in a way described by $\pi \in S_8$ and changes the orientations in a way described by the 8-tuple $\omega = (\omega_1, \ldots, \omega_8), \omega_i \in \{0, 1, 2\}$. We perform X on a solved cube after first performing the sequence Y that permutes the corners in a way described by σ and changes the orientations in a way described by $\epsilon = (\epsilon_1, \ldots, \epsilon_8)$, $\epsilon_i \in \{0, 1, 2\}$. Let the orientations after applying XY be described by ω'. We see that $\omega'_i = \omega_i$ precisely if $\epsilon_{i-1} = 0$ $(\epsilon_{1-1} = \epsilon_8)$, $\omega'_i = \omega_i + 1 (mod 3)$ precisely if $\epsilon_{i-1} = 1$ and $\omega'_i = \omega_i + 2 (mod 3)$ precisely if $\epsilon_{i-1} = 2$. This observation may be summarised

$$\omega' = \omega + \pi.\epsilon$$

where π acts on ϵ by permuting the indices according to π^{-1} and the sum is reduced modulo 3. We have thus shown that the positions and orientations of the edges and how they change are described by (some subgroup of) the group

$$S_8 \ltimes_\varphi \left(\underbrace{Z_3 \times Z_3}_{8 \text{ times}} \right) = S_8 \ltimes_\varphi Z_3^8$$

where $(\pi, \omega) *_\varphi (\sigma, \epsilon) = (\pi\sigma, \omega + \varphi_\pi(\epsilon))$, where $\varphi_\pi(\epsilon)$ is the element of Z_3^8 obtained from ϵ by permuting its indices according to π^{-1}. From the discussion above, we may now define a binary operator on the set describing the positions and orientations of edge and corner pieces respectively.

Definition 1.3.15. Let s_1 and s_2 be two scramblings of the cube and let them be described by the following 4-tuples:

$$s_1 = (\pi_C, o_C, \pi_E, o_E) : \pi_C \in S_8, o_C \in Z_3^8, \pi_E \in S_{12}, o_E \in Z_2^{12}$$
$$s_2 = (\pi'_C, o'_C, \pi'_E, o'_E) : \pi'_C \in S_8, o'_C \in Z_3^8, \pi'_E \in S_{12}, o'_E \in Z_2^{12}$$

The first element describes the position of the corner pieces, the second the orientation of the corner pieces, the third element descibes the position of the edge pieces and the fourth the orientation of the edge pieces. A binary operator on the set of scramblings, $\cdot$, is defined as follows:

$$s_1 \cdot s_2 = (\pi_C \pi'_C, o_C + \pi_C.o'_C, \pi_E \pi'_E, o_E + \pi_E.o'_E).$$

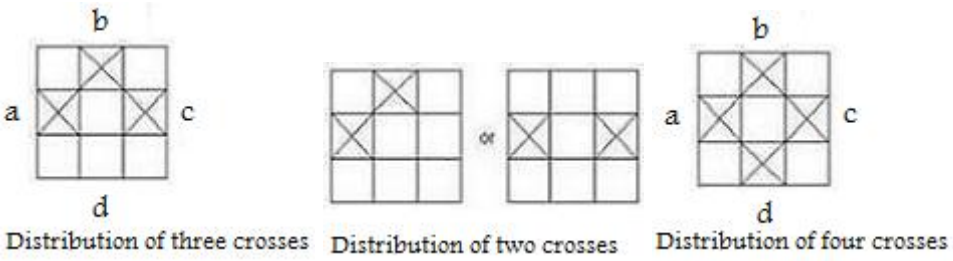


Figure 1.8: How to distribute crosses on one side

Different placements of the edge crosses will yield different 12-tuples for the generators. However, the following is true for any choice of placement of the crosses.

Lemma 1.3.16. *Regardless of placement of the crosses on the edges of the solved cube, the sum of the elements of the* 12*-tuples representing the edge orientation of the generators will always be a multiple of* 2*.*

Proof. We start by noting two things. Firstly, a generator will only change the orientation of edge pieces lying in that particular face. Secondly, there are only four different ways in which one can arrange the crosses of the edge pieces in a particular face without getting equivalent results. These four configurations are shown in figure 1.8. Denote the edge pieces of the particular face by a, b, c, d according to figure 1.8 and let the tuple (o_a, o_b, o_c, o_d) denote the part of the 12-tuple that represents the orientation of the particular edges. Now consider the different cross configurations and let $G = (o_a, o_b, o_c, o_d)$ be the effect of the generator rotating the considered face.

(1): $G = (0, 0, 0, 0)$
(2): $G = (1, 0, 0, 1)$
(3): $G = (0, 1, 0, 1)$
(4): $G = (1, 1, 1, 1)$

Since the rest of the edges will be unchanged, the rest of the 12-tuples will be filled with zeros. Thus, the sum of the change of orientations of the edge pieces induced by a generator will be a multiple of 2. This completes the proof. □

Proposition 1.3.17. *The sum of the orientations of the edges is a multiple of* 2*.*

Proof. Let $\sum \epsilon_i$ denote the sum of all elements of the tuple ϵ. The proof will use induction over the number of rotations of the cube. Firstly, consider the edges of a cube in the solved state, $(id, 0) \in S_{12} \rtimes Z_2^{12}$. The rotation of one side is given by (σ_G, ϵ_G) where G denotes generator. The new state of the cube is given by:

$$(\sigma_G, \epsilon_G) * (id, 0) = (\sigma_G id, \epsilon_G + \sigma_G.0) = (\sigma_G, \epsilon_G)$$

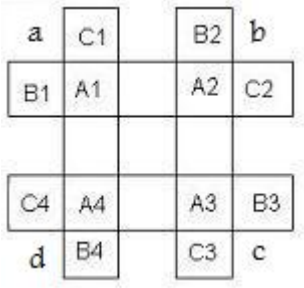


Figure 1.9: Sketch to help explain cross distribution on the corners of one side

Since the sum of all elements of the 12-tuple, $\sum(\epsilon_G)_i$, is a multiple of 2 for all the generators, we know that after one rotation $\sum(\epsilon_G)_i = 0(mod2)$. Let ϵ_n denote the edge orientation after n rotations. Assume that $\sum(\epsilon_n)_i = 0(mod2)$. Now consider the edges of the cube after $n+1$ rotations. These are given by:

$$(\sigma_G, \epsilon_G) * (\sigma_n, \epsilon_n) = (\sigma_G\sigma_n, \epsilon_G + \sigma_G.\epsilon_n)$$

for some generator G. Consider the element describing the edge orientation;

$$\epsilon_G + \sigma_G.\epsilon_n$$

We know that $\sum(\epsilon_G)_i = 0(mod2)$ for all generators and $\sum(\epsilon_n)_i = 0(mod2)$ by assumption. We note that the permutation of the elements in ϵ_n does not change $\sum(\epsilon_n)_i$. Thus;

$$\sum(\epsilon_G + \sigma_G.\epsilon_n)_i = \sum(\epsilon_G + \epsilon_n)_i = \sum(\epsilon_G)_i + \sum(\epsilon_n)_i = 0(mod2)$$

By induction we now know that $\sum(\epsilon)_i = 0(mod2)$ for any configuration of the cube. This completes the proof. □

We now want to do something similar for the corner pieces. We note that different placements of the corner crosses will yield different 8-tuples for the generators. However, the following is true for any choice of placement of the crosses.

Lemma 1.3.18. *Regardless of placement of the crosses on the corners of the solved cube, the sum of the elements of the 8-tuples representing the corner orientation of the generators will always be a multiple of 3.*

Proof. We note two things. Firstly, the generators will only change orientation of the corner pieces lying in that particular face. It is therefore enough to consider the four elements corresponding to the four corners of the face of the 8-tuple describing the orientations of the corners when stating how the

generators will change the orientation of the corner pieces. Secondly, there are only seven different ways in which one can put crosses on the corners of one face without obtaining equivalent configurations. These configurations are (with notation used in figure 1.9):

(1): Crosses on $A1, A2, A3, A4$
(2): Crosses on $A1, A2, A3, B4$
(3): Crosses on $A1, A2, A3, C4$
(4): Crosses on $A1, A2, B3, B4$
(5): Crosses on $A1, A2, B3, C4$
(6): Crosses on $A1, B2, A3, B4$
(7): Crosses on $A1, B2, A3, C4$

Let $G = (o_a, o_b, o_c, o_d)$ denote the 4-tuple corresponding to the four considered corners, with a, b, c, d given by figure 1.9. The seven cross configurations give the following 4-tuples for the generators:

(1): $G = (0, 0, 0, 0)$
(2): $G = (1, 0, 0, 2)$
(3): $G = (2, 0, 0, 1)$
(4): $G = (1, 0, 2, 0)$
(5): $G = (2, 0, 2, 2)$
(6): $G = (2, 1, 2, 1)$
(7): $G = (2, 2, 1, 1)$

The remaining corner pieces will not change their orientation and thus, the rest of the 8-tuple will consist of zeros. Hence, the change of orientation of the corner pieces induced by a generator will always be a multiple of 3. This completes the proof. □

Proposition 1.3.19. *The sum of the orientations of the corners is a multiple of* 3.

Proof. Let $\sum \epsilon_i$ denote the sum of all elements of the tuple ϵ. This proof will use induction over the number of rotations of the cube. Firstly, consider the corners of a solved cube, $(id, 0) \in S_8 \rtimes Z_3^8$. A generator is given by the element (σ_G, ϵ_G) where G denotes generator. Thus, the element obtained after one rotation is:

$$(\sigma_G, \epsilon_G) * (id, 0) = (\sigma_G id, \epsilon_G + \sigma_G.0) = (\sigma_G, \epsilon_G)$$

We know that $\sum(\epsilon_G)_i = 0(mod 3)$ for all generators. Therefore the sum of the orientations of the corners is a multiple of 3 after one rotation. Let (σ_n, ϵ_n) describe the corners after n rotations. Assume that $\sum(\epsilon_n)_i = 0(mod 3)$. Now consider the element describing the corners after $n+1$ rotations. It is given by:

$$(\sigma_G, \epsilon_G) * (\sigma_n, \epsilon_n) = (\sigma_g \sigma_n, \epsilon_G + \sigma_G.\epsilon_n)$$

for some generator G. Consider the element describing the corner orientation. We know that $\sum(\epsilon_G)_i = 0(mod 3)$ since this holds for all generators.

We also know that $\sum(\epsilon_n)_i = 0(mod3)$ by assumption. We note that the permutation of the elements of ϵ_n does not change the sum of the elements. Thus;

$$\sum(\epsilon_G + \sigma_G.\epsilon_n)_i = \sum(\epsilon_G + \epsilon_n)_i = \sum(\epsilon_G)_i + \sum(\epsilon_n)_i = 0(mod3)$$

By induction, we have $\sum \epsilon_i = 0(mod3)$ for any number of rotations of the cube. This completes the proof. □

Remark 1.3.20. Note that this gives restrictions regarding how one could orient the corners and edges. For example if one knows the orientations of 7 corners or 11 edges the orientation of the last one will be determined since we can't change the orientation of a single corner or edge. This also implies that if one flips two corners, one has to be flipped counterclockwise and the other has to be flipped clockwise. Other interesting properties include the fact that we cannot flip three edges at the same time but we can flip for example three corners in the same direction.

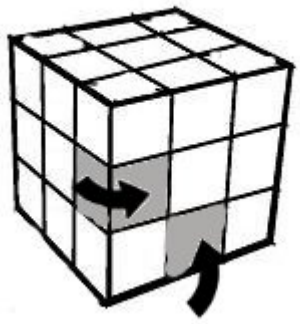


Figure 1.10: Flipping the edges.

Lemma 1.3.21. *The number of ways to orient the edge pieces is* 2^{11}.

Proof. The sequence given by

$$FRUR^{-1}U^{-1}RUR^{-1}F^{-1}L^{-1}ULU^{-1}L^{-1}U^2LF^{-1}U^{-1}FU^{-1}F^{-1}U^2$$

$$FRUR^{-1}URU^2R^{-1}F^{-1}U^{-1}FU^{-1}GF^{-1}U^2F$$

flips two edges according to the figure above without changing the position of the cubies. From symmetry one can deduct that one can obtain corresponding sequences for the rest of the edge pieces. Consider one such flip. By flipping another piece we can construct an independent flip of one of the edges. Continuing in this way, we will get 11 independent flips with two configurations, i.e. 2^{11} elements. But Theorem 1.3.17 states that the number of incorrectly oriented edge pieces is always even, i.e. it is impossible to flip a single edge, thus giving the upper limit $2^{12}/2$ which coincides with the constructed number. Thus, we have obtained all the possible flips. This completes the proof. □

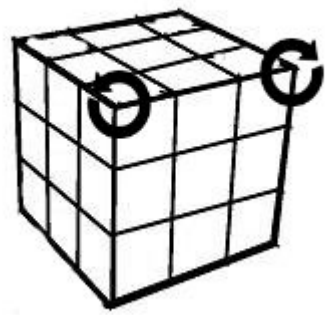


Figure 1.11: Flipping the corners.

Lemma 1.3.22. *The number of ways to orient the corner pieces is* 3^7.

Proof. The sequence given by $LU^2L^{-1}U^{-1}LU^{-1}L^{-1}RU^2RUR^{-1}UR$ gives an orientation change of two corner pieces, where one of them is turned counterclockwise and the other clockwise. By the same argumentation as in the proof of Lemma 1.3.21 one can obtain 7 independent rotations of the 8 corner pieces. This is the maximum number of configurations, since Proposition 1.3.19 states that it is impossible to flip a single corner. □

1.3.4 Rubik's Group and its cardinality

In the previous parts of this section, we have determined the number of possible ways to position corner and edge pieces, the number of ways one can orient corner and edge pieces and also expressed how the rotations of

the faces of the cube affect the positions and orientations of corner and edge pieces. From this, it is now possible to determine the structure of Rubik's Group.

Theorem 1.3.23. *Rubik's Group, G_R, is described by the set*

$$S = \{(\pi_C, o_C, \pi_E, o_E) : \pi_C \in S_8, o_C \in Z_3^8, \pi_E \in S_{12}, o_E \in Z_2^{12},$$
$$sgn(\pi_C) = sgn(\pi_E), \sum_{i=1}^{8}(o_C)_i \equiv 0(3), \sum_{i=1}^{12}(o_E)_i \equiv 0(2)\}$$

and the binary operator $\cdot$ defined by

$$(\pi_C, o_C, \pi_E, o_E) \cdot (\pi'_C, o'_C, \pi'_E, o'_E) = (\pi_C\pi'_C, o_C + \pi_C.o'_C, \pi_E\pi'_E, o_E + \pi_E.o'_E)$$

Proof. From Lemma 1.3.13 we know that the set of permutations describing the positions of the pieces is correct. From Proposition 1.3.17 and Proposition 1.3.19 we know that the set of tuples describing the orientations is correct. From Definition 1.3.15 we know that the binary operator works correctly for Rubik's Cube. This completes the proof. □

In addition to determine the structure of Rubik's Group, we may also determine the cardinality of Rubik's Group.

Theorem 1.3.24. *The cardinality of Rubik's Group, $|G_R|$, is $\frac{1}{2}\frac{1}{2}\frac{1}{3}12!8!2^{12}3^8$.*

Proof. We know from Theorem 1.3.13 that all of the odd/odd and even/even permutations lie in the image of $\phi_{C,E}$. This set has the cardinality $12!8!/2$, and we know from Lemma 1.3.21 and Lemma 1.3.22 that we can obtain 11 edge-orientations independently and 7 corner-orientations independently. Thus, the cardinality must be $\frac{1}{2}\frac{1}{2}\frac{1}{3}12!8!2^{12}3^8$. □

References

The background theory in section 1 has been written with the aid of the following textbooks:

Dummit, David S.; Foote, Richard M., "Abstract Algebra, Third Edition", John Wiley and Sons, 2003

Fraleigh, John B, "A First Course in Abstract Algebra, Seventh Edition", Addison Wesley, 2002

Chapter 2

"Short Sequences of Moves on Rubik's Cube"

by Patrick Masawe

2.1 Introduction

In this report we will show how to calculate the number of different patterns obtained on the Rubik's cube when applying some sequences of moves consisting of 90° and 180° turns on the cube.
The cube has six faces and consists of 26 smaller cubes which we shall continue refer to as **cubies**. As before we shall think of the cube as being fixed in space with one of its faces facing us. We call the face of the cube facing us the **front face** and the other sides are then called **back face**, **up face**, **down face**, **right face** and **left face**. We let F denote a 90° clockwise rotation of the front face when looking at the front face. Similarly, we let B, U, D, R and L denote 90° clockwise rotations of the corresponding faces of the cube when looking at the specific face. In this work we will refer to these moves as **rotations**, for example the move M = FUR consists of three rotations, the first one being R, the second U and the last rotation being F. Every face of the cube has a total of 9 cubies, the cubie at the center is called the **center cubie**, the four cubies at the corners are called **corner cubies** and the rest of the cubies are called **edge cubies**. Occasionally we will call the corner cubies and edge cubies simply corner and edge.
We will use the homomorphisms ϕ_C and ϕ_E developed in section 1.3.2 several times when studying the change of positioning of the cubies in the cube.

Now to some definitions from group theory. If S is a subset of a group G, then S generates a subgroup of G and as before we will denote this subgroup by <S>. The **order of a group G** is the number of elements in G and the **order of an element a of G** is the number of elements in the

cyclic subgroup of G generated by a. We denote the order of G by $|G|$ and the order of an element a of G by $|<a>|$.

So, the question of how many different patterns on the cube it is possible to obtain by the move, say UR, can with the above definitions from group theory be rephrased to, what is the order of UR. In this work we will show that the order of UR is 105 or using the notations above, |<UR>|= 105. Also, we will show that the order of the group generated by the move UU and RR is 12 or shorter, |<UU, RR>|= 12 and in the last chapters we will proove that |<UU, RR, LL>|= 96 and that |<UU, RR. LL, DD>|= 192. We begin by defining a homomorphism that we will use several times throughout this work.

2.1.1 Permutation for the orientations of the cubies

We define a group action $\mu : G \times X \to X$ where G is any subgroup of the Rubik's cube group and X is the set of orientations of one specific cubie. For example, a corner cubie with a total of three faces can be described by $X = \{f_1, f_2, f_3\}$ where the first coordinate is the top face (or down face) and the other two are the faces on both sides, see Figure 2.1. This group action gives rise to a homomorphism $\gamma : G \to S_X$. We will use this homomorphism γ several times when calculating the order of some groups.

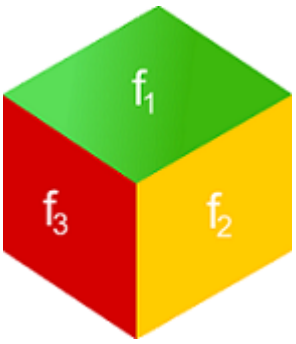


Figure 2.1: A corner cubie with its three faces marked with index f_1, f_2 and f_3.

2.1.2 Cyclic abelian groups

The moves we will be studying in this section are UR, UUR, URR, UUUR and URRR. These moves generate cyclic subgroups of movements on the Rubik's cube. The orders of the cyclic subgroups that they generate are as follows:

| <UR> |= 105
|<UUR>|= |<URR>|= 30
|<UUUR>|= |<URRR>|= 63

The above results can be obtained by just repeating the moves on a Rubik's cube, counting the number of rotations and then observing when the cube goes back to its original state. This can be very tedious, especially when the order of a movement is as large as 105.
There is however a mathematical approach to this problem of finding the order of these cyclic groups where it suffices to look at only a few sequences of moves. But before we begin we will first present a definition and with it an useful lemma.

Definition 2.1.1. Let cubie A and cubie B be two cubies in the cube and let M be any nonidentity move on the cube that brings cubie A and cubie B back to their original positions in the cube. Also, let $p_1, p_2, \ldots, p_n$ be the $n \geq 2$ labels for the positions that cubie A assumes in consecutive order for consecutive rotations in M, where p_1 is the label marking the first position in the cube that cubie A assumes by the first rotation in M and p_2 the label marking the second position in the cube that cubie A assumes by the second rotation in M etc, and lastly, p_n the label marking the original position in the cube that cubie A assumes by the last rotation in M. Note that different labels may mark the same position in the cube.
We will here introduce a new terminology, by saying that a cubie assumes a label p we mean that the cubie assumes the position in the cube that the label p is marking.
Now, if p_i for some $i \in \{1, 2, \ldots, n\}$ is a label marking the original position of cubie B and if cubie B assumes all the n labels of cubie A in consecutive order for consecutive rotations in M, starting with assuming p_{i+1} by the first rotation in M and then p_{i+2} by the second rotation in M etc, ending by assuming the label p_i by the last rotation in M, then we call the set P = $\{p_1, p_2, \ldots, p_n\}$ the **path through the cube of cubie A and cubie B under the move M** and we say that cubie A and cubie B **have the same path through the cube under the move M**.
As stated above, different labels may mark the same position in the cube. But this causes no problem. When this is the case it is all a matter of choosing the labels, if it is possible to choose the labels for two cubies moved by a move M so that the above conditions hold, then the cubies have the same path through the cube under the move M.

Remark 2.1.2. The above definition for a path through the cube of two cubies under a move M may at first be hard to grasp. The reader may think that it is complicated to determine if two cubies have the same path through the cube under a certain move, but it is actually a fairly easy observation. What

Definition 2.1.1 actually says is that two cubies have the same path through the cube under a move M if the two cubies have the same movement through the cube when moved by a move M.
So, to determine that two cubies have the same path through the cube under a move M, you first check that the cubies are of the same kind, that is, that both cubies are either corner cubies or edge cubies, since corner cubies always move to corner cubies and edge cubies move to edge cubies. Then, you check that the cubies assume the same positions in the cube when applying the move M. Finally, you check that the cubies assume these same positions in the same order. If all these three conditions apply to your cubies, then they have the same path through the cube under the move M.

Apply the move $(\mathrm{UR})^7$ on the cube. We observe that all edges have the same path through the cube under the move $(\mathrm{UR})^7$. The move $(\mathrm{UR})^7$ brings all edges back to their original positions in the cube and they all end up right orientated as well, all at once. This is not a coincidence but a general rule that leads us to the following lemma.

Lemma 2.1.3. *Let $c_1, c_2 \dots c_n$ be n cubies in the cube, with $n \geq 2$. Let M be any nonidentity move on the cube that brings all the n cubies back to their original positions in the cube. If all n cubies have the same path through the cube under the move M and if one of the cubies assumes its original orientation when the move M is made, then all the cubies assume their original orientation.*

Proof. Let cubie A and cubie B be any two of the n cubies. Consider cubie A at position A in the cube and cubie B at position B, see Figure 2.2 (cubie A and cubie B are not depicted).
The move M brings cubie A and B back to their original positions, position A and position B respectively. Cubie A and cubie B have the same path through the cube under the move M and therefore they must both be either corner cubies or edge cubies. So, we can label the faces of cubie A and B and give them an index depending on if the cubies are edges or corners. Here we use the set of orientations X and the homomorphism γ from section 2.1.1 and get that the move M gives rise to different orientation permutations on cubie A and B. These orientation permutations are illustrated in Figure 2.2.
Now, consider cubie A at position A and cubie B at position B. Cubie A goes through a change of orientation by the move M described by the permutation $\alpha = \beta\sigma$.
Cubie B, when moved to position A goes through a change of orientation described by the permutation β, and its change of orientation when moved from position A back to position B is described by the permutation σ. All in all, cubie B goes through a change of orientation by the move M described by the permutation $\mu = \sigma\beta$. These changes of orientation on cubie A and cubie B when moved back and forth from position A and B are all due to the

fact that cubie A and cubie B have the same path through the cube under the move M.
Let α be of order k, we shall prove the lemma by showing that μ is also of order k. We have that,

$$\alpha = \sigma^{-1}(\sigma\beta)\sigma = \sigma^{-1}\mu\sigma \quad (1)$$

and we get that,

$$\alpha = \sigma^{-1}\mu\sigma \Rightarrow \alpha^k = (\sigma^{-1}\mu\sigma)^k$$

$$= \underbrace{\sigma^{-1}\mu\sigma\sigma^{-1}\mu\sigma\cdots\sigma^{-1}\mu\sigma}_{k \text{ times}} = \sigma^{-1}\mu^k\sigma = id \Rightarrow \mu^k = id.$$

where id is the identity permutation.

The orientation permutations of the cubies in the cube can only be of order 1, 2 or 3, so $1 \leq k \leq 3$ and k has therefore no other divisors than 1 and k. If μ is of order 1, then from (1) we get that σ is also of order 1. Thus, μ is of order k. Since cubie A and cubie B are any two of the n cubies involved, this same condition holds for all n cubies. □

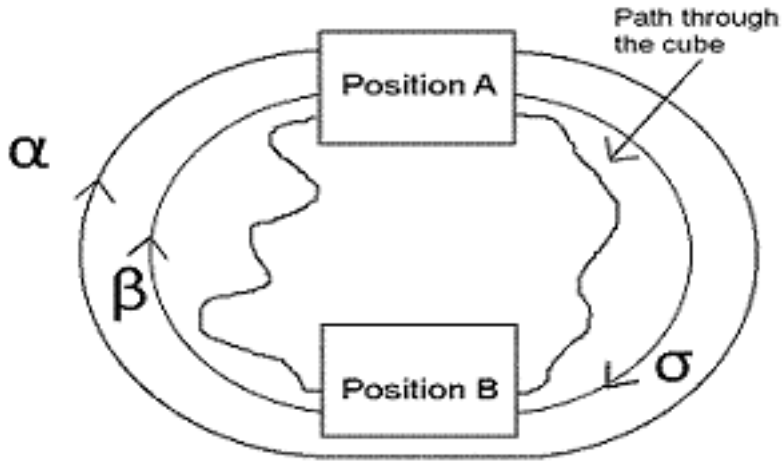


Figure 2.2: The inner line together with the boxes marking position A and B illustrate the path through the cube of cubie A and cubie B under the move M. The orientation permutations α, β and σ are also shown.

Proposition 2.1.4. *The group <UR> is of order 105.*

Proof. We start by considering the corner cubies.
Using the same notation as in section 1.3.2, we have that $\phi_C(\mathrm{UR}) = \phi_C(\mathrm{U})\phi_C(\mathrm{R}) = (c_1c_2c_3c_4)(c_3c_7c_8c_4) =$
$(c_3c_7c_8c_1c_2)$, so every fifth repetition of the move UR on the cube, brings every corner cubie back to its original position in the cube. This information is however not enough to determine the order of <UR> since the cubies may have changed their orientation so that the wrong colours are on the wrong faces of the cubies. We must consider the change of orientation that is made by the move UR.

Figure 2.3: The two sides of the cube that are taken into account by the move UR. We will look further into the movements of the corner cubies marked with a circle and a cross.

Consider Figure 2.3 showing the two sides of the Rubik's cube that are participating in the move UR. By repeating the move UR we observe that every corner cubie involved in the movement, except for the one marked with a cross in Figure 2.3, has the same path through the cube under the move $(\mathrm{UR})^5$, so by Lemma 2.1.3, it suffices to look at the change of orientation made on only one of these corner cubies.
Let us take a closer look at the corner cubie marked with a ring in Figure 2.3. The move $(\mathrm{UR})^5$ will move the corner cubie marked with a ring in Figure 2.3 back to its original position. The change of orientation made on that cubie after this move is illustrated in Figure 2.4.

If we label the green face 1, the red face 2 and the yellow face 3 of the cubie on the left in Figure 2.4, then the set X in section 2.1.2 is given by, $X = \{1, 2, 3\}$. The cubie on the right in Figure 2.4 shows that the move $(\mathrm{UR})^5$ gives rise to the permutation $\sigma = (123)$ on the set X. We have that

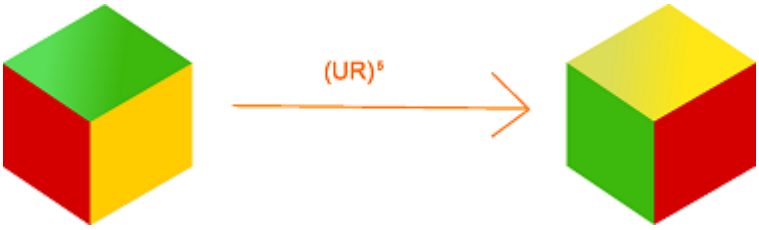


Figure 2.4: The change of orientation on cubie marked with a ring in Figure 2.3 when the move $(UR)^5$ is applied on the cube.

$\sigma = (123)$ is of order 3 and more generally,

$$(UR)^{15n} = id, n \in N \quad (2)$$

where id is the identity element in the case of corner positioning and orientation.

This result applies to all corner cubies involved, except for the one marked with a cross in Figure 2.3. Considering the corner cubie marked with a cross in Figure 2.3, we observe that it does not change its position for any of the moves in <UR>. Here again we find that the change of orientation of the corner cubie with a cross is given by the permutation $\sigma = (123)$ and more generally we have,

$$(UR)^{3n} = id, n \in N \quad (3)$$

for the corner cubie with a cross.

Now, considering the edges, we get that ϕ_E(UR)= ϕ_E(U)ϕ_E(R) = $(e_1e_2e_3e_4)(e_3e_7e_{11}e_8) = (e_3e_7e_{11}e_8e_4e_1e_2)$, so every seventh move of UR brings all the edges back to their original position. Here we observe that all edges have the same path through the cube under the move $(UR)^7$. We find that the orientation on one of the edge cubies does not change and conclude that the same holds for the rest of the edges. Thus,

$$(UR)^{7n} = id, n \in N \quad (4)$$

for all the edges.

The cube returns to its original state when all the equations (2)-(4) are simultaneously satisfied. So the order of UR is the least common multiple of 15, 3 and 7, that is, |<UR>|= 105. □

Remark 2.1.5. The proof that |<UUR>|= |<URR>|= 30 and |<UUUR>|= |<URRR>|= 63 is similar to the proof of Proposition 2.1.4.

Theorem 2.1.6. *Let G be a cyclic group of order n generated by an element a. Then every element of G in the form, a^m, for positive integer m, generates a subgroup H of G, where $|H| = n/gcd(m,n)$ and where $gcd(m,n)$ denotes the greatest common divisor of m and n.*

Proof: See Theorem 6.14 in "A First Course In Abstract Algebra" (Fraleigh).

Theorem 2.1.6 tells us the size of each and one of the subgroups of a cyclic group G provided that we know their generators.

Example 2. Take for example the element $(\mathrm{UUR})^{15}$ in the group <UUR>. Here n = 30, m = 15 and $H = <(\mathrm{UUR})^{15}>$, so by Theorem 2.1.6 we get that $|H| = 30/gcd(15,30) = 30/15 = 2$.

2.1.3 Nonabelian groups

Up till now we have only been looking at abelian subgroups of the Rubik's cube group. In this section we will consider some nonabelian subgroups. We will begin by presenting a lemma.

Lemma 2.1.7. *Let G be a finite group generated by two nonidentity elements a and b such that $a^2 = b^2 = id$, where id is the identity element of G. Then, $|G| = 2|<ab>| = 2|<ba>|$.*

Proof. Since the elements a and b of G are both of order two, every element of G can be written in one of five forms. These are,

(1) id

(2) $\underbrace{abab\ldots ab}_{i \text{ times}}$, for $1 \leq i \leq n-1$

(3) $\underbrace{baba\ldots ba}_{i \text{ times}}$, for $1 \leq i \leq n-1$

(4) $\underbrace{baba\ldots bab}_{i \text{ times}}$, for $0 \leq i \leq n-1$

(5) $\underbrace{abab\ldots aba}_{i \text{ times}}$, for $0 \leq i \leq n-1$

where n is the order of ab and ba

For an element of G can either be the identity element id or start with an "a" and end with an "a", or start with an "a" and end with a "b" etc, giving a total of five possible ways to express the elements in G.
The elements written in the form (3) are actually the inverses of the elements written in the form (2). The element $(ba)^i$, for $i \in \{1,2,\ldots,n-1\}$ in (3),

is the inverse of the element $(ab)^i$ and is therefore equal to $(ab)^{-i} = (ab)^{n-i}$ which is an element of (2), since $1 \leq n-i \leq n-1$. This shows that every element in (3) is in (2). Conversely, the element $(ab)^i$ in (2) is equal to $(ba)^{-i} = (ba)^{n-i}$ which is an element of (3), that is, every element in (2) is in (3). This shows that the elements in the form (2) and (3) are the same.
By the result above we see that the element $(ba)^i b$ for
$i \in \{0, 1, 2, \ldots, n-1\}$ in (4) is equal to $(ab)^{n-i}b$ which is an element of (5), since $1 \leq n-i \leq n$. Therefore every element in (4) is in (5). The proof that all elements in (5) are in (4) is similar. This shows that the elements in (4) and (5) are the same.
Now, we want to prove that (2) = (3) $\neq$ (4) = (5) by showing that (3) $\neq$ (5). Assume there are $i, j \in \mathbb{Z}$ such that $(ab)^i = (ab)^j a$. If $i = j$, then we get that $a = id$ which is a contradiction. With $i > j$ we have that,

$$(ab)^i = (ab)^j a \Leftrightarrow (ab)^{i-j} = a$$

which is a contradiction, so (2) = (3) $\neq$ (4) = (5).
This reduces the number of distinct forms to express the elements of G to only 3. These are,

(1) id

(2) $\underbrace{abab\ldots ab}_{i \text{ times}}$, for $1 \leq i \leq n-1$

(3) $\underbrace{baba\ldots bab}_{i \text{ times}}$, for $0 \leq i \leq n-1$

Here we see that the number of elements in G is equal to $2n$ =2<ab> = 2<ba>. □

Proposition 2.1.8. *The group <UU, RR> is of order 12.*

Proof. We have that $(\mathrm{UU})^2 = (\mathrm{RR})^2 = id$, where id is the identity move, so by Lemma 2.1.7 we get that |<UU, RR>| = 2|<UURR>|.
We will calculate the order of UURR in much the same way as when we calculated the order of UR in section 2.1.2. We shall begin by considering the edges.
Using the same notation as in section 1.3.2, we have that, $\phi_E(\mathrm{UURR}) = (\phi_E(\mathrm{U}))^2(\phi_E(\mathrm{R}))^2 =$
$(e_1e_2e_3e_4)^2(e_3e_7e_{11}e_8)^2 = (e_1e_3)(e_2e_4)(e_3e_{11})(e_7e_8) = (e_3e_{11}e_1)(e_2e_4)(e_7e_8)$, so every sixth move of UURR brings all the edges back to their original position.
We observe that the edges switches between only two positions in the cube and therefore it is easy to see that they do not change their orientation by the move $(\mathrm{UURR})^2$ and more generally we have, $(\mathrm{UURR})^{6n} = id$, $n \in N$ for

all the edges.
For the positioning of the corner cubies we get, ϕ_C(UURR)= $(c_1c_2c_3c_4)^2(c_3c_7c_8c_4)^2 = (c_1c_3)(c_2c_4)(c_3c_8)(c_7c_4) = (c_3c_8c_1)(c_4c_7c_2)$, so every third move of UURR brings all the corners back to their original position. Consider Figure 2.5, we see that the corner cubies marked with a ring have the same path through the cube under the move $(\text{UURR})^3$ and likewise with all the corners marked with a cross. So we need only to check the change of orientation on a corner cubie marked with a ring and a corner cubie marked with a cross. But by the symmetry of the cube, the change of orientation on the corner cubies marked with a ring will be the same as the change of orientation on the corner cubies marked with a cross. So, it suffices to check the orientation change on only one corner cubie. Doing that we see that the move $(\text{UURR})^3$ does not change the orientation of the corners and more generally, $(\text{UURR})^{3n} = id$, $n \in N$ for all the corners.
So the order of <UURR> is the least common multiple of 3 and 6, that is, |<UURR>| = 6, giving |<UU,RR>| = $2 \cdot 6 = 12$. □

Figure 2.5: The corners marked with a cross and a ring.

Theorem 2.1.9. *The set* $S = \{(12), (23), (34), \ldots, ((n-1)n)\}$ *for* $n \geq 2$, *generates* S_n *and* S_n *is of order* $n!$.

Proof: See Lemma 1.2.23 and Theorem 1.2.14.

We are now going to present a somehow trivial lemma.

Lemma 2.1.10. *Let* $H = <(ab), (ac), (cd)>$ *and* $K = <(ef), (eg), (gh)>$ *for* $(ab), (ac), (cd), (ef), (eg), (gh) \in S_n$, $n \geq 2$. *Then there exists an isomorphism* $\mu : H \to K$ *and if id is the identity permutation of* H, *then* $\mu(id)$ *is the identity permutation of* K.

Proof. Let μ be a function mapping the elements of H with the elements of K in the following way,

$a \to e$

$b \to f$

$c \to g$

$d \to h$

It is clear that μ as defined above form a homomorphism from how we multiply permutations. For example we have, $\mu((ab)(ac)) = \mu((acb)) = (egf)$ and $\mu((ab))\mu((ac)) = (ef)(eg) = (egf) = \mu((ab)(ac))$.
Since μ maps every "number" in the transpositions of H one-to-one onto the numbers in the transpositons of K according to the mapping scheme presented above, it is clear that any two permutations σ_1 and σ_2 in H satisfying $\mu(\sigma_1) = \mu(\sigma_2)$ must be the same. Moreover, since this mapping is onto the numbers in the transpositions in K and μ is a homomorphism we get that μ is surjective.
From Proposition 1.2.35, condition (1), we have that, $\mu(id)$ is the identity permutation of K. □

Proposition 2.1.11. *The group <UU, RR, LL> is of order 96.*

Proof. Recall that the only moves allowed are those in the group <UU, RR, LL>, so whenever we speak about an allowed move we shall always mean a move from this group.
Now, let us begin by considering the orientation of the cubies.
Since the only moves allowed are those generated by RR, UU and LL we see that every cubie involved has a limited path through the cube. For instance, if we regard the movement of the corners, we see that every corner has a limited movement through the cube as illustrated in Figure 2.6, a corner marked with a cross always moves to a corner marked with a cross and a corner marked with a ring always moves to a corner marked with a ring.
Consider a specific corner cubie marked with, say, a cross, which we shall call corner cubie A. Apply any move allowed on the cube that brings corner cubie A away from its original position, to a position B in the cube. From Figure 2.6 it is clear that in order to bring cubie A back to its original position in the cube, we must apply the same move on the cube, but in the reverse order, as we did when we brougth cubie A to position B. By doing that we obtain the identity move for corner cubie A, thus the orientation of corner cubie A will not change when moved back to its original position. This same argument applies to all corner cubies by the symmetry of the cube.

The edge cubies have an even more limited movement through the cube than the corner cubies. The edges switches between only two positions and it is easy to see that they do not change their orientation when moved back to their original positions.
Thus, every position configuration in the cube has only one orientation configuration and the order of <UU, RR, LL> is therefore entirely determined by the positioning of the cubies.

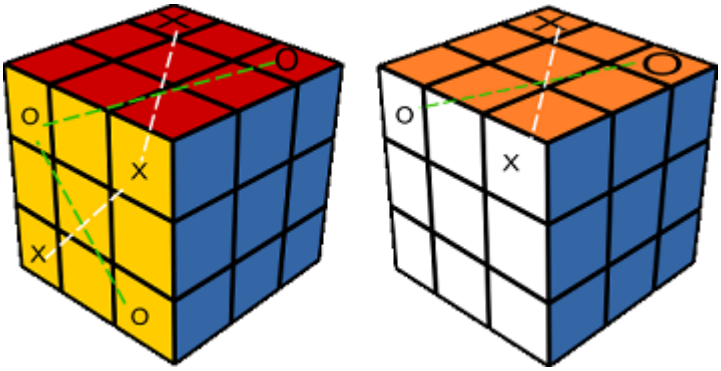


Figure 2.6: Corners marked with a cross and corners marked with a ring have their own limited movement through the cube. The green and white lines illustrates their movement through the cube.

By the indexation given in Figure 2.7, we get the following result for the positioning of the cubies.

ϕ_E(RR)=(21)(56); ϕ_C(RR)=(12)(47)
ϕ_E(UU)=(23)(78); ϕ_C(UU)=(16)(43)
ϕ_E(LL)=(34)(9(10)); ϕ_C(LL)=(65)(38)

Let σ be any product of (21), (23) and (34) and μ be any product of (56), (78) and (9(10)). Since σ and μ are products of disjoint cycles, the product $\sigma\mu$ is the identity permutation id when both $\sigma = id$ and $\mu = id$. This means that whenever we apply an allowed move on the cube that returns the edges marked with index 1-4 in Figure 2.7 back to their original positions in the cube, the edges marked with 5-10 return as well.
The permutations of the edges that do not commute, that is, (21), (23) and (34) are of the form (ab), (ac) and (cd). While the permutations of the corners (12), (16) and (65) are of the form (ef), (eg) and (gh). Also, (47), (43) and (38) are of the form (ij),(ik) and (kl).
Let H =<(21), (23), (34))>, K =<(12), (16), (65))> and

M =<(47), (43), (38)>.
By Lemma 2.1.10 there exist two isomorphisms f and g from H onto K and M respectively.
Let $\phi_{C,E}$: <UU, RR, LL>$\rightarrow S_8 \times S_{12}$ be such that $\phi_{C,E}(X) = (\phi_C(X), \phi_E(X))$ for a move X $\in$ <UU, RR, LL>. We know that $\phi_{C,E}$ is a homomorphism since ϕ_C and ϕ_E are homomorphisms.
This homomorphism describes the positioning of the corners and edges for every allowed move. The kernel of $\phi_{C,E}$ consists of moves that leaves the corners and edges untouched regarding their positions. For every allowed move X we have, $\phi_{C,E}(X) = (\phi_C(X), \phi_E(X)) = (\beta\gamma, \sigma\mu)$ where $\beta \in K$, $\gamma \in M$, $\sigma \in H$ and μ is a product of (56), (78) and (9(10)) that depends on σ. Note that β, γ and σ are not independent. By Lemma 2.1.10 we can write this relation as, $\phi_{C,E}(X) = (\beta\gamma, \sigma\mu) = (f(\sigma)g(\sigma), \sigma\mu)$.
Let M be any allowed move on the cube that do not change the positions of the edges, by the result above and by Lemma 2.1.10 we have that, $\phi_{C,E}(M) = (f(id)g(id), idid) = (id, id)$, thus M is in the kernel of $\phi_{C,E}$. This means that whenever the edges return to their original positions in the cube, the corners return as well.
So every position configuration of the edges has only one position configuration of the corners and we get that the order of <UU, RR, LL> is entirely determined by the positioning of the edge cubies.

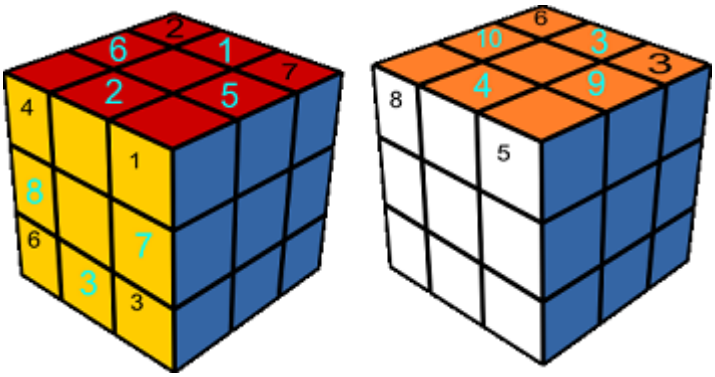


Figure 2.7: The red face of the cube is the right face, the yellow is the up face, the brown is the left face and the white is the down face of the cube.

Considering the permutations of the edges, we see that all products of (12), (23) and (34) combine to form all of S_4 which is of order 4! = 24, by Theorem 2.1.9. But we must also consider the permutations that commute, (56), (78) and (9(10)).
Consider a fix position configuration of the edges marked with index 1-4 in Figure 2.7. We want to know the number of ways we can change the posi-

tioning of the edges marked with index 5-10 in Figure 2.7 without changing the fix position configuration of the edges 1-4.
We see that applying the move $(RR)^n$ for any $n \geq 0$ on the cube provides only one way of having the edges 5-10 positioned for a fix position configuration of the edges 1-4. The same holds for the moves $(UU)^n$ and $(LL)^n$. So we need to combine these three moves, RR, UU and LL.
When combining we get that every fix position configuration of the edges 1-4 has at most 5 possible position configurations of the edges 5-10, these can be described by the permutations,

$$\text{Edges 5-10:} \quad \begin{matrix} (56)(78) \\ (56)(9(10)) \\ (78)(9(10)) \\ (56)(78)(9(10)) \\ id \end{matrix}$$

We now introduce a new terminolgy that we will use frequently in the remainder of the proof. Let M be a move on the cube, σ be a permutation and let cubie A be a cubie, then, whenever we say a move M produces σ for cubie A we mean that when applying the move M on the cube, M changes the position of cubie A in the cube in a way that can be described by σ.
Now, the move $(RRUU)^3$ produces id for the edges 1-4 and (56)(78) for the edges 5-10. This is one possible position configuration of the edges.
The move $(UURRUULL)^3$ produces id for the edges 1-4 and (56)(9(10)) for the edges 5-10. The move $(UULL)^3$ produces id for the edges 1-4 and (78)(9(10)) for the edges 5-10, so this is a third possible configuration of the edges.
However, there is no allowed move that produces id for the edges 1-4 and (56)(78)(9(10)) for the edges 5-10.
Because if there were such a move, then it must consist of all three moves, RR, UU and LL since each one of these moves are necessary to produce the permutations (56), (78) and (9(10)) for the edges 5-10.
Moreover, it must be a move that consists of an odd number of each of the moves RR, UU and LL. For example, the move RRUULLRR contains two moves of RR that produces $(56)^2(78)(9(10)) = (78)(9(10))$ for the edges 5-10 and this is not the one we want.
So, this move will therefore produce a permutation for the edges 1-4 that is a product of an odd number of transpositions, that is, an odd permutation. An odd permutation in S_4 is either a 2-cycle or a 4-cycle, both of these types of permutations are of even order. Thus, this move produces a permutation of even order for the edges 1-4. But the transpositions of the edges 5-10 commutes with each other and any product of these permutations is therefore a permutation of order at most 2. So we see that whenever this move

produces *id* for the edges 1-4, it also produces *id* for the edges 5-10.
In summary, we have that every fix position configuration of the edges 1-4 has the following possible position configurations of the edges 5-10.

Edges 5-10: $\begin{matrix}(56)(78)\\(78)(9(10))\\(56)(9(10))\\id\end{matrix}$

So every fix position configuration of the edges 1-4 has a total of four different positions configurations of the edges 5-10. This gives, |<UU,RR,LL>| $= 4! \cdot 4 = 24 \cdot 4 = 96$ □

Remark 2.1.12. It is possible to prove Proposition 2.1.8 by the methods used in Proposition 2.1.11.

Theorem 2.1.13. *Let H be a subgroup of a finite group G and let $(G : H)$ be the number of left cosets of H in G. Then, $|G| = (G : H)|H|$.*

Proof. The relation under which left cosets are formed is an equivalence relation. This means that every element of G is in exactly one of the left cosets of H. Also, the number of elements in each left coset of H is as many as the number of elements in H. So, the total number of elements in G is equal to the number of left cosets of H in G times the number of elements in H, that is, $|G| = (G : H)|H|$. □

Corollary 2.1.14. *The group <UU,RR,LL,DD> is of order 192.*

Proof. Remember that we are only dealing with moves from the group <UU,RR,LL,DD> which we refer to as allowed moves.
Let us begin by considering the orientation of the corner cubies.
The group we are dealing with here is the same at the one in Proposition 2.1.11 with the only difference that we have an extra move, the move DD.
In the proof of Proposition 2.1.11 we saw that the only possibilty to return a corner cubie to its original position, when the only allowed moves were from the group <UU,RR,LL>, is to apply the same moves, but in the reverse order, as we did when we brought the corner cubie away from its original position. This move turned out to be the identity move for the corner cubie and therefore did not change the orientation of the corner cubie.
But with the group <UU,RR,LL,DD> we have one more possibility to return a corner cubie to its original position.
We can return a corner cubie to its original position by moving it "around" the cube. For example, regard the corner cubie marked with 1 in Figure 2.8, the move RRDDLLUU brings that corner cubie "around" the cube and back

to its original position. This move may not be an identity move for the corner cubie when regarding its change of orientation. But by checking we see that it actually is. By the symmetry of the cube, we see that this same condition applies to all corner cubies. So, all in all, every move in the group <UU,RR,LL,DD> that brings the corner cubies back to their original positions does not change the orientation of the corner cubies.
The edge cubies have a limited movement when applying moves from the group <UU,RR,LL,DD>. They only switch between two positions and it is clear that they do not change their orientations when returning back to their original positions.

From the proof of Proposition 2.1.11 we know that the number of different patterns obtained on the cube, when applying 180° turns on the up, right and left faces of the cube, is entirely determined by the positioning of the edges. By the symmetry of the cube we get that the same holds when applying 180° turns on the down, right and left faces of the cube and therefore on all the four faces, up, right, left and down faces of the cube.
So, the order of the group <UU,RR,LL,DD> is entirely determined by the positioning of the edges.

Let G =<UU, RR, LL, DD> and H =<UU, RR, LL>. The product of the following permutations describes the positioning of the edges when applying a move in H.

Edges: (14)(56)
(14)(78)
(14)(9(10))

By the indexation in Figure 2.8 we get that $\phi_E(DD) = (14)((11)(12))$. So, if we only regard the edges 1-4, we see that H describes the move DD. But there is no move in H that affects the edges marked with index 11 and 12, see Figure 2.8.
Now, there are two types of moves in G, moves in H and moves in H containing the move DD. The latter type can further be categorized into moves consisting entirely of DD and nonidentity moves in H containing DD.
Consider the left cosets H and DDH of H in G. All moves in H are in the coset H. So, we are left to find the left cosets of H for the type of moves in H that contains DD.
Moves consisting entirely of DD are of the form DD^n for $n \in N$. When n is even we have that $\text{DD}^n = id$ where id denotes the identity move in G, this is a move that belongs to the coset H. When n is odd we have that $\text{DD}^n =$ DD and this is a move in the coset DDH.
Now we are left with nonidentity moves in H containing DD.

If we for the moment only regard the edges 1-4 we see that both cosets H and DDH describe DD by the arguments above. But if we regard the edges 5-12 we see that when we have nonidentity moves in H containing an odd number of moves of DD we get that the permutations describing the positioning of the edges has the factor $((11)(12))$, that is, we are dealing with a move that affects the edges 11 and 12. This type of move belongs to the coset DDH.
Nonidentity moves in H containing an even number of moves of DD do not affect the edges 11 and 12 and this type of move belongs therefore to the coset H.
So, the cosets H and DDH are enough to describe all moves in G, together they exhaust G. Thus, H has only two left cosets in G and by Theorem 2.1.13 and by Proposition 2.1.11, we get that $|G| = (G : H)|H| = 2 \cdot 96 = 192$. □

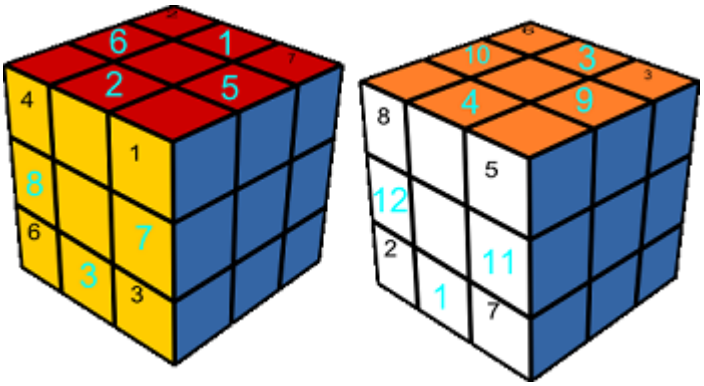


Figure 2.8: The red face of the cube is the right face, the yellow is the up face, the brown is the left face and the white is the down face of the cube.

Chapter 3

"Rubik's Cube Group Elements of Order Two"

by Joel Mickelin

This paper describes the elements of order two in the Rubik's Cube Group. They are first enumerated, and found to be of the order 10^{11} *many. They are then divided into conjugacy classes with respect to conjugation by the Rubik's Cube Group. Each conjugacy class will contain elements being composed of a fixed number of corner and edge transpositions. Finally, the structure of the subgroups of the Cube Group which are isomorphic to* S_3 *is discussed, and a lower limit to how many such groups exist is given as being of the order* 10^{12}*.*

Denna rapport syftar till att beskriva elementen av ordning två i Rubiks Kub-gruppen. Dessa element beräknas först vara av ordning 10^{11} *många. Elementen visas sedan kunna delas upp i konjugansklasser, under konjugans med Kub-gruppen. Varje konjugansklass kommer att innehålla element bestående av ett fixt antal transpositioner av kant- och hörnbitar. Slutligen diskuterar vi strukturen hos de delgrupper av Kub-gruppen som är isomorfa med* S_3*, och beräknar en lägre gräns för antalet sådana delgrupper som existerar, vilken bestäms till storleksordningen* 10^{12}*.*

3.1 Cube elements of order two

This section examines the Cube elements of order two, all of which fascinate the author for their ability to "unlock themselves", so to speak. The purpose of this section is first to enumerate the elements of order two using strictly combinatorial arguments, then to examine the elements of order two as distinct orbits of a conjugacy operation. Lastly, some interesting isomorphims to S_3 are pointed pout.

We will see that the elements of order two can be summarized as being of the order 10^{11} many. Merely a fraction, that is, of the total number of elements in the group (being of the order 10^{19}). We will further see that the elements of order two can be divided into conjugacy classes, where any given conjugacy class contains only elements being composed of a fixed number of transpositions of corner pieces and edge pieces, respectively.

Finally, we note that the subgroups of the Cube Group which are isomorphic to S_3, which all by necessity contain elements of order two, can be estimated as being at least 10^{12} many.

3.1.1 Counting the elements of order two

Our first task is to simply count the elements in question. We will see that these can be divided into three distinct subsets. We will be able to count the elements of order two in the cube group, using quite simple combinatorial arguments.

First, we note that the set of Cube elements of order two can be divided into three disjoint subsets (this is almost a tautology).

Definition 3.1.1. C_2 is the set of Cube elements of order two which are permutations of only corner pieces. E_2 is the set of Cube elements of order two which are permutations of only edge pieces. E_2C_2 is the set of Cube elements of order two which are permutations of both corner pieces and edge pieces.

We will examine the structure of each subset separately.

3.1.2 Elements permuting only corner pieces

Theorem 3.1.2. *An element in C_2 must be orientation preserving.*

Proof. Assume $x \in C_2$ alters (in keeping with the notation of Prop. 2.18) at least one coordinate ϵ_i of the corner orientation tuple. If

$$x(\epsilon_i) \equiv \epsilon_i + 1 \mod 3 \Rightarrow x^3(\epsilon_i) \equiv \epsilon_i \mod 3$$

and so x must be of order three. The same is true if $x(\epsilon_i) \equiv \epsilon_i + 2 \mod 3$. Hence, if x permutes at least one coordinate of the orientation tuple, the

order of x is at least three, which would contradict our assumption. Thus, the assumption is false. □

Proposition 3.1.3. *The elements of C_2 are swaps of an even number of corners.*

Proof. This follows from Lemma 1.3.13, and the fact that no edges are permuted by the elements in C_2 (i.e. the even identity permutation is used on the set of edge pieces). □

We will now proceed to compute the cardinality of C_2, and we do so by selecting the corner pairs to permute, noting that each pair can have three different orientations relative to each other, and that the order of the transpositions is irrelevant.

We summarize the above reasoning in writing the following proposition.

Proposition 3.1.4.

$$|C_2| = \frac{1}{4!}\binom{8}{2}\binom{6}{2}\binom{4}{2}3^4 + \frac{1}{2!}\binom{8}{2}\binom{6}{2}3^2 = 10395$$

Proof. We construct each element of C_2 thus: we choose the number of corners pairs to transpose, which must be even. We note that for each corner pair, we have three orientation preserving swaps (since each corner piece has three orientations, and an orientation shift in one piece would necessitate a corresponding shift in the other), so each corner transposition will give a contribution of 3 to the total number of elements. Finally, we note that the order in which we choose each pair is irrellevant, which accounts for the above divisions. Summing up after this fashion, we get the above result. □

3.1.3 Elements permuting only edge pieces

We now turn our attention to E_2.

What we first must be aware of is that the elements in E_2 need not be orientation preserving, as we concluded when proving Theorem 1.3.21 that the edge orientation can be choosen independently. Seeing as the edge pieces each have two possible orientations, we know the orientation changes to be of order two. By the same reasoning as for C_2, we know that the order two elements of E_2 are all even.

Theorem 3.1.5. *The elements of E_2 all contain zero or an even number of edge piece swaps.*

Proof. From the reasoning behind Lemma 1.3.21, we know that the 2^{11} possible orientations of the edge pieces can be achieved independently. Hence, the permutations generating them must be even. Thus, the elements of E_2, which may consist of both swaps and orientation flips, must contain an even number of edge piece transpositions in order to satisfy the demand for parity, since no corner pieces are moved. □

When counting the elements of E_2, we first choose the corner pairs to transpose, noting that each pair has two possible orientations relative to each other, and that we must choose an even number of pairs. We then notice that the orientations of the remaining pieces, save for one, can be chosen independently, according to Lemma 1.3.21.

We summarize the above into a proposition.

Proposition 3.1.6. $|E_2| = \frac{1}{6!}\binom{12}{2}\binom{10}{2}\binom{8}{2}\binom{6}{2}\binom{4}{2}2^6 + \frac{1}{4!}\binom{12}{2}\binom{10}{2}\binom{8}{2}\binom{6}{2}2^4 2^3 + \frac{1}{2!}\binom{12}{2}\binom{10}{2}2^2 2^7 + \binom{12}{0}2^{11} = 8080447$

Proof. We construct the elements of E_2 by first noting that all permutations involving an even number of edge transpositions are included in E_2 due to Lemma 1.3.13. Thus, we can proceed to choose an even number of edge pairs to transpose, noting that the order in which we choose pairs is irrelevant. We also note that there are two orientation preserving swaps for each for each edge transposition, so each edge transposition will contribue with a factor 2. Furthermore, according to Lemma 1.3.21, each edge piece not transposed save for one will contribute with a factor 2 as well, since its orientation can be switched independently. Summing up in this fashion, we get the above result. □

3.1.4 Elements permuting both edge pieces and corner pieces

Lastly, we turn our attention to E_2C_2. E_2C_2 can be further divided into two subsets. The first of these subsets contain all elements permuting an even number of corner pairs as well as an even number of edge pairs. We call this set $E_{2even}C_{2even}$ and its cardinality is simply $|E_2||C_2|$.

The second subset, that containing the elements transposing an odd number of corner pairs as well as an odd number of edge pairs, is a bit more interesting. Its cardinality will be that of $|E_{2odd}||C_{2odd}|$, where E_{2odd} and C_{2odd} are the sets of odd elements of order two permuting edges and corners, respectively.

Using ideas entirely analogous to those used in the previous two sections, we make the necessary computations.

Proposition 3.1.7.

$$|C_{2odd}| = \frac{1}{3!}\binom{8}{2}\binom{6}{2}\binom{4}{2}3^3 + \binom{8}{2}3 = 11424$$

Proof. We once more choose corner pairs to transpose, yet taking care to violate the demand for parity by choosing uneven numbers of corner pairs to transpose. We note that there are three orientation preserving swaps for each corner pair, and sum after that fashion. □

Proposition 3.1.8. $|E_{2odd}| = \frac{1}{5!}\binom{12}{2}\binom{10}{2}\binom{8}{2}\binom{6}{2}\binom{4}{2}2^5 \cdot 2 + \frac{1}{3!}\binom{12}{2}\binom{10}{2}\binom{8}{2}2^3 2^5 + \binom{12}{2}2 \cdot 2^9 = 7607424$

Proof. We take care to violate the demand for parity for the edges as well, yet must note that the edge orientation may be independently changed. □

3.1.5 Summation of the elements of order two

We now proceed to sum the elements of order two, using the above computations.

$$|E_2| + |C_2| + |E_2||C_2| + |E_{2odd}||C_{2odd}| = 170911549183 \approx 1.7 \cdot 10^{11}$$

We see that though the elements of order two are plentiful, they make up a mere fraction of the elements of the Cube group, which are of the order 10^{19} many.

The author has verified the above computations through comparison with those made by David Joyner (Adventures in Group Theory, John Hopkins University Press 2002) who makes analogous arguments using a slightly different notation.

3.1.6 Concerning conjugacy classes of elements of order two

Definition 3.1.9. Suppose we have a group G. $a, b \in G$ are **conjugate** if $\exists g \in G : g.a.g^{-1} = b$.

Theorem 3.1.10. *Conjugacy is an equivalence relation.*

Proof. We check the three conditions necessary for the theorem. Conjugacy is reflexive, since $id^{-1}.a.id = id.a.id = a \forall a \in G$. Conjugacy is symmetric, for $g^{-1}.a.g = b \Rightarrow g.b.g^{-1} = a \forall a, b \in G$. Lastly, conjugacy is transitive, for if $g^{-1}ag = b$ and $f^{-1}.b.f = c$ then $f^{-1}.g^{-1}.a.g.f = (gf)^{-1}.a.gf = c \forall a, b, c, \in G$. Hence, conjugacy is an equivalence relation. □

Definition 3.1.11. A **conjugacy class** C(a) of an element a in a group G is the set $\{g.a.g^{-1} : g \in G\}$.

Remark 3.1.12. Note that all conjugacy classes can be described as orbits of a group action $g.x = g.x.g^{-1}$.

Theorem 3.1.13. *A conjugacy operation of the Rubik's Cube Group on a Rubik's element x of order two cannot change the number of transpositions of edge or corner pieces of x.*

Proof. We study any cube element x, which can be written as a series of transpositions, where all transpositions may be written in coupled pairs. We note that any two permutation pairs may be interchanged, provided the Cube pieces one pair permutes are disjoint from those of the other pair. For example, $(c_1c_2)(c_3c_4)(c_5c_6)(c_7c_8) = (c_5c_6)(c_7c_8)(c_1c_2)(c_3c_4)$ but

$(c_1c_2)(c_3c_4)(c_5c_6)(c_1c_8) \neq (c_5c_6)(c_1c_8)(c_1c_2)(c_3c_4)$. We also note that if x is of order two, it can only contain one transposition of any Cube piece. Therefore, any two coupled transposition pairs may be freely interchanged in x.

Let us now see which effect the conjugation of x by a cube element g has. Imagine that g transposes no cube pieces which already occur in the transpositions of x. Then, since we can always interchange the coupled transposition pairs making up $g^{-1}.x.g$, provided we do not interchange any two pairs in neither g^{-1} nor g, we see that $g^{-1}.x.g = g^{-1}.g.x = id.x = x$.

Assume then that the transposition pairs of g do transpose elements already transposed in x. Using the interchange argument defined above, we can rearrange the series so that we may assume g to only be composed of one single transposition pair, since what we do otherwise is study the effect of sequentially applied transposition pairs of g. We may also, without loss of generality, study only the effect of g on either corner or edge pieces.

We assume g contains a transposition (x_1x_2), and that x contains a transposition (x_1x_3), where x_i are either corner or edge pieces. Through various rearrangements as detailed above, we end up with the permutation $\ldots(x_1x_2)(x_1x_3)(x_1x_2)\ldots = \ldots(x_2x_3)\ldots$ as part of the transposition series of $g^{-1}.x.g$. If x also contains a transposition (x_2x_4), we see that we can obtain a rearrangement so that part of the transposition series is $\ldots(x_1x_2)(x_1x_3)(x_2x_4)(x_1x_2)\ldots = \ldots(x_1x_4)(x_2x_3)\ldots$. In either case, each transposition pair acting on x by conjugation can only change the transpositions making up x, and not the number of them. By iteration, we see that neither can g as a whole. □

From the arguments presented in the above, rather lengthy proof, we obtain the following corollary.

Corollary 3.1.14. *Any transposition of two corner or two edge pieces in a cube element x of order two may be changed into any other independently, by conjugation.*

Proof. Imagine that we have the transposition (x_ix_j), which we want changed into (x_kx_l) without affecting any other transpositions in the series. This can be done by the following algorithm:

Pick any transposition (x_mx_n) in x, where $m, n \notin \{i, j, k, l\}$. Conjugate x with the cube element $(x_mx_n)(x_ix_k)$. This will not affect the transposition (x_mx_n), yet change (x_ix_j) into (x_kx_j). Conjugate once more, now with the element $(x_mx_n)(x_jx_l)$, which will change (x_kx_j) into (x_kx_l) without affecting any other transpositions. □

We now realise that we may divide the elements of order two into conjugacy classes using the above theorems. We shall now seek to compute how many there are.

Theorem 3.1.15. *C_2 can be divided into two conjugacy classes.*

Proof. We know that all permutations of two corner pairs, and all permutations of four corner pairs, respectively, can be conjugated into any other such permutations. □

Theorem 3.1.16. *E_2 can be divided into $2^{11}+2^7+2^3+1$ conjugacy classes.*

Proof. We know that any element of E_2 involving a certain number of transpositions may be conjugated into any other, save for differences in the orientation of the edge pieces, since changes to this orientation are independent from other permutations, and will thus cancel themselves out by conjugation. All elements having a certain orientation and being composed of a certain number of edge piece transpositions will thus constitute one conjugacy class. □

Theorem 3.1.17. *E_2C_2 may be divided into $2(2^{11}+2^7+2^3+1)+2(2+2^5+2^9)$ conjugacy classes.*

Proof. Since any permutation of two edge pieces or two corner pieces may be changed into any other such, we have that the number of conjugacy classes of even-even elements in E_2C_2 will simply be the product of the number of conjugacy classes in E_2 and C_2.

Using a similar reasoning as for C_2, we see that that the conjugacy classes of the set C_{2odd} are the sets of permutations composed of three or one corner transpositions, two in total. Analogously, but taking note of different orientations, as we did for E_2, we see that the elements of E_{2odd} contains elements having either 5, 3 or 1 transpositions, thus giving that the number of conjugacy classes in E_{2odd} are $2 + 2^5 + 2^9$. □

A quick summation gives that the total number of conjugacy classes of elements of order two is 7649.

3.1.7 Conjugative stabilizer subgroups of elements of order two

A natural question to ask is what the stabilizer of a given order two element under conjugation looks like.

Definition 3.1.18. Suppose we have a group action of a group G on a set X. For any element $x \in X$, we have that the **stabilizer** G_x of x is the set $G_x = \{g \in G : g.x = x\}$.

Theorem 3.1.19. *$\forall g \in G$, G_x is a subgroup of G.*

Proof. We need to prove that G_x is closed and that every element is invertible. First, we see that $\forall g_1, g_2 \in G_x, (g_1.g_2).x = g_1.(g_2.x) = g_1.x = x \Rightarrow g_1.g_2 \in G_x$. Moreover, $x = id.x = (g^{-1}.g).x = g^{-1}.(g.x) = g^{-1}.x \Rightarrow g^{-1} \in G_x$. Thus, G_x is a subgroup of G. □

Theorem 3.1.20. *For a group G acting on a set X, we have that*

$$|G| = |Gx||G_x| \qquad \forall x \in X$$

.

Proof. The result would follow if we could find a bijection from Gx to G/G_x, for then $|Gx| = |G/G_x| = |G|/|G_x|$. We do this by taking $y \in Gx$. We take g from G_y, and define a function $\phi(x_1) = gG$ from Gx to G/G_x. The function is independent of the choice of g, for if we also take $f \in G_x$, we see that $g.x = f.x \Rightarrow g^{-1}.(g.x) = g^{-1}.(f.x) = x \Rightarrow g^{-1}.f \in G_x \Rightarrow f \in gG_x$.

We need to first show the injectivity of ϕ. Suppose $y, z \in Gx$, and that $\phi(y) = \phi(z)$, which gives that there are $f, g \in G$ such that $f.x = y, g.x = z$ and $f \in gG_x$, from which we can deduce that there is an element $h \in G_x$ such that $g.h = f$. But then we have that $y = f.x = (g.h).x = g.(h.x) = g.x = z \Rightarrow y = z$. Thus, ϕ must be injective.

To show the surjectivity of ϕ, take a left coset gG_x, and note that $gG_x = \phi(g.x)$. Thus, ϕ is also surjective, therefore bijective, which proves our theorem. □

As a form of error check for our computation of the number of conjugacy classes, we may use the above theorem to see if $|G| = |Gx||G_x|$ for the corresponding orbits Gx. We note that, since the number of transpositions of corners and edges determines the conjugacy class, we can compute each Gx by noting how we choose these transpositions.

For example, the orbits of elements containing just two corner transpositions would contain $\frac{1}{2!}\binom{8}{2}\binom{6}{2}$ elements. The elements with the most multiplicative factors are those containing the most transpositions, that is the largest elements of the even-even and odd-odd permutations of elements permuting both corner and edge pieces.

The largest even-even orbits would have

$$\frac{1}{4!}\binom{12}{2}\binom{10}{2}\binom{8}{2}\binom{6}{2} \cdot \frac{1}{4!}\binom{8}{2}\binom{6}{2}\binom{4}{2}$$

elements, which factors as $3^4 \cdot 5^3 \cdot 7^2 \cdot 11$.

The largest odd-odd orbits would have

$$\frac{1}{5!}\binom{12}{2}\binom{10}{2}\binom{8}{2}\binom{6}{2}\binom{4}{2} \cdot \frac{1}{3!}\binom{8}{2}\binom{6}{2}\binom{4}{2}$$

elements, which factors as $2^3 \cdot 3^5 \cdot 5^2 \cdot 7^2 \cdot 11$.

The cardinality of the Rubik's Cube group G obtained in Theorem 1.3.24 factors as $2^{27}3^{14}5^3 7^2 11$, and we see that $|G|$ is divisible by $|Gx|$ for the largest orbits of elements of order two. The number of elements in these orbits contain the multiplicative factors of the number of elements in the other orbits. Therefore, $|G|$ is divisible by $|Gx|$ for every x of order two, when G acts on x by conjugation.

3.1.8 Isomorphisms to S_3

Finding subgroups of the Rubik's Cube is generally either very tricky or very boring, as many of the subgroups that are easy to find have a very simple structure. One notable, and in the author's opinion interesting, exception is the subgroups one may construct from elements of order two, which are isomorphic to S_3.

Lemma 3.1.21. *Assume a, b as elements of a group G. If a and b are of order two, and ab is of order three, then ba is of order three.*

Proof. We know that $ababab = id$, and therefore conclude that $aba = (bab)^{-1}$, but $(bab)^{-1} = bab$, since a and b are elements of order two. Therefore,

$$ababab = id = (aba)(bab) = (bab)(bab) = (bab)(aba) = bababa$$

and we see that $(ba)^3 = id$. □

We now provide a theorem concerning the structure of the subgroups of the Cube Group which are isomorphic to S_3.

Theorem 3.1.22. *If a, b are elements of the Cube Group, where a, b are of order two, and ab is of order three, then the group generated by a and b will be isomorphic to S_3.*

Proof. S_3 can be generated by the transpositions (1 2) and (2 3). We note that (1 2)(2 3) and (2 3)(1 2) are both of order three, as well as being each others' inverses. Therefore, the mapping $a \to (1\ 2), b \to (2\ 3)$ will be an isomorphism, since ab of order three gives that ba is of order three, according to Lemma 3.1.21, and we also know that $ba = (ab)^{-1}$, since a and b are of order two. □

We now proceed to compute a lower limit to how many subgroups of the Cube Group which are isomorphic to S_3 exist.

Remark 3.1.23. We know that a Cube Group element of order three must be composed of disjoint 3-cycles, where each 3-cycle contains either only corner pieces or only edge pieces.

Lemma 3.1.24. *Any Cube element composed of 3-cycles may be written as a concatenation of two Cube elements of order two.*

Proof. We begin by studying the elements composed of an even number of 3-cycles. We will, without loss of generality, study the element $(x_1x_2x_3)(x_4x_5x_6)$, where x_i are assumed to be distinct cube pieces such that each of the two 3-cycles permutes only corner pieces or only edge pieces. We see that this element is a concantenation of, for example, the two elements $(x_1x_2)(x_4x_5)$

and $(x_2x_3)(x_5x_6)$, these elements being of order two. We also see that an element of order three containing an uneven number of 3-cycles, like $(x_1x_2x_3)(x_4x_5x_6)(x_7x_8x_9)$ can be written as a concatenation of order two elements like $(x_1x_2)(x_4x_5)(x_7x_8)(x_{10}x_{11})$ and $(x_2x_3)(x_5x_6)(x_8x_9)(x_{10}x_{11})$. □

We will now proceed to compute a lower limit of the number of groups isomorphic to S_3, by computing the number of distinct generator pairs whose concatenation is composed of 3-cycles of corner Cube pieces and edge Cube pieces, respectively.

We will define the groups not by choosing the two generators a and b, but instead by defining their concatenation, ab, and accounting for all the possible generator pairs whose concatenation is the element ab.

We choose the elements of the 3-cycles, noting that a maximum of two 3-cycles of corner pieces and a maximum of four 3-cycles of edge pieces may be constructed. We also note that the elements in the 3-cycle may be permuted in 3! ways, yet each 3-cycle will be counted three times in this fashion. Thus, we must multiply by a factor $\frac{3!}{3} = 2$ for each cycle. We also note that S_3 has two elements of order three, so for each group counted, we will have two corresponding elements of order three. Thus, we must divide by a factor two. Thus, an element with n 3-cycles must be multiplied by a factor 2^{n-1}. We also note that the order in which we choose 3-cycles is irrelevant, so for x chosen 3-cycles, we divide by $x!$. We note that we may (and, in the case of an uneven number of 3-cycles, must) add a number of redundant transpositions not contributing to the 3-cycles in the concatenation, provided all of these transpositions are included in both generators, in which case they will cancel each other out during concatenation. We choose these transpositions from the elements not in the 3-cycles, taking care to adhere to the demand for parity, and noting the difference between having redundant transpositions of corner pieces, edge pieces, or both. For n chosen redundant transpositions of corner or edge pieces, we must also divide by $n!$, for the order in which they are choosen does not matter.

We shall now proceed with the promised calculations. The sensitive reader is warned that the calculations involved are slightly tedious.

We begin by choosing the groups concatenating to 3-cycles of corners, after the fashion described above:

$$\frac{1}{2!}\binom{8}{3}\binom{5}{3}2^1 \cdot (1 + (\binom{12}{2}\binom{10}{2}\binom{8}{2}\binom{6}{2}\binom{4}{2}\frac{1}{6!} + \binom{12}{2}\binom{10}{2}\binom{8}{2}\binom{6}{2}\frac{1}{4!} + \binom{12}{2}\binom{10}{2}\frac{1}{2!}) + \binom{2}{2} \cdot (\binom{12}{2}\binom{10}{2}\binom{8}{2}\binom{6}{2}\binom{4}{2}\frac{1}{5!} + \binom{12}{2}\binom{10}{2}\binom{8}{2}\frac{1}{3!} + \binom{12}{2}) + \frac{1}{1!}\binom{8}{3} \cdot (\binom{6}{2} + \binom{12}{2}\binom{10}{2}\binom{8}{2}\binom{6}{2}\binom{4}{2}\frac{1}{5!} + \binom{12}{2}\binom{10}{2}\binom{8}{2}\frac{1}{3!} + \binom{12}{2}) + (\binom{6}{2}\binom{4}{2}\frac{1}{3!} + \binom{6}{2})(\binom{12}{2}\binom{10}{2}\binom{8}{2}\binom{6}{2}\binom{4}{2}\frac{1}{6!} + \binom{12}{2}\binom{10}{2}\binom{8}{2}\binom{6}{2}\frac{1}{4!} + \binom{12}{2}\binom{10}{2}\frac{1}{2!}) + \binom{6}{2}\binom{4}{2}\frac{1}{2!}(\binom{12}{2}\binom{10}{2}\binom{8}{2}\binom{6}{2}\binom{4}{2}\frac{1}{5!} + \binom{12}{2}\binom{10}{2}\binom{8}{2}\frac{1}{3!} + \binom{12}{2})))$$
$$= 2962574720 \approx 2.7 \cdot 10^9$$

After the same fashion, we enumerate the elements forming 3-cycles of only corner pieces:
$\frac{1}{4!}\binom{12}{3}\binom{9}{3}\binom{6}{3}2^3\cdot(1+\binom{8}{2}\binom{6}{2}\binom{4}{2}\frac{1}{4!}+\binom{8}{2}\binom{4}{2}\frac{1}{2!})+\frac{1}{3!}\binom{12}{3}\binom{9}{3}\binom{6}{3}2^2\cdot(\binom{3}{2}+\binom{3}{2}(\binom{8}{2}\binom{6}{2}\binom{4}{2}\frac{1}{4!}+\binom{8}{2}\binom{6}{2}\frac{1}{2!})+((\binom{8}{2}\binom{6}{2}\binom{4}{2}\frac{1}{3!}+\binom{8}{2}))+\frac{1}{2!}\binom{12}{3}\binom{9}{3}2\cdot(1+\binom{6}{2}\binom{4}{2}\frac{1}{2!}+((\binom{8}{2}\binom{6}{2}\binom{4}{2}\frac{1}{4!}+\binom{8}{2}\binom{6}{2}\frac{1}{2!})+((\binom{6}{2}(\binom{8}{2}\binom{6}{2}\binom{4}{2}\frac{1}{3!}+\binom{8}{2}))+\binom{6}{2}\binom{4}{2}\frac{1}{2!}(\binom{8}{2}\binom{6}{2}\binom{4}{2}\frac{1}{4!}+\binom{8}{2}\binom{6}{2}\frac{1}{2!})+\binom{6}{2}\binom{4}{2}\frac{1}{3!}(\binom{8}{2}\binom{6}{2}\binom{4}{2}\frac{1}{3!}+\binom{8}{2}))+\frac{1}{3!}\binom{12}{3}\binom{9}{3}\binom{6}{3}2^2\cdot(\binom{3}{2}+(\binom{8}{2}\binom{6}{2}\binom{4}{2}\frac{1}{3!}+\binom{8}{2}))+\binom{3}{2}(\binom{8}{2}\binom{6}{2}\binom{4}{2}\frac{1}{4!}+\binom{8}{2}\binom{6}{2}\frac{1}{2!}))+\frac{1}{1!}\binom{12}{3}2^0\cdot(((\binom{8}{2}\binom{6}{2}\binom{4}{2}\frac{1}{3!}+\binom{8}{2}))(1+\binom{9}{2}\binom{7}{2}\binom{5}{2}\binom{3}{2}\frac{1}{4!}+\binom{9}{2}\binom{7}{2}\frac{1}{2!})+((\binom{9}{2}\binom{7}{2}\binom{5}{2}\frac{1}{3!}+\binom{9}{2}))\cdot(1+\binom{8}{2}\binom{6}{2}\binom{4}{2}\frac{1}{4!}+\binom{8}{2}\binom{6}{2}\frac{1}{2!}))$
$= 1449131200 \approx 1.5 \cdot 10^9$

We note that these numbers also have to be multiplied by a factor 2^{11}, corresponding to the possible independent edge orientation changes available. Any such change can be included in both generators, and will be negated during concatenation. Summing up, in total we so far have $2^{11} \cdot (1.5 + 2.7) \cdot 10^9 = 8.6106 \cdot 10^{12}$ possible groups.

The inquisitive reader can no doubt surmise the scope of the number of terms involved when computing the number of generator pairs whose concatenation involve both 3-cycles of corner pieces and 3-cycles of edge pieces. For the purpose of this text, that particular calculation has been omitted, and we will contend ourself with the lower limit we have calculated.

We conclude the text by remarking that the Cube subgroups isomorphic to S_3 are at least of the order 10^{12} many, an order of magnitude small in comparison to the total number of elements in the Cube Group, which are of the order 10^{19} many. Yet, this order of magnitude is quite large when compared to the number of elements of order two in the Cube Group, being of the order 10^{11} many.

References

The calculations of the number of elements of order two have been verified with the analogous calculations contained in: David Joyner "Adventures in Group Theory", John Hopkins University Press 2002

The theory concerning cosets and conjugacy classes was written with the help of:
Fraleigh, John B, "A First Course in Abstract Algebra, Seventh Edition", Addison Wesley, 2002

Chapter 4

"An Element of Greatest Order"

by Mikael Hedberg

4.1 Abstract

This paper examines two problems concerning Rubik's Cube. The first problem is the structure of Rubik's Cube which is proven in the end of section one. The second problem is to find the greatest order of an element, this order turned out to be 1260. While analysing the problem of proving the existence of this element, a theorem describing orders inside a general group similar to the one of Rubik's Cube was found.

4.2 Introduction

The paper is divided into two sections.

The first section, devoted to the structure of Rubik's Cube, is a consequence of the group $G = (\mathbb{Z}_3^8 \rtimes_{\varphi_1} S_8) \times (\mathbb{Z}_2^{12} \rtimes_{\varphi_2} S_{12})$. It is known that the abstract group of Rubik's Cube is isomorphic to a proper subgroup of G, thus it's desirable to investigate the possibility of finding an explicit group to which the group of Rubik's Cube is isomorphic. In effect, the outline of investigation is the following:

(1) Start by defining the abstract group of Rubik's Cube.
(2) Continue by proving recognition theorems.
(3) Apply the theorems on subgroups of the Cube.
(4) Iterate the process on the subgroups.

This lead to the theorem below:

Theorem 4.2.1. *Let G_R be the abstract group of Rubik's Cube, then $G_R \cong ((\mathbb{Z}_2^{11} \times \mathbb{Z}_3^7) \rtimes_{\varphi_1} ((A_{12} \times A_8) \rtimes_{\varphi_2} \mathbb{Z}_2))$ where φ_2, φ_1 is left conjugation by $\mathbb{Z}_2$ on $(A_8 \times A_{12})$ and by $(A_{12} \times A_8) \rtimes_{\varphi_2} \mathbb{Z}_2$ on $\mathbb{Z}_2^{11} \times \mathbb{Z}_3^7$ respectively.*

In the second section we are trying to find an element of greatest order inside G_R. The interpretation on the Cube is the following: given a sequence of turns on the Cube, then we know that this sequence can maximally be repeated as many times as the greatest order. Thus, let us continue by stating the theorem concerning this order, and afterwards by giving an outline of the proof.

Theorem 4.2.2. *An element of greatest order in Rubik's Cube has order 1260.*

Outline:
(1) Find a condition for orders of elements in G_R.
(2) Prove a general theorem that especially confines the orders of G_R.
(3) Find a way to express the orders in the mothergroup G of G_R.
(4) Find the supremum of the set of orders of the mothergroup.
(5) Prove the existence of an element having this order inside G_R.

A consequence of (2) in the outline is Theorem 4.4.4, affirming the fact that the orders of elements inside the generalised symmetric group[1] can be obtained by almost explicitly regarding the orders of the permutations.

[1] David Joyner, Adventures in Group Theory: Rubik's Cube, Merlin's Machine, and Other Mathematical Toys. Page 194, Example 9.7.3 [2008-15-05]

4.3 The abstract group of Rubik's Cube

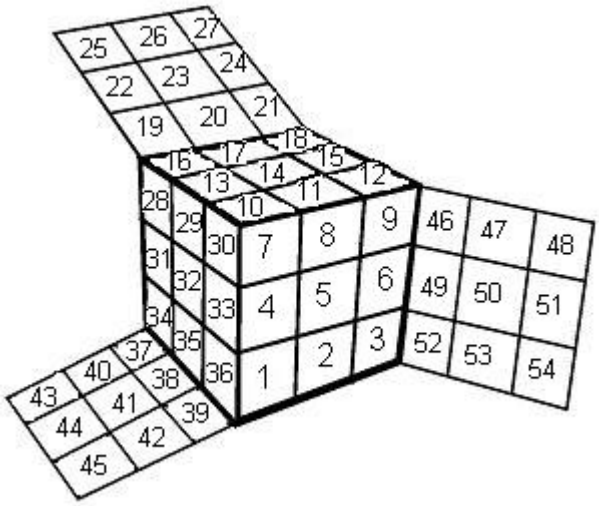


Figure 4.1: Facets with corresponding indexes

Let us start by defining the abstract group of Rubik's Cube, but first, some preparatory manoeuvres are needed. Adequately, fix the cube in space (since the symmetry of the cube itself is hardly relevant), then index all the facets with numbers 1 to 54 according to Figure 4.1. Afterwards, define the binary operator to be turnings of the layers, this is equivalent of saying: permutations of the indexes given by the corresponding turns of layers. Let F,B,U,D,R and L be the turns given on Page 1.3, then this will correspond to the permutations below.

$$\begin{aligned}
&\text{F} = (1,7,9,3)(2,4,8,6)(10,46,45,36)(30,12,52,39)(11,49,42,33)\\
&\text{B} = (19,25,27,21)(20,22,26,24)(16,34,43,48)(28,37,54,18)(17,31,40,51)\\
&\text{U} = (10,16,18,12)(11,13,17,15)(7,28,21,46)(30,19,48,9)(29,20,47,8)\\
&\text{D} = (43,37,39,45)(44,40,38,42)(1,52,21,34)(36,3,54,25)(2,53,26,35)\\
&\text{R} = (46,48,54,52)(47,51,53,49)(3,12,21,43)(45,9,18,27)(6,15,24,44)\\
&\text{L} = (28,30,36,34)(29,33,35,31)(1,37,19,10)(39,25,16,7)(13,4,38,22)
\end{aligned} \tag{4.3.1}$$

Definition 4.3.1. The abstract group of Rubik's Cube is the subgroup $G_R = \langle F, B, U, D, R, L \rangle \leq S_{54}$

Remark 4.3.2. According to the above definition $G_R \leq S_{54}$. This can be strengthened observing that the middle pieces do not move, hence $G_R \leq S_{48}$

Now when the abstract group of Rubik's Cube is defined, it's time to investigate if there is an explicit group to which G_R is isomorphic. Thus, let us continue by two definitions, afterwards moving on to proving some theorems that will help us with the recognition of the abstract group.

Definition 4.3.3. Let H and K be subsets of a group G, HK is then defined by $HK = \{hk \in G \,|\, h \in H, k \in K\}$.

Definition 4.3.4. Let G be a group and $K \leq G$. Recall that for any $g \in G$, $gKg^{-1} = \{gkg^{-1} \,|\, k \in K\}$. The normaliser of K in G is defined by $N_G(K) = \{g \in G \,|\, gKg^{-1} = K\}$.

Theorem 4.3.5. *If H and K are subgroups of a group G, then $HK \leq G$ if and only if $HK = KH$.*

Proof. Let H, $K \leq G$ and assume HK is a subgroup. Take $hk \in HK$, since HK is a subgroup we know that $k^{-1}h^{-1} \in HK$. But $k^{-1}h^{-1} \in KH$ which means that $HK \subseteq KH$. The reverse containment is similair, proving the right implication.
Now for the reverse statement assume that $HK = KH$. Take some $a, b \in HK$, then we know from the definition of HK that $a = h_1k_1$, $b = h_2k_2$ for $h_1, h_2 \in H$ and $k_1, k_2 \in K$. Thus $ab = h_1k_1h_2k_2 = h_1h_3k_3k_2$ where $k_1h_2 = h_3k_3 \in HK$ since $HK = KH$. But $h_1h_3 = h_4 \in H$ and $k_3k_2 = k_4 \in K$ since H and K are subgroups. Hence $ab = h_1k_1h_2k_2 = h_1h_3k_3k_2 = h_4k_4 \in HK$ and HK is closed. The fact that HK contains an inverse for each $a \in HK$ is due to $a^{-1} = k^{-1}h^{-1} \in KH = HK$. Thus $HK \leq G$.

□

Corollary 4.3.6. *If $H \leq N_G(K)$ then $HK \leq G$.*

Proof. Assume it holds, then $HK = \{hk \,|\, h \in H,\, k \in K\} = \{(hkh^{-1})h \,|\, h \in H,\, k \in K\} \subseteq KH$. The reverse containment is similar. □

Now we are prepared to prove the two recognition theorems. The first theorem will recognise direct products and the second will recognise semidirect products, where the homomorphism to the automorphism group will be given by left conjugation. Before doing this, a lemma is needed.

Lemma 4.3.7. *Let H and K be subgroups of a group G. The number of distinct ways of writing each element in HK on the form hk, for some $h \in H$ and $k \in K$ is $|H \cap K|$.*

Proof. Take some $a \in HK$ and we know from the definition of HK that $a = hk$, $h \in H$, $k \in K$. It is clear that $H \cap K \neq \emptyset$ since id is in both H and K. Now, if we take any $b_i \in H \cap K$ then b_i can be written as $\tilde{h}_i$ or as $\tilde{k}_i$. Thus for $hk \in HK$, $hk = h\tilde{h}_i\tilde{h}_i^{-1}k = (h\tilde{h}_i)(\tilde{k}_i^{-1}k)$. This equality holds for $|H \cap K|$ different b_i in the intersection $H \cap K$. Let us now show that this

equality holds only for elements in the intersection. Take any $c \in G$ where $c \notin H \cap K$, then $hk = (hc)(c^{-1}k)$. To be written differently it's necessary that $c^{-1}k \in K$, $hc \in H$. But since $c \notin H \cap K$ we know that either $c^{-1}k \notin K$ or $hc \notin H$ because one of them will be in a coset not equal to the group itself. This is a contradiction, thus we have $|H \cap K|$ different ways of writing $hk \in HK$. □

Theorem 4.3.8. *Suppose G is a group and H, K subgroups. If*

(1) $H, K \trianglelefteq G$ *and*
(2) $|H \cap K| = 1$,

then $G \geq HK \cong (H \times K)$

Proof. Suppose (1) and (2) holds. HK forms a subgroup by Corollary 4.3.6 since obviously $H \leq N_G(K) = G$. Define $\varphi : HK \to H \times K$ by $hk \mapsto (h, k)$. Observe that condition (2) in Lemma 4.3.7 makes this well defined. Before proving this is a homomorphism we observe that $k^{-1}(hkh^{-1}) \in K$ but $(k^{-1}hk)h^{-1} \in H$, hence (2) implies $k^{-1}hkh^{-1} = id \Leftrightarrow hk = kh$. Now $\varphi(h_1k_1h_2k_2) = \varphi(h_1h_2k_1k_2) = (h_1h_2, k_1k_2) = \varphi(h_1k_1)\varphi(h_2k_2)$. The fact that φ is a bijection is due to $ker(\varphi) = \{id\} \Rightarrow \varphi$ injective and by definition φ is surjective. □

Theorem 4.3.9. *Suppose G is a group and N, K subgroups. If*

(1) $N \trianglelefteq G$ *and*
(2) $|N \cap K| = 1$,

then $G \geq NK \cong (N \rtimes_\varphi K)$ *where* $\varphi : K \to Aut(N)$ *such that* $\varphi(k)$ *equals left conjugation on N by k.*

Proof. Assume (1) and (2) holds. We know from Corollary 4.3.6 as in the above proof that NK forms a subgroup. Let $\xi : NK \to N \rtimes_\varphi K$ by $nk \mapsto (n, k)$, ξ is well defined like in the proof above. Now we show that this mapping is a homomorphism. $\xi((h_1k_1)(h_2k_2)) = \xi(h_1(k_1h_2k_1^{-1})k_1k_2) = \xi(h_1h_3k_1k_2) = (h_1h_3, k_1k_2) = (h_1(k_1h_2k_1^{-1}), k_1k_2) = (h_1\varphi(k_1)(h_2), k_1k_2) = (h_1, k_1)(h_2, k_2) = \xi(h_1k_1)\xi(k_2h_2)$. From the very definition of ξ it's clear that ξ is bijective. □

Definition 4.3.10. Let N, K, G be according to the above theorem.
If $NK = G$ then K is called a complement of N.

Now when all preparations are done, we can start looking at the actual structure of G_R. In order to do this, we begin by noting that the set of all orientation changes, referred to as flips, is a normal subgroup $\mathcal{F}$ of G_R. This will be proved, and afterwards we try to find a complement $\mathcal{P} \leq G_R$ of $\mathcal{F}$. Hence by Theorem 4.3.9 we can split G_R itself into a semidirect product.

Proposition 4.3.11. *The nonempty set $\mathcal{F} \subseteq G_R$ consisting of all possible flips and the identity, without permuting the cubies, forms a normal subgroup in G_R.*

Proof. It is clear from Lemma 1.3.21, Lemma 1.3.22 that $\mathcal{F} \neq \emptyset$. Furthermore $\mathcal{F} \leq G_R$, since for all $f_1, f_2 \in \mathcal{F}$ we know that $f_1 f_2$ flips edges or corners and that $f_1 f_2$ can not permute cubies. Hence $f_1 f_2 \in \mathcal{F}$ and since G_R is finite this implies $\mathcal{F} \leq G_R$. Suppose $\mathcal{F}$ is not normal, then we have at least one $g \in (G_R \setminus \mathcal{F})$, $f \in \mathcal{F}$ such that $gfg^{-1} \notin \mathcal{F}$.
This is clearly a contradiction since g permutes cubies and therefore g^{-1} permutes them back, leaving $gfg^{-1} \in \mathcal{F}$. □

Now it's desirable to find a complement of $\mathcal{F}$. We know from Lemma 1.3.13 that all the allowed corner and edge permutations can be generated, but the elements corresponding to this are far from unique. Thus, if we can pick a subset of all the allowed permutations respecting the orientations in Figure 4.2, we can be sure that this set will form a complement of $\mathcal{F}$ since the permutations don't flip any corner/edges in accordance with the given definition. This observation needs however a proof.

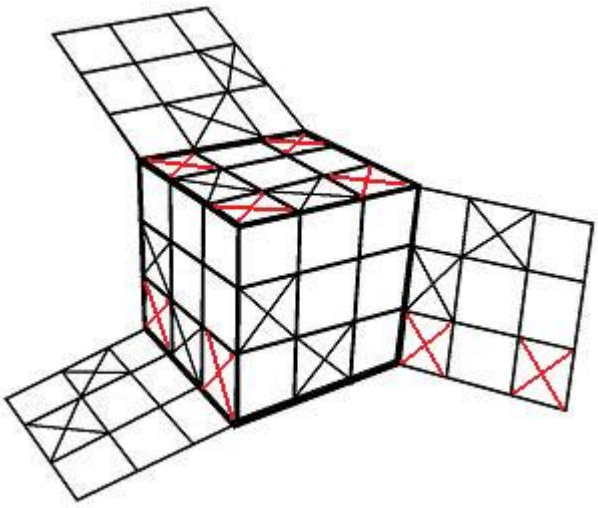


Figure 4.2: Red cross for corner orientation and black cross for edge orientation

Proposition 4.3.12. *The nonempty set $\mathcal{P} \subseteq G_R$ of corner/edge permutations respecting the orientations in Figure 4.2 forms a complement of $\mathcal{F}$.*

Proof. Firstly, we prove that $\mathcal{P}$ is a subgroup and that it contains all the permutations of corners/edges according to Lemma 1.3.13 in the common part. The only difference is that the permutations are contained in this orientation. In effect, we know from Lemma 1.3.13 that we can obtain all the pairs $(\sigma_C, \sigma_E) \in S_8 \times S_{12}$ where σ_E, σ_C must have the same sign (recall that we can't establish other permutations). Thus, reconstruct the proof of Lemma 1.3.13 with 3-cycles contained in the orientation in accordance with Figure 4.2 and observe that this can always be done due to the proof of Lemma 1.3.21 and of Lemma 1.3.22. Now, let $\mathcal{P}$ be the set of the newly constructed permutations (obviously nonempty). Thus $\tau_1, \tau_2 \in \mathcal{P}$ and since both τ_1, τ_2 are contained in the orientation according to Figure 4.2, we know that $\tau_1\tau_2 \in \mathcal{P}$. Hence $\mathcal{P} \leq G_R$ since G_R is finite.
Secondly, let us prove that $|\mathcal{P} \cap \mathcal{F}| = 1$ and $\mathcal{P}\mathcal{F} = G_R$. $|\mathcal{P} \cap \mathcal{F}| = 1$ is clear since the only element in common is the identity. Finally, recall that $|\mathcal{P}| = \frac{8!12!}{2}$, $|\mathcal{F}| = 2^{11}3^7$ and since $|\mathcal{P}\mathcal{F}| = |\mathcal{P}||\mathcal{F}| = 3^7 2^{10} 8!12! = |G_R|$ according to the proof of Theorem 1.3.24, we know that $\mathcal{P}\mathcal{F} = G_R$. Hence $\mathcal{P}$ is a complement of $\mathcal{F}$. □

Corollary 4.3.13. *$G_R \cong \mathcal{F} \rtimes_\varphi \mathcal{P}$ where φ is left conjugation by $\mathcal{P}$ on $\mathcal{F}$.*

Proof. Apply Theorem 4.3.9. □

Remark 4.3.14. It is interesting to note that this complement is far from unique. We know that it is possible to find at least $2^{11}3^7$ different complements. So, how many are they?

Neither $\mathcal{F}$ nor $\mathcal{P}$ gives much information about the group G_R itself. Continuing in the same manner with the subgroups $\mathcal{F}$ and $\mathcal{P}$ we can hopefully obtain a more "enlightened" group.

Definition 4.3.15. Let $\vec{v} \in \mathbb{Z}_k^n$ then $sum(\vec{v}) = \sum_{i=1}^n c_i$ where c_i is the coordinate i in $\vec{v}$.

Proposition 4.3.16. *$\mathcal{F}$ is isomorphic to the abelian group $\mathbb{Z}_3^7 \times \mathbb{Z}_2^{11}$.*

Proof. Let C, E be the sets of corner rotations and edge rotations respectively. These are obviously two subgroups of $\mathcal{F}$, where both of them are normal and $|E \cap C| = 1$. Using the same definition of the orientations as before, we know from Proposition 1.3.17, Proposition 1.3.19 in the common part that $C = \{\vec{c} \in \mathbb{Z}_3^8 \,|\, sum(\vec{c}) = 0\}$ and $E = \{\vec{e} \in \mathbb{Z}_2^{12} \,|\, sum(\vec{e}) = 0\}$. For $\vec{c_1}, \vec{c_2} \in C$ we have that $sum(\vec{c_1} + \vec{c_2}) = sum(\vec{c_1}) + sum(\vec{c_2}) = 0$. Thus $\vec{c_1} + \vec{c_2} \in C$ and C forms a subgroup of $\mathbb{Z}_3^8$. But the only isomorphic alternative for C is $\mathbb{Z}_3^7$ since $|C| = 3^7$ by Lemma 1.3.22 and the fundamental theorem of finitely generated abelian groups gives the rest. An equivalent calculation

shows the same for E. Thus since $|EC| = |E||C| = 2^{11}3^7 = |\mathcal{F}|$ by the proof of Theorem 1.3.24 in the common part we know $\mathcal{F} \cong E \times C \cong \mathbb{Z}_2^{11} \times \mathbb{Z}_3^7$. □

Now it is also desireable to look at the structure of the group $\mathcal{P}$.

Proposition 4.3.17. *$\mathcal{P}$ is isomorphic to $(A_8 \times A_{12}) \rtimes_\varphi \mathbb{Z}_2$ where φ is left conjugation by $\mathbb{Z}_2$ on $(A_8 \times A_{12})$.*

Proof. We know from the proof of Lemma 1.3.13 in the common part that a subgroup of even permutations only permuting edges is isomorphic to A_{12} and that another subgroup of even permutations only permuting corners is isomorphic to A_8. Denote the isomorphic copies inside $\mathcal{P}$ by E and C respectively. It is clear that subgroups only permuting edges exclusively or corners are normal inside $\mathcal{P}$ and that $E \cap C = 1$. Thus $P \geq EC \cong A_8 \times A_{12}$ according to Theorem 4.3.8. It is immediate that $A_8 \times A_{12}$ is normal inside $\mathcal{P}$ since it has index 2 (recall that $|\mathcal{P}| = 8!12!\frac{1}{2}$ from the proof of Theorem 1.3.24, common part). But now we want a complement $K \leq \mathcal{P}$ such that $|A_8 \times A_{12} \cap K| = 1$. Consequently, K can be the subgroup generated by any odd permutation of order two inside $\mathcal{P}$; to be precise, this means that the pair $(\sigma_C, \sigma_E) \in S_8 \times S_{12}$ according to Lemma 1.3.13 is odd and that it has order 2. Hence $|(A_8 \times A_{12}) \cap K| = 1$ since K contains the identity and an odd permutation. Furthermore we know that $K \cong \mathbb{Z}_2$ since it is cyclic. Thus, $|(EC)K| = |E||C||K| = 8!12!\frac{1}{2} = |\mathcal{P}|$ and by Theorem 4.3.9 we know that $(EC)K \cong (A_8 \times A_{12}) \rtimes_\varphi \mathbb{Z}_2$ where φ is left conjugation by $\mathbb{Z}_2$ on $(A_8 \times A_{12})$. □

Thanks to all of the calculations above the proof of the theorem below is very short. The theorem shows the structure of Rubik's Cube.

Theorem 4.3.18. *Let G_R be the abstract group of Rubik's Cube, then $G_R \cong ((\mathbb{Z}_2^{11} \times \mathbb{Z}_3^7) \rtimes_{\varphi_1} ((A_{12} \times A_8) \rtimes_{\varphi_2} \mathbb{Z}_2))$ where φ_2, φ_1 is left conjugation by $\mathbb{Z}_2$ on $(A_8 \times A_{12})$ and by $(A_{12} \times A_8) \rtimes_{\varphi_2} \mathbb{Z}_2$ on $\mathbb{Z}_2^{11} \times \mathbb{Z}_3^7$ respectively.*

Proof. Firstly, it's known from Corollary 4.3.13 that $G_R \cong \mathcal{F} \rtimes_{\phi_1} \mathcal{P}$ where ϕ_1 is left conjugation. Secondly, we know that $\mathcal{F} \cong \mathbb{Z}_3^7 \times \mathbb{Z}_2^{11}$ according to Proposition 4.3.16. Lastly, $\mathcal{P} \cong (A_8 \times A_{12}) \rtimes_{\varphi_2} \mathbb{Z}_2$ in accordance with Proposition 4.3.17. Thus $G_R \cong ((\mathbb{Z}_2^{11} \times \mathbb{Z}_3^7) \rtimes_{\varphi_1} ((A_{12} \times A_8) \rtimes_{\varphi_2} \mathbb{Z}_2)$ which proves the theorem. □

4.4 An element of greatest order

Let us begin this section by writing out the Theorem which is the main result.

Theorem 4.4.1. *An element of greatest order in Rubik's Cube has order 1260.*

The mothergroup of a group G is a group in which G is contained. Now recall from the introduction that the outline, in order to prove the theorem, is the following:

(1) Find a condition for orders of elements in G_R.
(2) Prove a general theorem that especially confines the orders of G_R.
(3) Find a way to express the orders in the mothergroup of G_R.
(4) Find the supremum of the set of orders of the mothergroup.
(5) Prove the existence of an element having this order inside G_R.

In effect, let us summarise some facts about Rubik's Cube that are helpful in the quest of finding an element of greatest order. Afterwards, the general theorem describing orders in the mothergroup of G_R will be written out. The theorem is important in the sense of confining the possible orders in Rubik's Cube.

Let $(\vec{v},\sigma),(\vec{u},\tau) \in (\mathbb{Z}_3^8 \rtimes_\varphi S_8)$, we know from Page 1.3.3

$$(\vec{v},\sigma) *_\varphi (\vec{u},\tau) = (\vec{v} + \varphi_\sigma(\vec{u}), \sigma\tau) \tag{4.4.1}$$

where φ_σ acts as a permutation on the coordinates according to σ^{-1}. This notation is a bit tedious, therefore we will denote $\varphi_\sigma(\vec{u})$ by $\sigma.\vec{u}$. It is exactly the same for any element in $\mathbb{Z}_2^{12} \rtimes_\varphi S_{12}$. Furthermore, we know from Theorem 1.3.23 that $G_R \leq (\mathbb{Z}_3^8 \rtimes_{\varphi_1} S_8) \times (\mathbb{Z}_2^{12} \rtimes_{\varphi_2} S_{12})$ where $(\vec{v},\sigma,\vec{u},\tau) \in (\mathbb{Z}_3^8 \rtimes_{\varphi_1} S_8) \times (\mathbb{Z}_2^{12} \rtimes_{\varphi_2} S_{12})$ is in G_R if and only if:

$$\begin{array}{ll} (1) & sgn(\sigma) = sgn(\tau) \\ (2) & sum(\vec{v}) = 0 \\ (3) & sum(\vec{u}) = 0 \end{array} \tag{4.4.2}$$

Equation 4.4.1 implies quickly a condition for an element of order d in each coordinate of the direct product. Let $(\vec{v},\sigma) \in \mathbb{Z}_3^8 \rtimes_{\varphi_1} S_8$ and $(\vec{u},\tau) \in \mathbb{Z}_2^{12} \rtimes_{\varphi_2} S_{12}$, then

$$\begin{array}{l} \vec{v} + \sigma.\vec{v} + \cdots + \sigma^{d_1-1}.\vec{v} = \vec{0}\ ,\ \sigma^{d_1} = id \\ \vec{u} + \tau.\vec{u} + \cdots + \tau^{d_2-1}.\vec{u} = \vec{0}\ ,\ \tau^{d_2} = id \end{array} \tag{4.4.3}$$

Now when we have a bit of information about the problem of actually determining the greatest order of an element, we continue by writing out the

theorem mentioned in the beginning of this section. Before doing this, it is worth stressing the importance of this theorem. Recall from Equation 4.4.3 that in order to have an element of a certain order, it's necessary that the sum in Equation 4.4.3 is equal to the zero vector. If all the values d_1,d_2 for which the sum is the zero vector are known, it is an easy task to calculate the least common multiple of the orders of the permutations, and of the given values d_1,d_2. Effectively, let us continue by confining the values for which the sum is the zero vector when the permutation is a cycle.

Theorem 4.4.2. *Let $n, k \in \mathbb{N} \setminus \{0\}$, $k \geq 2$ and let σ be a n-cycle in S_n.*
(1) If d is any positive divisor of nk, then there exists at least one $\vec{v} \in \mathbb{Z}_k^n$ such that $\sum_{i=0}^{d-1} \sigma^i.\vec{v} = \vec{0}$ and $\sum_{i=0}^{q-1} \sigma^i.\vec{v} \neq \vec{0}$ for $0 < q < d$.
(2) Let $\vec{u} \in \mathbb{Z}_k^n$. If $d \neq 0$ is the smallest positive integer such that $\sum_{i=0}^{d-1} \sigma^i.\vec{u} = \vec{0}$, then $d \mid nk$.

Proof. Part (1), assume that $d \mid nk$ and $\sigma = (12\ldots n)$. The statement will be divided in two cases and afterwards generalised to an arbitrary n-cycle.

(a) $d = n_1 k_1$ where $n_1 \mid n$ and $k_1 \mid k$ such that $k_1 \neq 1$.
Now, let $x \in \mathbb{Z}_k$ such that $|x| = k_1$; this is possible since $\mathbb{Z}_k$ is cyclic. Consider the vector $\vec{v} = (\underbrace{\underbrace{0,\ldots,x}_{\text{length } n_1}, \underbrace{0,\ldots,x}_{\text{length } n_1}, \ldots \underbrace{0,\ldots,x}_{\text{length } n_1}}_{\text{length n}})$ and observe that $\vec{v}$ can always be constructed since $n_1 \mid n$. From the fact that $\sigma = (12\ldots n)$, it's clear that $\sum_{i=0}^{n_1-1} \sigma^i.\vec{v} = (x, x, \ldots, x)$. Furthermore, since $|x| = k_1$ we know that $\sum_{i=0}^{n_1 k_1 - 1} \sigma^i.\vec{v} = k_1(x, x\ldots, x) = \vec{0}$ and that $\sum_{i=0}^{a-1} \sigma^i.\vec{v} \neq \vec{0}$ for $0 < a < n_1 k_1$. Hence the statement holds for conditions under (a) with the given σ.

(b) $d = n_1$ where $n_1 \mid n$.
Here it's necessary to choose a vector differently from the case (a). If $d \neq 1$, then let $x \in \mathbb{Z}_k$ and $x \neq 0$. Now, consider the vector:

$$\vec{v} = (\underbrace{\underbrace{0,\ldots,-x,x}_{\text{length d}}, \underbrace{0,\ldots,-x,x}_{\text{length d}}, \ldots \underbrace{0,\ldots,-x,x}_{\text{length d}}}_{\text{length n}})$$

and we see directly that $\sum_{i=0}^{d-1} \sigma^i.\vec{v} = \vec{0}$ and that $\sum_{i=0}^{b-1} \sigma^i.\vec{v} \neq \vec{0}$ for $0 < b < d$. If $d = 1$, then $\vec{v} = \vec{0}$ which is the trivial case. Hence the statement holds for conditions under (b) with the given σ.

To generalise the above proof for a general n-cycle τ, let us note that $\tau = \alpha\sigma\alpha^{-1}$ since σ and τ have the same type$(\sigma, \tau, \alpha \in S_n)$. Let $\vec{u} \in \mathbb{Z}_k^n$ and note also that if $\sum_{i=0}^{d-1} \sigma^i(\alpha^{-1}.\vec{u}) = \vec{0}$, then $\sum_{i=0}^{d-1} \tau^i.\vec{u} = \alpha(id + \sigma +$

$\cdots + \sigma^{d-1})\alpha^{-1}.\vec{u} = \vec{0}$. Thus let $\vec{u} = \alpha.\vec{v}$, which proves the statement in the general case.

Part (2), assume that $\vec{v} \in \mathbb{Z}_k^n$ and $\sigma \in S_n$. Let $P_n(\sigma) = 1 + \sigma + ... + \sigma^{n-1}$ denote a polynomial in σ, and $P_0(\sigma) = 0$. Let a, b be positive integers such that $d = ab$, then we know that $P_n(\sigma) = P_a(\sigma^b)P_b(\sigma) = P_b(\sigma^a)P_a(\sigma)$. Let $n = mq + r$ where m, q, r integers such that $0 \leq r < q$. If $P_q(\sigma)(\vec{v}) = \vec{0}$ then $P_{mq}(\sigma)(\vec{v}) = P_m(\sigma^q)P_q(\sigma)(\vec{v}) = 0 \Rightarrow \sigma^r P_{mq}(\sigma)(\vec{v}) = \vec{0}$. This means that if $P_d(\sigma)(\vec{v}) = \vec{0}$ and $P_q(\sigma)(\vec{v}) = \vec{0}$, then $P_d(\sigma)(\vec{v}) = \underbrace{\sigma^r P_{mg}(\sigma)(\vec{v})}_{=\vec{0}} + P_r(\sigma)(\vec{v}) = \vec{0} \Rightarrow P_r(\sigma)(\vec{v}) = \vec{0}$. Effectively, let $P_d(\sigma)(\vec{v}) = \vec{0}$ and d_0 be the smallest integer such that $P_{d_0}(\sigma)(\vec{v}) = \vec{0}$, then $P_d(\sigma)(\vec{v}) = \sigma^r P_{qd_0}(\sigma)(\vec{v}) + P_r(\sigma)(\vec{v}) = \vec{0}$ $(0 \leq r < d_0)$. But since d_0 is the smallest integer, this forces $r = 0$, hence $d_0 \mid d$.

Now let us look at $P_{nk}(\sigma)(\vec{v})$, we know that $P_{nk}(\sigma)(\vec{v}) = P_k(\sigma^n)P_n(\sigma)(\vec{v}) = P_k(1)P_n(\sigma)(\vec{v}) = kP_n(\sigma) = \vec{0}$ since $\vec{v} \in \mathbb{Z}_k^n$. But this means that if we let $d_0 \geq 1$ be the smallest positive integer such that $P_{d_0}(\sigma)(\vec{v}) = \vec{0}$, then $d_0 \mid nk$. This proves the second statement of the theorem.

□

A natural question is now, if it's possible to generalise the above theorem for any permutation $\sigma \in S_n$. This is indeed the case, but first we need a lemma.

Lemma 4.4.3. *Let $n, c_i \in \mathbb{N} \setminus \{0\}$ and let $l = lcm(c_1, c_2, \ldots, c_s)$.*
If $A = \{lcm(d_1, d_2, \ldots, d_s) : d_i \mid c_i n\}$ and $B = \{k \in \mathbb{N} \setminus \{0\} : k \mid ln\}$, then $B = A$.

Proof. We will show that $A \subseteq B$ and $B \subseteq A \Leftrightarrow A = B$.

$$lcm(c_1 n, c_2 n, \ldots, c_s n) = lcm(\ldots lcm(lcm(c_1 n, c_2 n), c_3 n) \ldots, c_s n) \quad \Leftrightarrow$$
$$lcm(c_1 n, c_2 n, \ldots, c_s n) = lcm(\ldots lcm(n \cdot lcm(c_1, c_2), c_3 n) \ldots, c_s n) \quad \Leftrightarrow$$
$$lcm(c_1 n, c_2 n, \ldots, c_s n) = n \cdot lcm(c_1, c_2, \ldots, c_s) = ln.$$

Take an $a = lcm(d_1, d_2, \ldots, d_s) \in A$, but $d_i \mid c_i n$ which means that a must divide $lcm(c_1 n, c_2 n, \ldots, c_s n) = ln$, thus $A \subseteq B$.
Let $b \in B$, by definition we know that $b \mid ln$. Therefore, let $b = n_1 l_1$ where $n_1 \mid n$ and $l_1 \mid l$. It is obvious that if $l = lcm(c_1, c_2, \ldots, c_s)$, then $l_1 = lcm(\tilde{c}_1, \tilde{c}_2, \ldots, \tilde{c}_s)$ where $\tilde{c}_i \mid c_i$. In effect, let us choose $k_i = n_1 \tilde{c}_i$ which implies that $b = lcm(k_1, k_2, \ldots, k_s) = lcm(n_1\tilde{c}_1, n_1\tilde{c}_2, \ldots, n_1\tilde{c}_s) = n_1 lcm(\tilde{c}_1, \tilde{c}_2, \ldots, \tilde{c}_s) = n_1 l_1$. But $k_i \mid nc_i$, thus $b \in A \Rightarrow B \subseteq A$ and hence $A = B$. □

Theorem 4.4.4. *Let $n, k \in \mathbb{N} \setminus \{0\}$ and let $\sigma \in S_n$ where $s = |\sigma|$.*
(1) If d is any positive divisor of sk, then there exists at least one $\vec{v} \in \mathbb{Z}_k^n$ such that $\sum_{i=0}^{d-1} \sigma^i.\vec{v} = \vec{0}$ and $\sum_{i=0}^{q-1} \sigma^i.\vec{v} \neq \vec{0}$ for $0 < q < d$.

(2) Let $\vec{u} \in \mathbb{Z}_k^n$. If $d \neq 0$ is the smallest positive integer such that $\sum_{i=0}^{d-1} \sigma^i.\vec{u} = \vec{0}$, then $d \mid sk$.

Proof. Part (1): If $\vec{v} \in \mathbb{Z}_k^n$, then we can partition the coordinates in $\vec{v}$ according to the orbits of σ. A cell of the partition of $\vec{v}$ will be denoted subvector of $\vec{v}$. Thus, we know that $\sum_{i=0}^{d-1} \sigma^i.\vec{v} = \vec{0}$ when the corresponding sums of all the subvectors of $\vec{v}$ are zero, because they permute internally according to the cycles of σ. Hence from Theorem 4.4.2 we know that we can establish a subvector of $\vec{v}$ for each divisor q of kr ,where r is the size of the orbit, such that the subvector is zero in the sum $\sum_{i=0}^{q-1} \sigma^i.\vec{v}$ and nonzero in $\sum_{i=0}^{c-1} \sigma^i.\vec{v}$ where $0 < c < q$. Thus, we can construct a vector $\vec{u} \in \mathbb{Z}_k^n$ for each $a \in A = \{lcm(d_1, d_2, \ldots, d_m) : d_i \mid c_i k\}$ where c_i is the size of an orbit corresponding to a subvector, such that $\sum_{i=0}^{a-1} \sigma^i.\vec{u} = \vec{0}$ and that $\sum_{i=0}^{c-1} \sigma^i.\vec{u} \neq \vec{0}$, $0 < c < a$. But from Lemma 4.4.3 we know that $A = \{z \in \mathbb{N} \setminus \{0\} : z | sk\}$ since $s = lcm(c_1, ...c_m)$. This proves the statement.

Part (2) is proved in Theorem 4.4.2.

□

Remark 4.4.5. Knowing that the theorem is true, it gives very nice conditions for orders of elements in the group $(\mathbb{Z}_3^8 \rtimes_{\varphi_1} S_8) \times (\mathbb{Z}_2^{12} \rtimes_{\varphi_2} S_{12})$. Maybe it is possible to prove a similar theorem applieable to G_R? That is, to take into account that the vector sums is zero. This can be examined by regarding the vectors in the proof of Theorem 4.4.2.

Finally it's time to investigate an element of greatest order in G_R. What is done in the previous page is actually to give a general condition not only applicable to G_R. Of course we can't apply the conditions in Theorem 4.4.4 directly to describe all the possible orders of elements in Rubik's Cube, since we can't guarantee the existence of $\vec{v}$ in the theorem. But what we can do is to describe all the orders of the group in which G_R is contained, thus making it plausable that maybe, if we find an element of greatest order in $(\mathbb{Z}_3^8 \rtimes_{\varphi_1} S_8) \times (\mathbb{Z}_2^{12} \rtimes_{\varphi_2} S_{12})$, then this element is found in G_R. Let us start with the general question of determining all possible orders of the mothergroup of G_R.

Definition 4.4.6. The set of induced orders by $\sigma \in S_n$ in $\mathbb{Z}_k^n$ is $D_\sigma = \{z \in \mathbb{N} \setminus \{0\} : z \text{ divides } k|\sigma|\}$

Example 3. Let $G = (\vec{v}, \sigma) \in \mathbb{Z}_3^8 \rtimes_{\varphi_1} S_8$ where $\vec{v}$ is arbitrary and $\sigma = (12345)(67) \Rightarrow |\sigma| = 10$. Let us now study powers of $(\vec{v}, \sigma)$. We know that $(\vec{v}, \sigma)^{d_1} = (\vec{0}, id) \Leftrightarrow (\vec{v} + \sigma.\vec{v} + \cdots + \sigma^{d_1 - 1}.\vec{v}, \sigma^{d_1}) = (\vec{0}, id)$. But the left coordinate is exactly the sum given in Theorem 4.4.4, hence we know directly for which d_1 the sum is $\vec{0}$. The values are in this case all the divisors of $3 * 10 = 30$, since according to Theorem 4.4.4 (1), there is a $\vec{v}$ for each $d|30$ such that $\vec{v} + \sigma.\vec{v} + \cdots + \sigma^{d-1}.\vec{v} = \vec{0}$ ($\neq \vec{0}$ for values less than d).

Furthermore, according to (2) we know that there can not exist a vector $\vec{v}$ such that $\vec{v}+\sigma.\vec{v}+\cdots+\sigma^{q-1}.\vec{v}=\vec{0}$ and q is not a divisor of 30. This implies that if we want to study orders of elements inside G, we can just look at the least common multiple between the order of σ and members of the set of induced orders by σ.

A direct consequence of this example is the theorem below.

Theorem 4.4.7. *Let $G=(\mathbb{Z}_3^8 \rtimes_{\varphi_1} S_8)\times(\mathbb{Z}_2^{12} \rtimes_{\varphi_2} S_{12})$ and $\sigma \in S_8$, $\tau \in S_{12}$. Furthermore let D_σ,D_τ be the sets of induced orders by σ and by τ in $\mathbb{Z}_3^8$, $\mathbb{Z}_2^{12}$ respectively, then:*
(1) the set $O_{\sigma,\tau}=\{lcm(lcm(d_\sigma,|\sigma|),lcm(d_\tau,|\tau|)) : d_\sigma \in D_\sigma, d_\tau \in D_\tau\}$ contains all the possible orders given by σ and by τ, and consequently
(2) the set $\mathcal{O}=\bigcup_{\sigma\in S_8,\tau\in S_{12}} O_{\sigma,\tau}$ contains all the possible orders of G.

Proof. Part (1), let $\vec{v}\in\mathbb{Z}_3^8$ and $\vec{u}\in\mathbb{Z}_2^{12}$ be two arbitrary vectors. It's known from Condition 4.4.3 that $(\vec{v},\sigma)^d=(\vec{0},id)\Leftrightarrow(\vec{v}+\sigma.\vec{v}+\cdots+\sigma^{d-1}.\vec{v},\sigma^d)=(\vec{0},id)$. But we know from Theorem 4.4.4 that $\sum_{i=0}^{d-1}\sigma^i.\vec{v}=\vec{0}$ for $d \mid 3|\sigma|$ and that this holds only for d ($\neq\vec{0}$ for values less than d). But $d=d_\sigma\in D_\sigma$, which means that the orders of elements inside $\mathbb{Z}_3^8\rtimes_{\varphi_1}S_8$, given by σ, are $lcm(d_\sigma,|\sigma|)$. A similair argument for τ and the arbitrary vector $\vec{u}$ shows that the orders of elements inside $\mathbb{Z}_2^{12}\rtimes_{\varphi_2}S_{12}$, given by τ, are $lcm(d_\tau,|\tau|)$. Effectively, since we have the orders in each coordinate in the direct product of G, it's clear that $O_{\sigma,\tau}=\{lcm(lcm(d_\sigma,|\sigma|),lcm(d_\tau,|\tau|)) : d_\sigma\in D_\sigma, d_\tau\in D_\tau\}$ contains all possible orders inside G, given by σ and by τ.
Part (2) is just a direct consequence of Part (1) as indicated in the theorem. □

Remark 4.4.8. It is very important to observe that the orders in G only depend on the orders of the permutations in S_8 and in S_{12}.

Let us not be too hasty and trying to find $\sup\mathcal{O}$ in order to search this element in G_R. There is a huge probability that we will not find the element in G_R since the parity condition in Condition 4.4.2 will reduce the number of orders dramatically. Therefore, let us look at a subset of $\mathcal{O}$ where the parity condition holds.

Remark 4.4.9. The cases one needs to consider in the unconstrained group are not too many and $\sup\mathcal{O}$ is actually 2520, hence giving at the moment a upper limit of 2520.

Since we observed in Remark 4.4.8 that the orders of elements inside G only depend on the orders of the permutations, we can partition the integers 8 and 12. These partitions will correspond to the sizes of the possible orbits in the permutations, hence making it easy to find the possible orders of the permutations. The number of partitions of 8 is 22 and of 12 is 77, thus it does not make sense writing out all of them. Therefore a list of the partitions of 8 is satisfactory because the method applied is the same for 12.

A list of even partitions

7+1
6+2
5+3
5+1+1+1
4+4
4+2+1+1
3+3+1+1
3+2+2+1
3+1+1+1+1+1
2+2+2+2
2+2+1+1+1+1
1+1+1+1+1+1+1+1

A list of odd partitions

8
6+1+1
5+2+1
4+3+1
4+2+2
4+1+1+1+1
3+3+2
3+2+1+1+1
2+2+2+1+1
2+1+1+1+1+1+1

Analysing these lists, one finds quickly all the possible orders of permutations in S_8. They are just written out here without calculations since the author finds this very straightforward (just look at the lcm of the partitions). Let $\mathfrak{A}_o^{(8)}$ be the set of orders of odd permutations and $\mathfrak{A}_e^{(8)}$ the set of orders of even permutations, we then summarise it in the equations below.

$$\mathfrak{A}_e^{(8)} = \{1, 2, 3, 4, 5, 6, 7, 15\} \tag{4.4.4}$$

$$\mathfrak{A}_o^{(8)} = \{2, 4, 6, 8, 10, 12\} \tag{4.4.5}$$

Analysing the permutations in S_{12} in the same manner we will obtain the sets below.

$$\mathfrak{A}_e^{(12)} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 14, 15, 20, 21, 30, 35\} \tag{4.4.6}$$

$$\mathfrak{A}_o^{(12)} = \{2, 4, 6, 8, 10, 12, 14, 18, 20, 24, 28, 30, 42, 60\} \tag{4.4.7}$$

Finally it's time to actually give a strong upper limit for the elements in G_R. This will be done by looking at the subset $O_p \subseteq \mathcal{O}$ where p stands for parity i.e the permutations in Theorem 4.4.7 who are both even or both

odd. Furthermore, we see from Theorem 4.4.7 that the induced orders by $\sigma \in S_8$ in $\mathbb{Z}_3^8$ can be a product of 3 and that the induced orders by $\tau \in S_{12}$ in $\mathbb{Z}_2^{12}$ ca be a product of 2. If they are not, we are only examining the orders of the permutations. Thus we can assume, in order to find the maximum value of O_p, that the induced orders are $3|\sigma|$ and $2|\tau|$, hence the least common multiples are always $lcm(3|\sigma|, 2|\tau|)$. This means that $\sup O_p$ is the same as supremum of the set $B = \{lcm(3a, 2b) \mid a \in \mathfrak{A}_e^{(8)}, b \in \mathfrak{A}_e^{(12)}$ or $a \in \mathfrak{A}_o^{(8)}, b \in \mathfrak{A}_o^{(12)}\}$. A quick examination of the multiples, one find that $\sup O_p = \sup B = lcm(3 * 15, 2 * 14) = 1260$. Let us state this in a lemma in order to find an element of greatest order. The proof is omitted of course since all the calculations are done.

Lemma 4.4.10. *The upper limit for orders of elements in Rubik's Cube is 1260.*

The final result of this section is stated and prooved in the theorem below

Theorem 4.4.11. *An element of greatest order in Rubik's Cube has the order 1260.*

Proof. Let $A \subseteq G_R$ be the set of elements with order 1260. We will now prove that this set is nonempty, hence proving the theorem. Take $\sigma = (12345)(678) \in S_8$ and $\vec{v} = (1, 0, 0, 0, 0, 0, 0, 0, 2) \in \mathbb{Z}_3^8$. Now take $\tau = (1234567)(89)(10\,11) \in S_{12}$ and $\vec{u} = (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \in \mathbb{Z}_2^{12}$. We realise quickly that $sum(\vec{v}) = 0$, $sum(\vec{u}) = 0$ and $sgn(\sigma) = sgn(\tau)$, hence by Condition 4.4.2 this is a valid element of G_R.
Let us examine the order of this element in $(\mathbb{Z}_3^8 \rtimes_{\varphi_1} S_8) \times (\mathbb{Z}_2^{12} \rtimes_{\varphi_2} S_{12})$. The induced order of $\vec{v}$ by σ is $3 * lcm(5, 3) = 3 * 15$ and the induced order of $\vec{u}$ by τ is $2 * lcm(7, 2, 2) = 2 * 14$. Thus $|(\vec{v}, \sigma, \vec{u}, \tau)| = lcm(3 * 15, 2 * 14) = 1260$ and $A \neq \emptyset$. But we know from Lemma 4.4.10 that this is the greatest order, hence proving the theorem. □

Chapter 5

"The Void Cube"

by Olof Bergvall

Abstract

The Void Cube is a variation of Rubik's Cube obtained by making the center facets indistinguishable. We see that also the Void Cube may be given a group structure and that this group can be seen as a subgroup of the Rubik's Cube group.

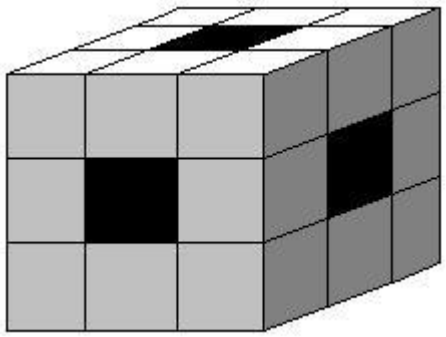


Figure 5.1: The Void Cube.

5.1 Introduction

The Void Cube is a variation of Rubik's Cube that is obtained by making the center facets indistinguishable. The manufacturer of the Void Cube achieves this by removing the center of the cube, though the same effect can be obtained by simply painting the center facets black. However, by

removing the center one acquires the first iteration of a *Menger sponge*, a three dimensional fractal set similar to the *Sierpinski triangle*.

In Rubik's Cube the center facets serve as a reference frame since their relative positions never change. Thus, when this reference frame is removed some states that used to be different become indistinguishable. A number of natural questions arises. Do the states of the Void Cube form a group? In that case, which cardinality does this group have? Which distinguishable states in Rubik's Cube are indistinguishable in the Void Cube?

In the following sections we will see that the states of the Void Cube indeed form a group, which we shall denote G_V. This group is a subgroup of G_R of cardinality $\frac{1}{12}|G_R|$, where G_R is the Rubik's Cube group. The states of Rubik's Cube that become indistinguishable in the Void Cube form a subgroup of G_R isomorphic to A_4, the group of rotational symmetries of a tetrahedron. However, we shall see that A_4 is not normal in G_R so G_V is not expressible as a quotient G_R/A_4. We shall also find that G_V is not normal in G_R so it is not possible to express the relationship between G_R and G_V by expressing G_R as a semidirect product $G_V \rtimes A_4$. Section 5.5.3 is devoted to somewhat overcome these difficulties. In the last section some possible generalisations are informally discussed.

5.2 Solved States of the Void Cube

In this section we shall discuss the states of Rubik's Cube that appear as solved when seen as states of the Void Cube. We have mostly discussed Rubik's Cube in terms of permutations and orientations of cubies. When discussing solved states of the Void Cube it turns out to be more useful to use terms of (allowed and forbidden) permutations of facets, although we shall occasionally use the "old" terminology as well.

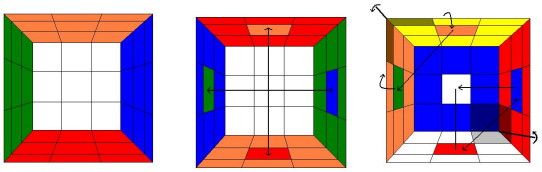
The main results of this section is summarised in the following theorem:

Theorem 5.2.1. *The states of Rubik's Cube that appear as solved states of the void cube are*

(i) the (one) identity state (see Figure 5.2a),

(ii) the (three) states where two opposite center facets are fixed and the two other opposite pairs of center facets are transposed (see Figure 5.2b) and

(iii) the (eight) states where two sets of three pairwise adjacent center facets are permuted cyclically around two opposite corners (see Figure 5.2c).



(a) Case 1. (b) Case 2. (c) Case 3.

Figure 5.2: The three cases.

A state of a Rubik's Cube will be a solved state of a Void Cube precisely if it is obtained from a solved Rubik's by permuting its center facets in some way. Since there are six faces of the cube, a person without any knowledge about Rubik's Cube might expect 6! of the states of Rubik's Cube to be solved states of the Void Cube. However, we know that the relative positions of the center facets never change and we therefore conclude that 6! is a gross overestimation.

To obtain a more reasonable upper bound (and eventually the correct number) we may reason as follows. Consider a solved Void Cube, such as the one seen in Figure 5.1. We may construct a state of Rubik's Cube from the solved Void Cube by first choosing one of the six "holes" to be, for instance, the white center facet. Since the relative configuration of the center facets is fixed we know that the opposite center facet must be the

yellow one (provided that the standard colouring is used, see Figure 5.2 for the standard colouring). We then have a certain freedom in choosing how to place the remaining center facets. Let us begin by placing the blue center facet. There are four "holes" left and any is valid. When we have chosen the hole to contain the blue center facet we know that the green center facet must be opposite. The placement of the remaining center facets is now completely determined. Hence there are at most $6 * 4 = 24$ states of Rubik's Cube that appear as solved states in the Void Cube.

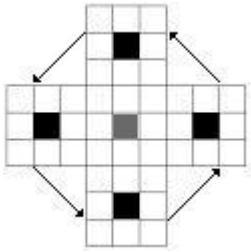


Figure 5.3: Permuting four adjacent center facets.

The states described above are the only ones that satisfy the requirement that the relative configuration of the center facets is fixed. This is however not enough for the states to be valid states of Rubik's Cube. Consider, for instance, the state obtained by fixing one of the center facets in its right place and thereafter permuting the adjacent center facets counterclockwise one step, as seen from the fixed facet, see Figure 5.3. This state has the required relative configuration of the center facets. However, if we were to obtain this state by permuting the corner and edge cubies this would require the corner cubies to be permuted in two disjoint 4-cycles and the edges in three disjoint 4-cycles. Hence, the permutation of the corners would be even and the permutation of the edges would be odd. This shows that these states are not possible states of Rubik's Cube. There are six states of this type (each corresponding to a face of the cube) so we see that there are at most $24 - 6 = 18$ states of Rubik's Cube that appear as solved states in the Void Cube.

If we instead permute the adjacent facets two steps we still end up with the required configuration of the center facets but this time the corner cubies have to be permuted according to four transpositions and the edge cubies according to six transpositions. Thus, both the permutation of the corners and the permutation of the edges are even. This could be a possible state of Rubik's Cube but we still have to check if the change of orientation satisfies the conditions that we derived in the chapter about Rubik's Cube. The choice of orientation seen in Figure 5.4 gives the same orientation before and after the permutations, both for the edges and the corners. Hence, these states are possible states of Rubik's Cube. There are 3 such states (since

permuting the center facets two steps counter clockwise seen from one side gives the same result as permuting them two steps counterclockwise seen from the opposite side). Since the solved state of Rubik's Cube also will appear as solved in the Void Cube we have at least $3 + 1 = 4$ states of Rubik's Cube that appear as solved states in the Void Cube.

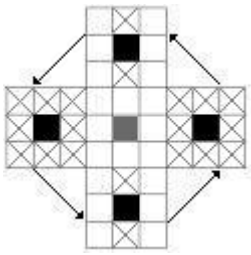


Figure 5.4: A choice of orientation.

To continue the investigation pick a center facet, X, and place it in the hole of the Void Cube opposite to its right place. Since the relative configuration of the center facets is fixed it is impossible to have one center facet in the hole opposite to its right place while all adjacent center facets are in their right places. However, it is possible to have two center facets adjacent to X and opposite to each other, in their right positions (in fact, this is one of the states we obtain by permuting the four facets adjacent to a fixed center facet two steps counterclockwise). If we permute the four center facets adjacent to X one step counterclockwise, see Figure 5.5, we obtain a state where no center facet is in its right place that is in accordance with the relative configuration of the center facets. We now want to see if this is a possible state of Rubik's Cube.

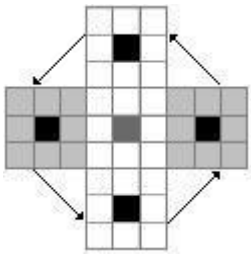
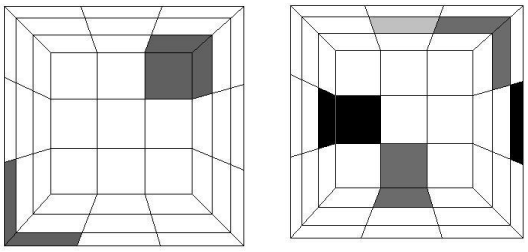


Figure 5.5: The center facets on the grey faces are wrong and the center facets on the white faces are right before the counter clockwise permutation by one step.

To obtain the required state the corner cubies have to be permuted by four transpositions, see Figure 5.6a. The edges on the other hand have to

be permuted by five transpositions, see Figure 5.6b (one of the black kind and four of the grey kind). The remaining two edges have to be mapped to themselves. Hence the corner permutation is even and the edge permutation is odd. Hence this state is impossible. There are 6 such states (each corresponding to a particular center facet of Rubik's Cube) so we have at most $18-6=12$ states of Rubik's Cube that appear as solved in the Void Cube.



(a) Corner transposition. (b) Edge transpositions.

Figure 5.6: The different transpositions.

Let us again pick a center facet, X, but this time we place it in one of the holes adjacent to its right position (and once the position of X is known, the position of the center facet opposite to X is known). Because of the fixed relative configuration of the center facets it is impossible for the four remaining center facets to all be in their right positions, however two may be. Let us place the center facets in such a way. Now we permute the four center facets adjacent to X one step counter clockwise, seen from X. The resulting state is a permutation of the center facets in two disjoint 3 cycles, see Figure 5.7.

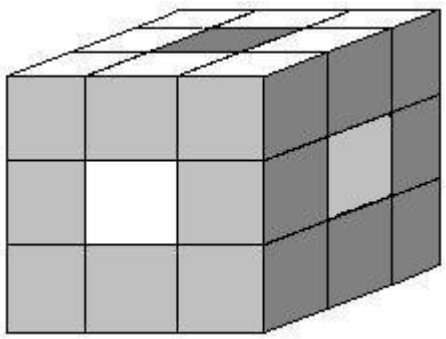


Figure 5.7: The permutation of the center facets.

We now consider if this is a possible state of Rubik's Cube. Two of the corner cubies are in their right positions, (but are turned 1 respectively

2 steps counter clockwise). The other corner cubies are permuted in two disjoint 3-cycles. The edges are permuted in four disjoint 3-cycles. Hence both the permutation of the corners and the permutation of the edges are even. From Figure 5.8 we see that two corners have unchanged orientation, three corners have orientation of type 1 and three of type 2. Hence the sum of the changes of orientation is $3*1+3*2 = 9$ which is a multiple of 3. From Figure 5.9 we see that four edges have unchanged orientation and eight have changed orientation. Hence the sum of the changes of orientation is $8*1 = 8$ which is a multiple of 2.

Of course, the sum of the changes of orientation depends on our particular choice of definition of orientation but the fact that they are multiples of 3 and 2 respectively is independent of choice of orientation, by the chapter about Rubik's Cube. Hence the permutations of the corners and the edges are both even and the sum of changes of orientations is a multiple of 3 for the corners and a multiple of 2 for the edges. This state is thereby a possible state of Rubik's Cube.

There are 8 such states (since there are 4 ways of placing X and permuting the adjacent center facets counter clockwise one step and 4 ways of choosing X and permuting the adjacent center facets clockwise one step. The latter case is not included in the discussion above, but choosing the center facet X' opposite to X instead of X reduces this case to the case discussed above). Hence there are at least $4 + 8 = 12$ states of Rubik's Cube that will appear as solved in The Void Cube. But we have already seen that there are at most 12 states that appear as solved in the Void Cube. This shows that there are precisely 12 such states.

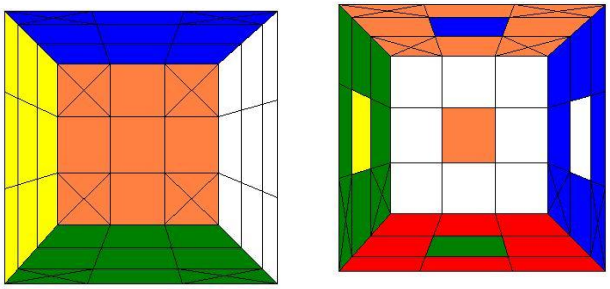
We conclude this section by restating Theorem 5.2.1:

Theorem 5.2.1 *The states of Rubik's Cube that appear as solved states of the void cube are*

(i) *the (one) identity state (see Figure 5.2a),*

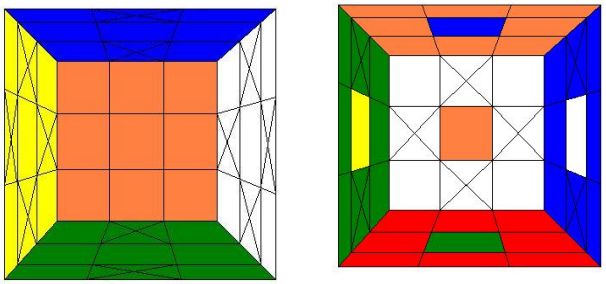
(ii) *the (three) states where two opposite center facets are fixed and the two other opposite pairs of center facets are transposed (see Figure 5.2b) and*

(iii) *the (eight) states where two sets of three pairwise adjacent center facets are permuted cyclically around two opposite corners (see Figure 5.2c).*



(a) A definition of orientation. (b) A state of the considered type.

Figure 5.8: Orientation of the corners before and after the permutation.



(a) A definition of orientation. (b) A state of the considered type.

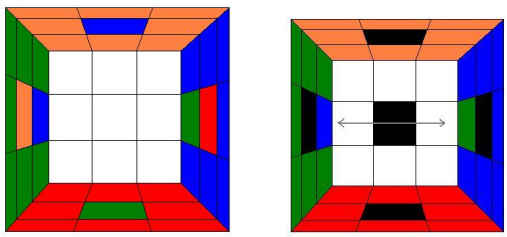
Figure 5.9: Orientation of the edges before and after the permutation.

5.3 Transpositions in the Void Cube

The main result of this section is:

Theorem 5.3.1. *In the Void Cube, corner cubies and edge cubies may be transposed independently.*

We saw in Section 5.2 that it is impossible to permute the center facets of Rubik's Cube in a way which fixes two opposite facets while it permutes the other four cyclically. The reason for this was that such a state would require the corner cubies to be permuted by four transpositions while the edges had to be permuted by five transpositions. However, if we require all cubies, except two opposite edge cubies of a face of the cube, to be permuted as described in Figure 5.10 we obtain a possible state of Rubik's Cube. The state in Figure 5.10 is possible because it requires the corners to be permuted in two 4-cycles and the edges in two 4-cycles and two transpositions, i.e. both the corners and the edges are permuted evenly, while it is possible to define the orientation such that this state has orientation 0 both for the corners and the edges (see Figure 5.11). By the symmetry of the cube we may transpose any pair of facewise opposite edge cubies ("facewise opposite" means that the edge cubies are opposite on a particular face of the cube, see Figure 5.10b).



(a) The state of Rubik's Cube. (b) The state in the Void Cube.

Figure 5.10: A transposition of edges.

We may permute one pair of facewise opposite edge cubies and at the same time transpose any other pair of edge or corner cubies. The permutation of the edges will thus have the same sign as the permutation of the corners so this is a valid state of Rubik's Cube. If we regard the state as a state of the Void Cube we may now transpose the pair of facewise opposite edges back to their original position leaving only the other pair of cubies transposed. This shows that any pair of edge or corner cubies may be transposed without any other effect on the Void Cube.

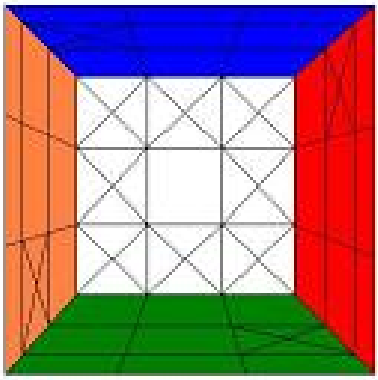


Figure 5.11: A definition of orientation.

5.4 The Void Cube Group

Since it is possible to define a group that describes the different states of Rubik's Cube it is natural to ask whether this is possible for the Void Cube as well. The easiest way to do so would be to use the states of Rubik's Cube that become solved in the Void Cube to define an equivalence relation on Rubik's Cube and then let the equivalence classes be the Void Cube group, i.e. to describe the Void Cube by a group of fractions. However, for this to make sense the set of elements of the Rubik's Cube group that becomes the identity in the Void Cube group must be a normal subgroup of the Rubik's Cube group. To simplify the further discussion we denote the Void Cube group (yet undefined) by G_V and the set of states of Rubik's Cube that are solved states of the Void Cube by G_I. Remember that the Rubik's Cube group, G_R, is the set

$$\begin{aligned} G_R =&\{(\sigma_C, o_C, \sigma_E, o_E) : \sigma_C \in S_8, \sigma_E \in S_{12}, o_C \in Z_3^8, o_E \in Z_2^{12}, \\ &sgn(\sigma_C) = sgn(\sigma_e), \sum_{i=1}^{8} o_{C,i} \equiv 0(3), \sum_{i=1}^{12} o_{E,i} \equiv 0(2)\} \end{aligned}$$

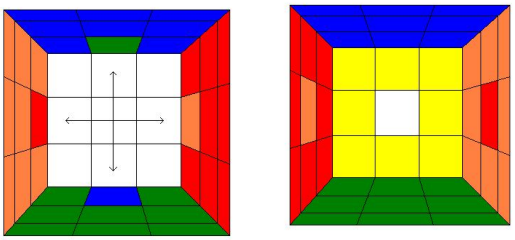
under the product defined by

$$(\sigma_C, o_C, \sigma_E, o_E)(\pi_C, o'_C, \pi_E, o'_E) = (\sigma_C\pi_C, o_C + \sigma_C.o'_C, \sigma_E\pi_E, o_E + \sigma_E.o'_E).$$

Since each state in G_I fixes the relative positions and orientations of the corners and edges, a product of states in G_I will also have this property. We deduce that G_I is a subgroup of G_R. For G_I to be normal we must have $g^{-1}sg \in G_I$ for all $g \in G_R$ and $s \in G_I$. Let g be the element depicted in Figure 5.12a and let s be the element depicted in Figure 5.12b. We see that $g^{-1}sg \notin G_I$ (g transposes two pairs of edge cubies on the white face, s moves the pairs to the yellow face and $g^{-1} = g$ transposes two other pairs of edge cubies). Hence G_I is not normal so the suggested approach to the problem would not be very fruitful.

Instead we might try to mimic the approach used when the Rubik's Cube group was constructed. In that case it was easy to define the "right" position and orientation of a cubie in terms of the fixed center facets. This is clearly not possible in this case so we need some other way of defining the right position and orientation of a cubie. To do this we choose an edge cubie and fix it (both its position and its orientation). In the solved state the relative configuration of the colours of the faces is fixed so fixing this edge cubie defines the right position and orientation of each cubie, see Figure 5.13.

Note that fixing an edge cubie makes two moves "forbidden" (in our case F and D). On the other hand it is no longer meaningful to "forbid" rotations of the center layers that do not contain the fixed edge cubie. It is thus better to discuss the Void Cube, described in this way, through the



(a) $g \in G_R$. (b) $s \in S_R$.

Figure 5.12: An element of G_R and an element of S_R.

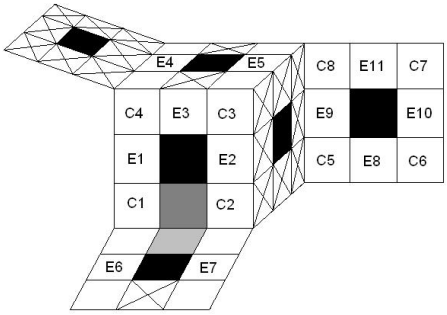


Figure 5.13: A definition of positions and orientations.

rotations $S_V = \{R, L, U, B, C_F, C_D\}$ where the rotation C_F is a 90°-rotation counter clockwise of the center layer between F and B, seen from the front, and C_D is a 90°-rotation counter clockwiseof the center layer between U and D, seen from the down face of the cube. Our previous discussion of the Void Cube through Rubik's Cube carries over to these rotations since the rotation F in Rubik's Cube is equivalent to the sequence $C_F^{-1}B$ and the rotation D is equivalent to the sequence $C_D^{-1}U$.

Let M be the set

$$M = \{(\sigma_C, o_C, \sigma_E, o_E) : \sigma_C \in S_8, \sigma_E \in S_{11}, o_C \in Z_3^8, o_E \in Z_2^{11}\}.$$

As for Rubik's Cube we define the **free Void Cube group**, $\mathfrak{G}_V$, as the set of reduced finite sequences of the rotations in S_V (and corresponding inverses). We then define a function $\Phi : \mathfrak{G}_V \to M$ by first defining the image of the elements in S_V as the permutations and orientation changes corresponding

to that particular rotation

$$\begin{aligned}
\Phi(R) &= ((2583),(0,0,0,0,0,0,0,0),(2\,7\,9\,5),(0,0,0,0,0,0,0,0,0,0,0,0)),\\
\Phi(L) &= ((1476),(0,0,0,0,0,0,0,0),(1\,4\,10\,6),(0,0,0,0,0,0,0,0,0,0,0,0)),\\
\Phi(U) &= ((3874),(0,0,2,2,0,0,1,1),(3\,5\,11\,4),(0,0,1,1,1,0,0,0,0,0,1)),\\
\Phi(B) &= ((5678),(0,0,0,0,1,2,1,2),(8\,10\,11\,9),(0,0,0,0,0,0,0,0,0,0,0,0)),\\
\Phi(C_F) &= (id,(0,0,0,0,0,0,0,0),(4\,6\,7\,5),(0,0,0,1,1,1,1,0,0,0,0)),\\
\Phi(C_D) &= (id,(0,0,0,0,0,0,0,0),(1\,10\,9\,2),(1,1,0,0,0,0,0,0,1,1,0)),
\end{aligned}$$

and then define the image of a sequence to be the product of the images of the rotations in the sequence

$$\Phi(X_1X_2\dots X_n) = \Phi(X_1)\Phi(X_2)\dots\Phi(X_n), X_i \in S_V \text{ or } X_i^{-1} \in S_V.$$

We see that Φ, by definition, is a homomorphism from $\mathfrak{G}_V$ to the group $(M,*)$ where $*$ is defined by

$$(\sigma_C,o_C,\sigma_E,o_E)*(\pi_C,o'_C,\pi_E,o'_E) = (\sigma_C\pi_C, o_C+\sigma_C.o'_C, \sigma_E\pi_E, o_E+\sigma_E.o'_E)$$

where $\sigma.o, \sigma \in S_n, o \in Z_r^n$ is defined by

$$\sigma.o = (o_{\sigma^{-1}(i)}, o_{\sigma^{-1}(2)}, \dots, o_{\sigma^{-1}(n)}).$$

Finally, we define the **Void Cube group**, G_V, to be the image of Φ.

As seen in Section 5.3, the corner and edge cubies can be transposed independently, although here the reason is more apparent; $\Phi(C_F)$ and $\Phi(C_D)$ permute the corner cubies according to an odd permutation while the edges are not permuted at all. Hence the corner cubies may be permuted according to any permutation in S_8 and the edge cubies may be permuted by any permutation in S_{11}.

The sums of the orientations of the generators are however still multiples of 3 and 2, respectively. Hence the proof from the chapter about Rubik's Cube carries over word for word.

Hence the Void Cube group can be expressed as $G_V \leq (S_8 \ltimes Z_3^8) \times (S_{11} \ltimes Z_2^{11})$

$$\begin{aligned}
G_V = \{&(\sigma_C,o_C,\sigma_E,o_E) : \sigma_C \in S_8, \sigma_E \in S_{11}, o_C \in Z_3^8, o_E \in Z_2^{11},\\
&\sum_{i=1}^{8} o_{C,i} \equiv 0(3), \sum_{i=1}^{11} o_{E,i} \equiv 0(2)\}.
\end{aligned}$$

We see that the cardinality of the Void Cube group, $|G_V|$, is

$$|G_V| = \frac{1}{2\cdot 3}\cdot 11!\cdot 8!\cdot 3^8\cdot 2^{11} = \frac{1}{12}|G_R|.$$

Remark 5.4.1. One could equally well define positions and orientations by fixing a corner. One would then obtain the Void Cube as a subgroup of $(S_7 \ltimes Z_3^7) \times (S_{12} \ltimes Z_2^{12})$.

5.5 The Void Cube Group as a Subgroup of the Rubik's Cube Group

As it is, it is not very obvious whether or not the Void Cube group is a subgroup of the Rubik's Cube group or not. Intuitively, it should be but it is very much desirable to prove this and to express the groups in a way that makes this relationship apparent. Since it is not possible to express G_V as a quotient G_R/G_I we investigate the possibility to express G_R as $G_V \rtimes G_I$, but before doing this we investigate G_I a little further.

5.5.1 The Identity States Subgroup

We have already noted that the 12 states of Rubik's Cube that become the identity in the Void Cube, G_I, form a subgroup of the Rubik's Cube group. The aim of this section is to determine the isomorphism class of this group.

We already know that $|G_I| = 12$. There are not many isomorphism classes of groups of order 12, in fact one can show that any group of order 12 is isomorphic to one of the following five groups; Z_{12}, $Z_2^2 \times Z_3$, A_4, D_{12} or $Z_3 \rtimes Z_4$ [1] (the group D_{12} is called the *dihedral group of order 12*). We note that the first two groups are abelian while the other three are nonabelian.

To determine the structure it would be convenient to describe G_I in a suitable way. To attempt this we note that every state in G_I corresponds to a permutation of the center facets of Rubik's Cube. The previous discussion suggests that opposite center facets are related in some way. We should therefore try to take some care to describe this when we label the faces. Let the center face on the face U be given the label 1, D be given 4, F be given 2, B be given 5, R be given 3 and L be given 6. With this choice of labels opposite faces are of the same congruence class modulo 3.

With these labels the allowed permutations of the center faces, i.e. the elements of G_I, are

$$\{id, (14)(25), (14)(36), (25)(36),$$
$$(123)(456), (132)(465), (153)(426), (135)(462),$$
$$(126)(453), (162)(435), (156)(423), (165)(432)\}.$$

We see that in the last eight permutations the second 3-cycle might be determined by the first according to the rule; if the first 3-cycle is (abc) then the second is $(a'b'c')$ where a' is the element in $\{1, \ldots, 6\}$ of the same congruence class modulo 3 as a but not equal to a.

Now consider the elements $\sigma_1 = (14)(25)$ and $\sigma_2 = (123)(456)$. A short computation shows

$$\sigma_1\sigma_2 = (14)(25)(123)(456) = (156)(423)$$

and

$$\sigma_2\sigma_1 = (123)(456)(14)(25) = (153)(426).$$

Hence $\sigma_1\sigma_2 \neq \sigma_2\sigma_1$, so G_I is not abelian and hence not isomorphic to Z_{12} or $Z_2^2 \times Z_3$. We thus only have three candidates left.

We now remember that D_{12} has elements of order 6. G_I only has elements of order 1, 2 and 3. Hence G_I is not isomorphic to D_{12}.

Now consider A_4;

$$\begin{aligned} A_4 =&\{id, (12)(34), (13)(24), (14)(23), (123), (132), \\ &(124), (142), (134), (143), (234), (243)\}. \end{aligned}$$

Note that A_4 contains three pairs of disjoint transpositions and eight 3-cycles, not completely unlike G_I. We therefore try to construct an explicit isomorphism between G_I and A_4.

To do this let

$$H = \{(123)(456), (153)(426), (126)(453), (156)(423)\}$$

and

$$K = \{(123), (124), (134), (234)\}$$

We now note that

$$G_I =< H > \text{ and that } A_4 =< K > .$$

Define $\Phi : G_I \to A_4$ by

$$\Phi(h_i) = k_i, \text{ for all } h_i \in H$$

and

$$\Phi(h_{i_1} \cdots h_{i_r}) = \Phi(h_{i_1}) \cdots \Phi(h_{i_r}) = k_{i_1} \cdots k_{i_r}.$$

Φ is clearly surjective and since we know that $|G_I| = |A_4| = 12$ we conclude that it must also be injective. Hence Φ is a bijection.

Let $\sigma_1, \sigma_2 \in G_I$, $\sigma_1 = h_{i_1} \cdots h_{i_r}$ for some $h_{i_1}, \ldots, h_{i_r} \in H$ and $\sigma_2 = h_{j_1} \cdots h_{j_r}$ for some $h_{j_1}, \ldots, h_{j_s} \in H$. By the definition of Φ we have

$$\begin{aligned} \Phi(\sigma_1\sigma_2) =&\Phi(h_{i_1} \cdots h_{i_r} h_{j_1} \cdots h_{j_s}) = \Phi(h_{i_1}) \cdots \Phi(h_{i_r})\Phi(h_{j_1}) \cdots \Phi(h_{j_s}) = \\ &= \Phi(h_{i_1} \cdots h_{i_r})\Phi(h_{j_1} \cdots h_{j_s}) = \Phi(\sigma_1)\Phi(\sigma_2). \end{aligned}$$

This shows that Φ is an homomorphism. Φ is thereby a bijective homomorphism from G_I to A_4. Hence $G_I \cong A_4$, and the goal of this section is thereby achieved.

Remark 5.5.1. The group A_4 is isomorphic to the group of rotational symmetries of a tetrahedron. Note that in Figure 5.14, each edge of the tetrahedron coincides with a center facet of the cube.

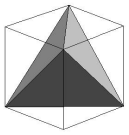


Figure 5.14: A tetrahedron inside a cube.

5.5.2 Normal Subgroups of the Rubik's Cube Group

To understand Rubik's Cube more fully it is very helpful to be familiar with its normal subgroups. This will also greatly simplify our further investigation of the relationship between Rubik's Cube and the Void Cube. In this section we shall therefore briefly consider the normal subgroups of Rubik's Cube.

Several of the normal subgroups of G_R are discovered quite easily through simple observations. Firstly we have the normal subgroups

$$C_O = \{(id, o_C, id, 0) : o_C \in Z_3^8, \sum_{k=1}^{8} \equiv 0(3)\},$$

and

$$E_O = \{(id, 0, id, o_E) : o_E \in Z_2^{12}, \sum_{k=1}^{12} \equiv 0(2)\}.$$

The normality of these groups follows directly from the construction of G_R. Since C_O and E_O are abelian, every subgroup is normal, seen as a subgroup of C_O or E_O. However, the only subgroup that remains normal when seen as a subgroup of G_R is the group

$$E'_O = \{(id, 0, id, o'_E) : o'_{E,i} = o'_{E,j}, i, j = 1, \ldots, 12\}.$$

To see this, take a nonzero element of any other subgroup and conjugate with a transposition that takes a nonzero coordinate outside the group in the first step. This nonzero coordinate will remain nonzero after the inverse has been applied, so the product will not be an element of the subgroup.

Now consider the subgroup that only affects positions and orientations of corners. Since the edge permutation in this group is the identity and the edge and corner permutation must have the same sign, we conclude that the corner permutation is even. We have seen that this is the only restriction so this group is isomorphic to $A_8 \ltimes C_O$. Since the operation of G_R does not relate the corners and the edges and $A_8 \trianglelefteq S_8$ we conclude that this group is normal.

With an analogous argument we also see that $A_{12} \ltimes E_O$ is normal in G_R.

Of course we may take direct products of the above subgroups to obtain new normal subgroups, provided that their intersection is trivial. In this way

we obtain the groups

$$
\begin{aligned}
&E'_O;\\
&E_O;\\
&C_O;\\
&C_O \times E'_O;\\
&C_O \times E_O;\\
&A_8 \ltimes C_O;\\
&A_{12} \ltimes E_O;\\
&(A_8 \ltimes C_O) \times E'_O;\\
&(A_8 \ltimes C_O) \times E_O;\\
&C_O \times (A_{12} \ltimes E_O);\\
&(A_8 \ltimes C_O) \times (A_{12} \ltimes E_O).
\end{aligned}
$$

We have thus found 11 nontrivial, proper normal subgroups of G_R. It can be shown that this is a complete list, see [2].

One important consequence of the above is that none of the normal subgroups has the same cardinality as the Void Cube group. Hence it is impossible to describe the Rubik's Cube group as a semidirect product $G_V \ltimes G_I$.

Another interesting consequence is that the smallest normal subgroup containing G_I is $(A_8 \ltimes C_O) \times (A_{12} \ltimes E_O)$, a subgroup of cardinality $\frac{1}{2}|G_R|$ and a little more than $1.8 \cdot 10^{18}$ times the cardinality of G_I.

5.5.3 The Rubik's Cube Group in a New Way

One could say that the underlying reason of the different appearance of G_R and G_V is that their reference frames are different. Rubik's Cube has a "natural" reference frame in the center facets while the reference frame of the Void Cube is not very natural.

However, it should be possible to describe the states of Rubik's Cube from the same frame of reference as the Void Cube, i.e. by relating the positions and orientations to a fixed edge cubie. A major difference from the old frame is that the center facets are no longer fixed.

Let us label each center facet with an integer in the set $\{1, \ldots, 6\}$ in such a way that opposite facets are congruent modulo 3. There are several ways of labeling the center facets in such a way, but let us label them in a way such that turning the center layers by 90° counter clockwise will correspond to the 4-cycles (1245), (1346) and (2356). Since one edge cubie is fixed, we are "forbidden" to rotate one of the center layers. Hence one of the 4-cycles is not obtainable by a single center layer rotation. Let us assume that this 4-cycle is (2356). Now consider

$$\big((1245)(1346)(1245)(1346)^2\big)^3 = (2356).$$

Hence (2356) is still a possible permutation of the center facets.

Now let $G_C =< (1245), (1346), (2356) >$ and let R be the group of rotational symmetries of an ordinary cube. There are three types of rotations in R, see Figure 5.15. If S is a set containing one rotation of each type then $< S >= R$. If we label each face with an integer $1, \ldots, 6$ in such a way that opposite faces are congruent modulo 3, a possible choice of S is $S = \{(1245), (135)(462), (13)(25)(46)\}$.

Now consider

$$(1245)(1346) = (135)(462) \tag{a}$$

and

$$(1245)(2356)(1245) = (13)(25)(46). \tag{b}$$

Hence we can express a set of generators of R with products of generators of G_C. Hence $R \leq G_C$.

On the other hand, (1245) is an element of R so its inverse, i.e. $(1245)^3$, is also an element of R. Hence we may multiply (a) by $(1245)^3$ from the left and thus see that $(1346) = (1245)^3(135)(462) \in R$. Similarly, we may multiply (b) by $(1245)^3$ from the left and the right to obtain $(2356) = (1245)^3(13)(25)(46)(1245)^3$. Hence the generators of G_C are expressible as products of elements of R so $G_C \leq R$ as well. This shows that $G_C = R$.

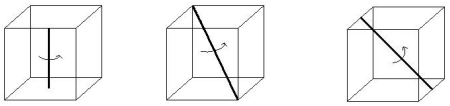


Figure 5.15: The three types of rotations of a cube.

It is well known that $R \cong S_4$ so the above shows that $G_C \cong S_4$. However, if we take all cubies into account, that is edge and corner cubies as well as center cubies, not all permutations of the center facets are obtainable without affecting the other cubies. We have already seen that the only permutations with this property are the permutations of G_I which we have shown to be isomorphic to A_4. The odd permutations of the center facets require that either the permutation of the corner or the edge cubies is odd. Somewhat conversely, we saw in the section about transpositions in the Void Cube that corner cubies and edge cubies can be transposed independently, provided the permutation of the center facets is odd if the sign of the corner permutation differs in sign from the sign of the edge permutation. This can also be deduced from the fact that each of the moves U, B, R, L, C_F, C_D either permutes four corners and four edges cyclically or permutes four centers and four edges cyclically. Every element is a product of such elements so if a permutation of one type of cubie is odd we must have that precisely one of

the other two permutations must be odd and if a permutation of one type of cubie is even the other two must either both be odd or both be even.

The above discussion leads us to define:

$$S'_R = \{(g,\pi) : g = (\sigma'_C, o'_C, \sigma'_E, o'_E) \in G_V, \pi \in S_4, \\ \textit{an even number of } \pi, \sigma'_C \textit{ and } \sigma'_E \textit{are odd}\}.$$

Our aim is to find a binary operation, $*$, on S'_R that makes $(S'_R, *)$ into a group isomorphic to G_R. It is close at hand to chose $*$ to be "the usual" operation in the first four coordinates and composition in the fifth. However, this choice implies that $(A_8 \ltimes C_O) \times (A_{11} \ltimes \tilde{E}_O)$ is normal in $(S'_R, *)$, where

$$\tilde{E}_O = \{o'_E \in Z_2^{11} : \sum_{i=1}^{12} o'_{E,i} \equiv 0(2)\}.$$

This is not a normal subgroup of G_R so this choice of $*$ is a poor one.

The failure above suggests that the center facets are not permuted independently of the edges and corners (apart from being entangled because of the requirement of the sign). Since we have imposed a restriction on the edges it is not too farfetched to suspect that the edges may act on the centers in some sense.

To see why this is the case we may reason as follows. Consider a state g in G_R. The edge piece labeled 12 will have some position α and some orientation a. We now bring it to its original position and orientation by applying a rigid rotation of the cube, π. This will bring the cube to a state in S'_R described by $s = (\sigma_C, o_C, \sigma_E, o_E, \pi)$ where the first four coordinates generally are not the same as the coordinates in g.

Let us interpret all elements of S'_R as described above. Let s_1 and s_2 be elements of S'_R. We may define the product $s_1 s_2$ by first mapping s_1 and s_2 back to G_R, taking the product of the preimages and finally mapping the product back to S'_R.

Let us investigate the process described above more carefully. Let

$$s_1 = (\alpha_C, a_C, \alpha_E, a_E, \pi_1),$$

and let

$$s_2 = (\beta_C, b_C, \beta_E, b_E, \pi_2).$$

Let g_1 and g_2 be the preimages of s_1 and s_2 respectively. We see that

$$g_1 = (\pi_1.\alpha_C, \pi_1.a_C, \pi_1.\alpha_E, \pi_1.a_E)$$

and

$$g_2 = (\pi_2.\beta_C, \pi_2.b_C, \pi_2.\beta_E, \pi_2.b_E)$$

where the action is inverse rotation of the cube. We now take the product

$$\begin{aligned} g_1 g_2 =& (\pi_1.\alpha_C, \pi_1.a_C, \pi_1.\alpha_E, \pi_1.a_E)(\pi_2.\beta_C, \pi_2.b_C, \pi_2.\beta_E, \pi_2.b_E) = \\ & ((\pi_1.\alpha_C)(\pi_2.\beta_C), (\pi_1.a_C) + (\pi_1.\alpha_C).(\pi_2.b_C), \\ & (\pi_1.\alpha_E)(\pi_2.\beta_E), (\pi_1.a_E) + (\pi_1.\alpha_E).(\pi_2.b_E)) = \\ & = \pi_1.(\alpha_C(\pi_2.\beta_C), a_C + \alpha_C.(\pi_2.b_C), \\ & \alpha_E(\pi_2.\beta_E), a_E + \alpha_E.(\pi_2.b_E)). \end{aligned}$$

The image of $g_1 g_2$, $s_1 s_2$, is thus determined by $\pi_1.(\alpha_E(\pi_2.\beta_E))(12)$ and $\pi_1.(a_E + \alpha_E.(\pi_2.b_E)))_{12}$. In particular this means that the fifth coordinate of $s_1 s_2$, i.e. the permutation of the center cubies, is determined independently of the states of the corner cubies in s_1 and s_2.

Further, we may take the above as a definition of a binary operator, $*$, on S'_R. That $(S'_R, *)$ is a group follows from the fact that G_R is a group and it is isomorphic to G_R by the definition of $*$. From now on we shall denote $(S'_R, *)$ by G'_R.

5.5.4 The Void Cube Subgroup

G'_R has an appearance that is much more similar to G_V than G_R. This suggests that it might be easier to deduce whether or not G_V is a subgroup of G'_R.

Note that if g is an element of G_V, there are many elements in G'_R which have the same four first coordinates as g. If the edge and corner permutation of g have the same sign there is an element g' in G'_R with the same four first coordinates as g and the identity in the last coordinate. If the edge permutation differs in sign from the corner permutation there is no such element. However, there is an element g'' in G'_R with the same first four coordinates as g and the last coordinate the permutation corresponding to the rotation around a diagonal passing through the edge labeled 12, see Figure 5.16. Let this permutation be denoted by χ. Then χ transposes three pairs of center facets and is thus odd and of order two.

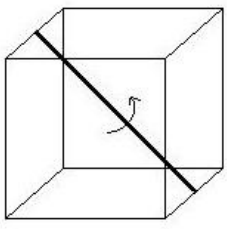


Figure 5.16: Rotation around a diagonal passing through the edge labeled 12.

Now consider the map $\Phi : G_V \to G'_R$ defined by

$$\Phi((\sigma_C, o_C, \sigma_E, o_E)) = \begin{cases} (\sigma_C, o_C, \sigma_E, o_E, id), & \text{if } sgn(\sigma_C) = sgn(\sigma_E), \\ (\sigma_C, o_C, \sigma_E, o_E, \chi), & \text{if } sgn(\sigma_C) \neq sgn(\sigma_E). \end{cases}$$

Since χ is its own inverse and the edge labeled 12 never changes position we deduce that $Im(\Phi)$ is a subgroup of G'_R. Moreover, Φ is injective and a homomorphism so $Im(\Phi) \cong G_V$. This shows that the Void Cube group is a subgroup of the Rubik's Cube group, as expected. This subgroup can be identified with the subgroup of Rubik's Cube where one edge cubie, say 12, is fixed in position i.e.

$$G_V \cong \{g = (\sigma_C, {}_C, \sigma_E, {}_E) : g \in G_R, 12 \in fix(\sigma_E)\} \leq G_R.$$

5.6 Generalisation

As mentioned in the introduction, the Void Cube is the first iteration of a fractal set called the *Menger sponge*. The Menger sponge is constructed from a solid cube by dividing it into 27 smaller cubes, removing the center cube of each face as well as the interior cube. The process is then repeated on the smaller cubes. The second iteration is shown in Figure 5.17. As more and more steps are carried out the remaining cubes converge to a fractal set of (topological) dimension 1, this is what is called the Menger sponge.

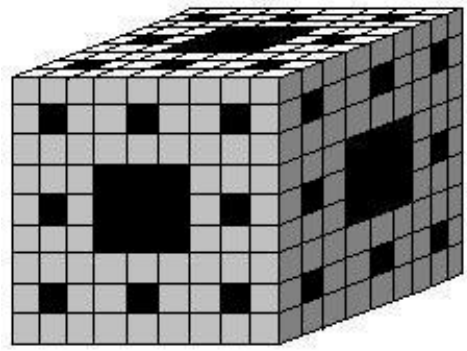


Figure 5.17: The second iteration in the construction of the Menger sponge.

A possible generalisation of the Void Cube would be Menger sponge cube of higher order. Let the $n:th$ Menger cube be denoted M_n. Thus M_0 is a single cube, M_1 is the Void Cube, M_2 is the cube depicted in Figure 5.17 and so on. Let M_∞ denote the group of symmetries of the Menger sponge.

Assume that the layers of M_n can be rotated as in Rubik's Cube or the Void Cube. We can impose a group structure on M_n by assigning each facet a unique integer and identifying a sequence of rotations of layers with the corresponding permutation (note that we by assigning each facet a unique integer avoid the consideration of the possibility of equivalent elements in M_n).

We shall not delve too deeply in this subject, but a few things are rather immediate. Firstly, we may identify the group M_n as a subgroup of M_{n+1}, or higher order Menger cubes for that matter. We thus obtain an infinite chain of subgroups $M_0 \leq M_1 \leq M_2 \leq \ldots$. Further, except for M_0, M_i is not normal in M_{i+k} for $k \geq 1$. One may also note that $M_i \leq M_{i+1}$ for all (at least finite) i.

Another possible generalisation in a slightly different direction would be to colour the interior facets of the $n:th$ Menger cube as well, yielding a still more complex object, see Figures 5.18- 5.19. This makes no difference in the case of M_0 and M_1 but for higher order cubes it might.

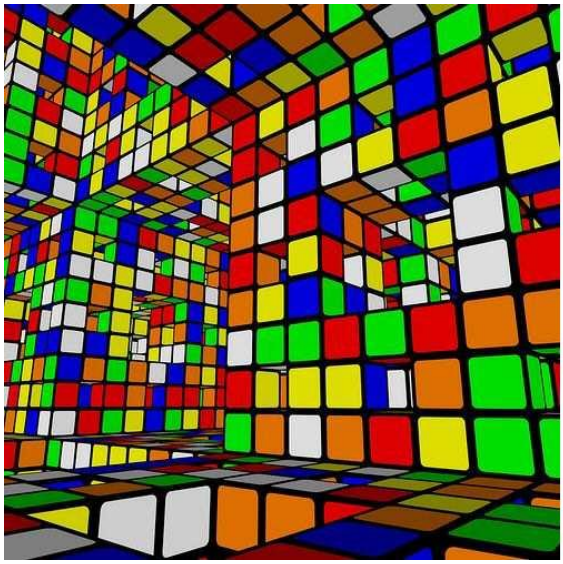


Figure 5.18: Inside a Menger cube (figure used under creative commons licence).

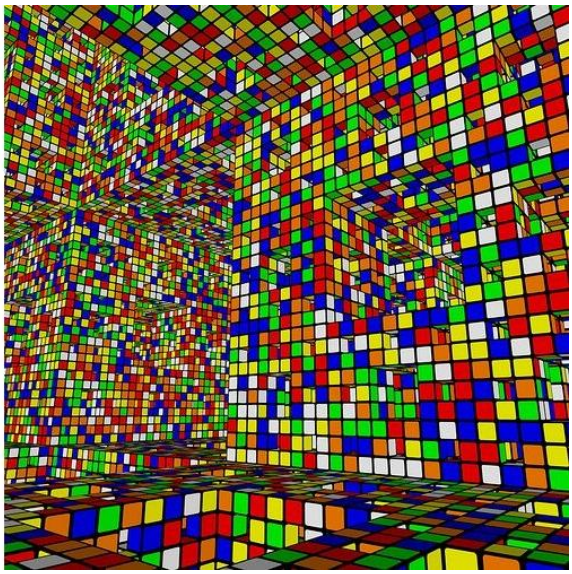


Figure 5.19: Inside a larger Menger cube (figure used under creative commons licence).

Bibliography

[1] Dummit, D.S., Foote, R.M., *Abstract Algebra, 3rd Edition*; John Wiley & Sons, 2004.

[2] Frey, A.H., Singmaster, D., *Handbook of Cubik Math*; Enslow Publishers, 1982.

Chapter 6

"The Black-and-White Cube"

by Elin Hynning

Abstract

Denna artikel behandlar problem relaterade till en Rubiks kub som är färgad med endast två färger. Huvudproblemet som tas upp är huruvida man får en gruppstruktur med de olika blandningarna av en tvåfärgad kub som element och sammansättning av rotationer av kuben som binär operator. Även antalet olika blandningar som finns för olika tvåfärgade kuber tas upp, samt hur många färger man behöver för att få en gruppstruktur av ovan nämnda typ.

Något överraskande visar det sig att man inte får någon gruppstruktur som är analog med den som bestämts för Rubiks kub när man betraktar en tvåfärgad kub. Anledningen till detta är att den binära operatorn inte blir väldefinierad när en kub har flera identiska bitar. Därför undersöks även om man kan få någon grupp mindre än Rubiks Grupp genom att märka likadana bitar. Det visar sig att alla likadana bitar måste märkas och att man inte kan konstruera någon grupp mindre än Rubiks Grupp. Det visar sig även att man behöver sex olika färger för att kunna få en gruppstruktur med sammansättning av rotationer som binär operator. De två olika typerna av tvåfärgade kuber har $\binom{8}{3,3,1,1} \cdot \binom{12}{3,3,6} \cdot 3^6 \cdot 2^6$ respektive $\binom{8}{4,4} \cdot \binom{12}{2,2,8} \cdot 3^7 \cdot 2^8$ olika blandningar.

6.1 The Black-and-White Cube

6.1.1 Introduction

The black-and-white cube is a cube with the same mechanical properties as Rubik's Cube, with the only difference that just two colours have been used to colour the faces of the cube. We will only consider colourings where three faces are black and three faces are white. There are two ways in which one may colour three faces black and three faces white. These will be referred to as the **corner colouring** and the **strip colouring** and are shown in Figure 6.1.

With these new types of cubes we essentially want to do the same thing as we did with Rubik's Cube in section 1.3, i.e. determine whether or not we can form a group of the scramblings of the different black-and-white cubes together with the binary operator consisting of concatenation of rotations of the cubes. We also want to determine how many different scramblings there are, regardless of whether or not they actually form a group.

We will obtain the somewhat surprising result that the different scramblings of the black-and-white cubes together with the above mentioned binary operator do not form a group. When we determine the number of different scramblings, we will find that there are $\binom{8}{3,3,1,1} \cdot \binom{12}{3,3,6} \cdot 3^6 \cdot 2^6$ different scramblings of the corner coloured cube and that the number of different scramblings of the strip coloured cube is $\binom{8}{4,4} \cdot \binom{12}{2,2,8} \cdot 3^7 \cdot 2^8$. We will also see that in order to form a group structure, every face of the cube needs to be coloured in a unique colour, thus making it the ordinary Rubik's Cube.

In order to investigate the group structure of the different black-and-white cubes we will start out in the same way as we did with Rubik's Cube. We consider the free group consisting of concatenation of rotations of the six faces of the cube and their respective inverses, i.e. $\mathfrak{G}_R$ of Proposition 1.3.5. We then consider this free group acting on the set of different scramblings of the black-and-white cubes. Let S denote the set of different scramblings of the considered black-and-white cube. The group action will work as follows: consider a sequence of rotations $g \in \mathfrak{G}_R$ and a scrambling $s_1 \in S$. The group action $g \times s_1 \to s_2$ represents applying the sequence of rotations g to the scrambling s_1 and thus obtaining a new scrambling s_2. (Note that s_1 and s_2 might be the same scrambling.) Two sequences of rotations $g_1, g_2 \in \mathfrak{G}_R$ will be considered to be the same if they have the same effect when applied to the cube. This group action will thus be used to form a group consisting of the set S and the binary operator consisting of concatenation of rotations of the cube. The binary operator, $\cdot$, will work in the following way: consider two scramblings $s_1, s_2 \in S$. The scrambling, s_3, obtained from the following operation $s_2 \cdot s_1 = s_3$ is the scrambling one would get if one starts from a solved cube, then applies the rotations that scramble the cube to s_1, and then from this scrambling applies the rotations that would scramble a solved

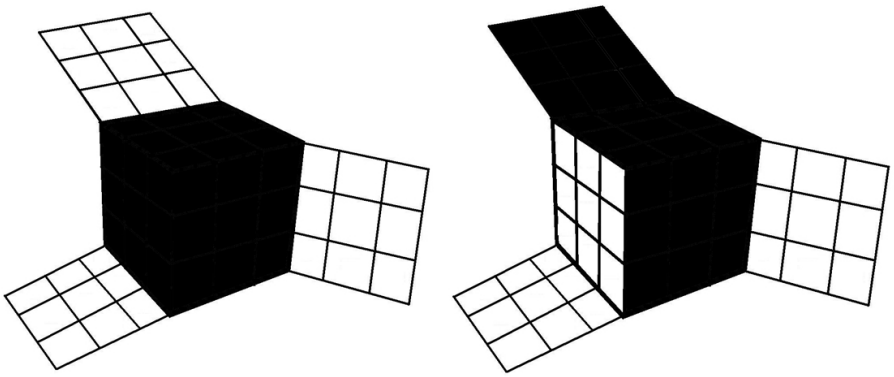


Figure 6.1: The two different ways of colouring three faces of the cube black and three faces white. The left cube shows the corner colouring and the right cube shows the stripcolouring

cube to s_2.

The group action defined above is essentially the same as the one used in order to form Rubik's Group. The only difference is that now $\mathfrak{G}_R$ is acting on a subset of the set used when Rubik's Group was defined. We realise that the difference between the black-and-white cubes and the Rubik's Cube, i.e. the difference between the sets on which $\mathfrak{G}_R$ is acting, will be the occurence of identical pieces in the black-and-white cubes. There will also be pieces for which orientation lacks importance, since there are unicoloured pieces in the black-and-white cubes.

In order to determine whether or not a cube colouring is a group, we start out by determining when the binary operator obtained from the group action is well defined.

Lemma 6.1.1. *For a cube where three corner pieces or three edge pieces are identical, and there exist corner pieces and edge pieces that are not identical to these three, the binary operator consisting of concatenation of rotations of the cube does not yield a group together with the different scramblings of the cube.*

Proof. Consider a cube where corner pieces 1, 2 and 3 are identical. We know from section 1.3.4 that there exists a series of rotations $A_1 \in < F, B, R, L, U, D >$ that will permute corner pieces at position 1, 2 and 3 among themselves and not affect the cube in any other way. Consider applying A_1 on a solved cube. Then A_1 will have no visible effect on the cube and will thus be considered to be the identity element. Now consider a state where the cube has been scrambled in such a way that the corner pieces currently in position

1, 2 and 3 are not identical. If we apply the rotations A_1 on this state, we will obtain a different state of the cube, since we have permuted three non-identical corner pieces. Thus, from this state, A_1 is not the identity element. Hence, the binary operator does not yield a group together with the different scramblings of the cube.

Now consider a cube where edge pieces 1, 2 and 3 are identical. We know from section 1.3.4 that there exists a series of rotations $A_2 \in < F, B, R, L, U, D >$ that permutes edge pieces at positions 1, 2 and 3 without affecting the cube in any other way. The rest of the proof is completely analogous to the case with identical corner pieces. This completes the proof. □

Lemma 6.1.2. *For a cube where two pairs of pieces, either corner pieces or edge pieces, are identical, and there exist pieces that are not identical to these pieces, the binary operator consisting of concatenation of rotations of the cube does not yield a group together with the different scramblings of the cube.*

Proof. Consider a cube where pieces, either corner or edge, 1 and 2 are identical and pieces 3 and 4 are identical. We know from section 1.3.4 that there exists a series of rotations $A \in < F, B, R, L, U, D >$ such that pieces in positions 1 and 2 switch positions and pieces in positions 3 and 4 switch positions and the rest of the cube is left unchanged. Consider applying A to a solved cube. Then there will be no visible change and A will be the identity. Now consider a state of the cube where the pieces in positions 1 and 2 are not identical or pieces in positions 3 and 4 are not identical. If we apply A to this state, there will be a visible change of the cube. Thus, A is no longer the identity, and the binary operator does not yield a group together with the different scramblings of the cube. This completes the proof. □

Lemma 6.1.3. *For a cube where two corner pieces are identical and two edge pieces are identical, and there exist corner pieces and edge pieces that are not identical to these pieces, the binary operator consisting of concatenation of rotations of the cube does not yield a group together with the different scramblings of the cube.*

Proof. Consider a cube where corner pieces 1 and 2 are identical and edge pieces 1 and 2 are identical. We know from section 1.3.4 that there exists a series of rotations $A \in < F, B, R, L, U, D >$ such that corner pieces in positions 1 and 2 are interchanged and edge pieces in positions 1 and 2 are interchanged, and the rest of the cube is left unchanged. If A is applied to a solved cube, the cube will be left unchanged and A will be the identity element. Now consider a state where the cube has been scrambled in such a way that the corner pieces currently at corner positions 1 and 2 are non-identical, or the edge pieces currently at edge positions 1 and 2 are non-identical. If we apply A to this state, we will end up in a different state,

since we have interchanged at least two pieces that are non-identical. Thus, in this state, A is no longer the identity element. Hence the binary operator does not yield a group together with the different scramblings of the cube. This completes the proof. □

Lemma 6.1.4. *For a cube where two pieces of the same kind are unicoloured, i.e. unoriented, and there exist pieces of this kind that are not unicoloured, the binary operator consisting of concatenation of rotations of the cube does not yield a group together with the different scramblings of the cube.*

Proof. Consider a cube where pieces 1 and 2 of the same kind are both unicoloured. We know from section 1.3.4 that there exists a series of rotations $A \in < F, B, R, L, U, D >$ such that pieces at positions 1 and 2 change orientation, regardless of whether 1 and 2 are corner pieces or edge pieces, and the rest of the cube is left unchanged. Consider applying A on a solved cube. There will be no visible change of the cube, and thus A will be an identity element. Now consider applying A to a scrambled state of the cube where pieces at positions 1 and 2 are not both unicoloured. Then at least one piece has changed its orientation and a different scrambling is obtained. Thus, A is not an identity element for this state. Hence, the binary operator does not yield a group together with the different scramblings of the cube. □

6.1.2 The Corner Colouring

The corner coloured cube has two fixed points, namely the unicoloured corner pieces. Regardless of how we rotate the corner coloured cube in space, these two pieces will always have a fixed position in reference to the corner coloured cube itself. With Rubik's Cube we have the same phenomenon; with reference to the cube, we always know where the different pieces are supposed to be positioned no matter how the cube is rotated in space. Therefore, we do not need to fix the corner coloured cube in space in order to consider the same rotations, and thus the same binary operator, as the ones used in Rubik's Group operating on the corner coloured cube.

The corner coloured cube have four different kinds of corner pieces; one with three black facets, one with three white facets, three with two black facets and one white facet and three with one black facet and two white facets. Let them be numbered as shown in Figure 6.2.

The corner coloured cube also has three different kinds of edge pieces; three with two white facets, three with two black facets and six with one black and one white facet. Let them be numbered as shown in Figure 6.3.

We can now determine whether or not the corner coloured cube together with the binary operator of concatenation of rotations of the cube form a group.

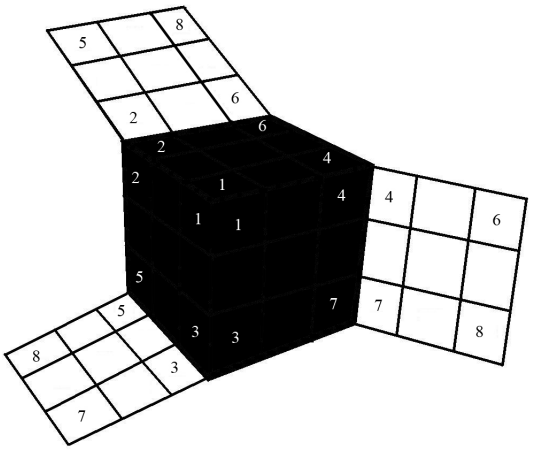


Figure 6.2: Numbering of the corner pieces of the corner coloured cube.

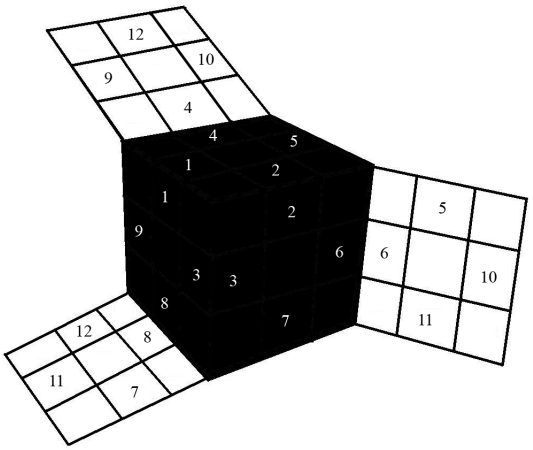


Figure 6.3: Numbering of the edge pieces of the corner coloured cube.

Theorem 6.1.5. *The different scramblings of the corner coloured cube together with the binary operator of concatenation of rotations of the cube do not form a group.*

Proof. We see that the corner coloured cube have two groups of three identical corner pieces. By Lemma 6.1.1 we know that the binary operator does not yield a group together with the different scramblings of the cube. Hence, no group can be formed. Furthermore, we also have two groups of three identical edge pieces, one group of six identical edge pieces, two unicoloured corner pieces, and six unicoloured edge pieces. By Lemmas 6.1.3 and 6.1.4 the binary operator does not yield a group together with the different scramblings of the cube. We are thus far away from being able to form a group. □

This result is somewhat surprising. Since the corner coloured cube is so similar to Rubik's Cube, and Rubik's Cube has a group structure when we consider the different scramblings together with the concatenation of rotations, we expect the same result to hold for the corner coloured cube. However, as seen above, the intuition leads us wrong in this case. The fact that we cannot form a group structure in the same way as we did with Rubik's Cube for the corner coloured cube also says something about the rotations in $\mathfrak{G}_R$ that leave the corner coloured cube unchanged.

Corollary 6.1.6. *The set of sequences of rotations in* $< F, B, U, D, R, L >$ *that leave the corner coloured cube unchanged does not form a normal subgroup in* $\mathfrak{G}_R$.

Proof. Assume that the sequences of rotations that leave the corner coloured cube unchanged form a normal subgroup, N, in $\mathfrak{G}_R$. Then one would be able to form the quotient group $\mathfrak{G}_R/N$ and its elements would be precisely the different scramblings of the corner coloured cube. From Theorem 6.1.5 we know that these elements do not form a group with the binary operator of concatenation of rotations. Hence, the sequences that leave the corner coloured cube unchanged cannot form a normal subgroup in $\mathfrak{G}_R$. This completes the proof. □

Now that we have determined that the different scramblings of the corner coloured cube do not form a group with the binary operator of the Rubik's Group, the natural thing to investigate is whether or not there is a way to obtain a group from the corner coloured cube. One way to do this, which is analogous to the way one specifies the group of the $4 \times 4 \times 4$-cube, is by "marking" identical pieces so that scramblings that look the same are considered to be different when different, but identical, pieces are in different places. If we were to mark pieces in this way, would all identical pieces need to be marked in order to form a group, or is it possible to only mark a few of them and obtain some kind of group structure smaller than Rubik's Group?

We already know that we cannot have three identical pieces, two pairs of identical pieces or two identical corner pieces and two identical edge pieces at the same time. We also know that we cannot have two unicoloured pieces of the same kind, so the only way we might obtain a group smaller than Rubik's Group is if the binary operator yields a group with two identical pieces. Thus, we need to determine if the binary operator yields a group for two identical pieces. If we use the regular definition of the group, i.e. we fix the six center facets and rotate the faces, we will see that the binary operator does not yield for two identical pieces.

Lemma 6.1.7. *For a cube where two pieces, either corner or edge, are identical, and other pieces exist that are not identical to these two, the binary operator consisting of concatenation of rotations of the cube does not yield a group together with the different scramblings of the cube.*

Proof. Consider a cube where pieces, either edge or corner, 1 and 2 are identical. Consider a sequence of rotations, A, that cycically rotates pieces at position 1, 2 and 3 and leaves the rest of the cube unchanged. We know from section 1.3.4 that such sequences exist. If A is applied to a solved cube, it will appear as though only two pieces have switched position, and A will be a transposition of pieces. Now consider a scrambling of the cube where pieces at positions 1, 2 and 3 are all different. If we apply A to this scrambling, three pieces will change position, and A will be a 3-cycle. Thus, the binary operator does not yield a group together with the different scramblings of the cube. This completes the proof. □

However, there might be another way to define the group such that we are able to have two identical pieces. We could do this by defining the cube group from one edge piece or one corner piece and allow for one piece of the same kind to be identical to this piece. These two pieces will not cause a problem in our attempt to form a group, since one of them is allowed to move and the other one is not. In section 5.5.3, Rubik's Group is defined from one single piece, and results from that section will be used here. However, a new problem arises when we define our group from one edge or corner piece, namely the fact that the center facets are allowed to move relative to the fixed piece. In order to determine whether or not we can have two identical pieces, we thus have to determine whether or not the binary operator yields a group when we have identical center facets.

Lemma 6.1.8. *For a cube where two center facets are identical, and there exist center facets that are not identical to these two, and we do not have that every center facet is identical to the opposite center facet, the binary operator defined in section 5.5.3 does not form a group.*

Proof. Consider a cube where center facets 1 and 2 are identical. We realise that we have two cases, either these two identical facets are situated on

adjacent faces or they are situated on opposite faces. First consider the case where they are adjacent. Now consider a sequence of rotations, A_1, that cyclically rotates center facets in positions 1, 2 and 3 among each other and cyclically rotates center facets in positions 4, 5 and 6 among one another and does not change the cube in any other way. We know from Theorem 5.2.1 that such sequences exist. Consider applying A_1 to a solved cube. Then A_1 will be represented as a product of two disjoint cycles where one is a transposition and the other is a 3-cycle. Now consider a scrambling of the cube such that center facet 1 is in position 1, 2 or 3 and center facet 2 is in position 4, 5 or 6. If we apply A_1 to this scrambling, then it will be represented as a product of two disjoint 3-cycles. Thus, the binary operator does not yield a group.

Now consider the case where center facets 1 and 2 are opposite. Consider a sequence of rotations, A_2, such that center facets in opposite positions 1 and 2 switch positions and center facets in opposite positions 3 and 4 switch positions and the rest of the cube is left unchanged. We know from Theorem 5.2.1 that such sequences exist. Consider applying A_2 to a solved cube. Then A_2 will be represented as a transposition. Now consider a scrambling where center facets 1 and 2 are at opposite positions 5 and 6. We know from the section of the void cube that such scramblings exist. If we apply A_2 to this scrambling, it will be represented by a product of two disjoint transpositions. Hence, the binary operator does not yield a group. This completes the proof. □

Remark 6.1.9. One could make all center facets identical and obtain a group structure, i.e. the group structure of the void cube. But since we will always have two different colours of the center facets when considering a black-and-white cube, this colouring of the center facets concerns a different problem than the one considered here.

Remark 6.1.10. This proof does not cover the case where all opposite center facets are identical. However, neither of the black-and-white colourings have all opposite center facets identical, thus this does not matter when considering black-and-white cubes.

From these two lemmas we can deduct that we cannot have two identical pieces, unless no center facets are identical, and with no identical center facets, we have Rubik's Group. However, we might still be able to have a smaller group than Rubik's Group by leaving one corner piece and one edge piece unicoloured.

Lemma 6.1.11. *If one corner piece and one edge piece are left unicoloured, the number of possible orientations will be the same as the number of possible orientations for a cube where no corner piece or edge piece is unicoloured.*

Proof. From Lemma 1.3.21 we know that the number of possible edge orientations is 2^{11} and from Lemma 1.3.22 we know that the number of possible

corner orientations is 3^7. We also know from the investigation of Rubik's Cube that there exist sequences of rotations such that two edge pieces change their respective orientations or two corner pieces change their respective orientations, and the rest of the cube is left unchanged. Now consider applying a sequence where one of the pieces that changes its orientation is unicoloured. We have thus achieved a sequence where one piece changes its orientation and the rest of the cube is left unchanged. This enables all possible orientations of the eleven edge pieces that are not unicoloured, i.e. 2^{11} edge orientations, and all possible orientations of the seven corner pieces that are not unicoloured, i.e. 3^7 corner orientations. We see that the number of possible orientations of edge and corner pieces are the same regardless of the existence of a single unicoloured edge or corner piece. This completes the proof. □

Now we have determined how we need to mark the pieces in order to obtain a group structure and may draw conclusions on the group we can obtain.

Proposition 6.1.12. *The smallest group one can obtain by marking identical pieces and different facets of unicoloured pieces of the corner coloured cube that is a subgroup of Rubik's Group is Rubik's Group itself.*

Proof. From Lemma 6.1.7 we see that the ordinary binary operator is not well defined when we have identical pieces, thus giving us the same number and structure of positions for edge pieces and corner pieces for the smallest possible group structure as for Rubik's Group. From Lemma 6.1.8 we see that we cannot have two identical center facets, unless all center facets are identical to their opposite center facets. However, with the corner coloured cube we do not have all center facets identical to their opposite center facets, and therefore we need to have no identical center facets. With no identical center facets, we have the same number and structure of positions as for Rubik's Group defined from one fixed piece. From Lemma 6.1.4 we see that we cannot have more than one unicoloured piece of each kind and still have the binary operator yield a group together with the different scramblings of the cube. Lemma 6.1.11 shows that one unicoloured piece does not make a difference in the cardinality of the group. Hence, the smallest group structure of the positions of the pieces is the structure of Rubik's Group and the smallest group structure of orientations of corner and edge pieces is the structure of Rubik's Group. This completes the proof. □

Although we know that the different scramblings of the corner coloured cube do not form a group, we may determine how many different scramblings there are. In order to determine this, we start by determining the number of different corner positions there are.

Lemma 6.1.13. *The number of different corner positions is* $\binom{8}{1,1,3,3}$.

Proof. This proof is strictly combinatorial. From Figure 6.2 we see that we have four kinds of corner pieces. One with three black facets, one with three white facets, three with two black and one white facet and three with one black and two white facets. We know from section 1.3.2 that any positioning of these corner pieces is allowed if matched with a suitable positioning of the edge pieces. Thus, we have 8 positions where we are supposed to place three identical black-black-white pieces, three identical black-white-white pieces, one unicoloured black piece and one unicoloured white piece. From basic combinatorics, we know that the number of ways in which we can do this is $\binom{8}{1,1,3,3}$. This completes the proof. □

The next thing to determine is the number of ways in which we can position the edge pieces.

Lemma 6.1.14. *The number of different edge positions is* $\binom{12}{3,3,6}$.

Proof. This proof is strictly combinatorial. From Figure 6.3 we see that we have three different kinds of edge pieces. Three unicoloured white pieces, three unicoloured black pieces and six black-and-white pieces. We know from section 1.3.2 that any positioning of the edge pieces is possible as long as it is matched with a suitable positioning of the corner pieces. Thus, we have 12 positions where we are supposed to place three identical white pieces, three identical black pieces and six identical black-and-white pieces. From basic combinatorics we know that the number of ways to do this is $\binom{12}{3,3,6}$. This completes the proof. □

To completely determine the number of positions that can be achieved we need to investigate whether every corner position can be matched with every edge position.

Lemma 6.1.15. *Every corner position can be matched with every edge position. The total number of different positions is* $\binom{8}{1,1,3,3} \cdot \binom{12}{3,3,6}$.

Proof. We know from Lemma 1.3.13 that every corner position represented by an odd permutation can be matched with every edge position represented by an odd permutation and that every corner position represented by an even permutation can be matched with every edge position represented by an even permutation. Now consider a position of corner pieces described by the permutation σ_c. Let corners 1 and 2 be identical and consider the position of corner pieces described by the permutation $\sigma_c \cdot (12)$. Since corners 1 and 2 are identical, the positions described by σ_c and $\sigma_c \cdot (12)$ are the same. Since we have considered an arbitrary position we see that any corner position can be described by both even and odd permutations. Now consider an edge position described by the permutation σ_e and let edges 1 and 2 be identical. Consider the position described by $\sigma_e \cdot (12)$. We realise that this position is the same as the one described by σ_c since edges 1 and 2 are identical. Since

σ_c is an arbitrary position, every edge position can be described by both even and odd permutations. Since every position, both for corners and edges, can be described by both even and odd permutations, every combination of edge and corner positions is allowed. This gives us the total number of different positions as the product of the number of corner positions and the number of edge positions, i.e. $\binom{8}{1,1,3,3} \cdot \binom{12}{3,3,6}$. This completes the proof. □

We now only need to determine the number of different corner orientations and edge orientations we may have in order to completely determine the number of different possible scramblings.

Lemma 6.1.16. *The number of different corner orientations that are possible is* 3^6.

Proof. From Figure 6.2 we know that we have two unicoloured corner pieces, and six corner pieces that can be oriented in three different ways. From section 1.3.3 we know that in order to change the orientation of one corner piece, we need to change the orientation of another corner piece. We also know that there are rotations such that the orientation of two corner pieces are changed, but the rest of the cube stays the same. Consider a rotation where two corner pieces have their orientation changed. Let one of these corners be unicoloured. The orientation change of this piece will not be noticed, and thus we have rotations that only change the orientation of one corner piece. Hence, all different orientations of the corner pieces are possible. Since we have six corner pieces that can be oriented in three different ways, we have a total of 3^6 different corner orientations. This completes the proof. □

In the final step in order to determine the number of different scramblings, we need to determine the number of possible edge orientations.

Lemma 6.1.17. *The number of different edge orientations that are possible is* 2^6.

Proof. From Figure 6.3 we know that we have six unicoloured edge pieces and six edge pieces that can be oriented in two different ways. From section 1.3.3 we know that in order to change the orientation of one edge piece, we need to change the orientation of another edge piece. We also know that there are rotations such that two corner pieces change orientation whereas the rest of the cube is left unchanged. Consider one such rotation. Let one of the edge pieces that change orientation be a unicoloured piece. The orientation change of this piece will not show and thus we have rotations that only change the orientation of one edge piece. Hence, every different orientation of the edge pieces will be possible. Since we have six edge pieces that can be oriented in two different ways, we have a total of 2^6 different edge orientations. This completes the proof. □

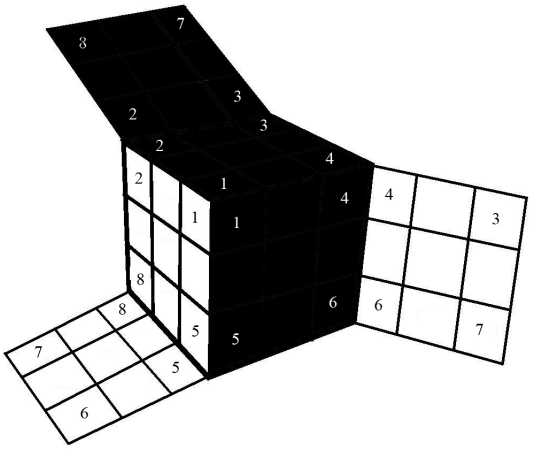


Figure 6.4: Numbering of the corner pieces of the strip colouring.

With the previous lemmas, we may now determine the number of different scramblings of the corner coloured cube.

Theorem 6.1.18. *The number of different scramblings of the corner coloured cube is* $\binom{8}{3,3,1,1} \cdot \binom{12}{3,3,6} \cdot 3^6 \cdot 2^6$.

Proof. We know from section 1.3.4 that any corner and edge orientation can be combined with any position of the pieces. From Lemmas 6.1.15, 6.1.16 and 6.1.17 we have determined the number of positions, corner orientations and edge orientations and the total number of different scramblings is just the product of these numbers. This completes the proof. □

6.1.3 The Strip Colouring

As opposed to the corner coloured cube, the strip coloured cube does not have any fixed pieces. Thus, in order to be able to treat the strip coloured cube in the same way as Rubik's Cube and the corner coloured cube, we need to lock the strip coloured cube in space, or equivalently, specify which of rotations from $\{F, B, R, L, U, D\}$ that rotate which particular face. Assume we do that.

We now want to investigate whether or not the strip coloured cube form a group with the binary operator from Rubik's Group. We start out by specifying the pieces. From Figure 6.4 we see that we have two different kinds of corner pieces, namely the black-black-white ones and the black-white-white ones. In addition, we have three different kinds of edge pieces, the black ones, the white ones and the black-and-white ones.

Now that we have determined the different pieces we have to work with, we can determine whether or not the different scramblings of the strip

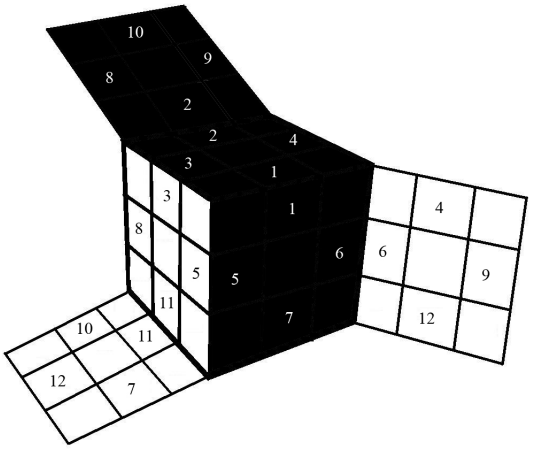


Figure 6.5: Numbering of the edge pieces of the strip colouring.

coloured cube form a group with the concatenation of rotations as the binary operator.

Theorem 6.1.19. *The different scramblings of the strip coloured cube do not form a group with the concatenation of rotations as the binary operator.*

Proof. By Lemmas 6.1.1, 6.1.3 and 6.1.4 we know that the specified binary operator does not yield a group when we have three identical pieces, or two identical pieces of each kind, or two unicoloured pieces of the same kind. With the strip colouring, we have two groups of four identical corner pieces, two groups of two identical edge pieces, one group of eight identical edge pieces, and four unicoloured edge pieces. Thus, the binary operator is far away from being well defined. Hence, we cannot obtain a group with the specified binary operator. □

Since we already know that the corner coloured cube does not form a group of the same kind as Rubik's Group, we might have expected this result for the strip coloured cube. However, it is still surprising that the strip coloured cube does not have a group structure similar to the one of Rubik's Cube if one only considers how similar Rubik's Cube and the strip coloured cube are as objects. In the same way as in the case of the corner coloured cube, we may now also draw some conclusions regarding the sequences of rotations that leave the strip coloured cube unchanged.

Corollary 6.1.20. *The set of sequences of rotations in* $< F, B, U, D, R, L >$ *that leave the strip coloured cube unchanged does not form a normal subgroup in* $\mathfrak{G}_R$.

Proof. Assume that the set of sequences of rotations in $< F, B, U, D, R, L >$ that leave the strip coloured cube unchanged does form a normal subgroup,

N, in $\mathfrak{G}_R$. Then one can form the quotient group $\mathfrak{G}_R/N$. The elements in this group would be precisely the different scramblings of the strip coloured cube. But we know from Theorem 6.1.19 that these elements do not form a group with the binary operator of concatenation of rotations. Hence the set of sequences of rotations that leave the strip coloured cube unchanged cannot be a normal subgroup in $\mathfrak{G}_R$. This completes the proof. □

We might try, as we did with the corner coloured cube, to mark the identical pieces and identical facets of the unicoloured pieces in order to obtain some kind of group structure. However, we will end up with Rubik's Group for this colouring as well.

Proposition 6.1.21. *The smallest group one can obtain by marking identical pieces and different facets of unicoloured pieces of the strip coloured cube that is a subgroup of Rubik's Group is Rubik's Group itself.*

Proof. The proof is completely analogous to the proof of Proposition 6.1.12. □

Although the strip coloured cube does not form a group with its different scramblings and the natural binary operator, we might still, as well as for the corner coloured cube, determine the number of different scramblings that are possible with this colouring. In order to determine this, we start by determining the number of different corner positions.

Lemma 6.1.22. *The number of different positions of the corner pieces is* $\binom{8}{4,4}$.

Proof. This proof is strictly combinatorial. We know from section 1.3.2 that any corner position is possible, as long as it is matched with an appropriate edge position. From Figure 6.4 we know that we have four identical pieces with two black facets and one white facet, and four identical pieces with one black facet and two white facets. These pieces are supposed to be placed in 8 positions. From basic combinatorics we know that this can be done in $\binom{8}{4,4}$ ways. This completes the proof. □

The next step in order to determine the number of different scramblings is to determine the number of different edge positions.

Lemma 6.1.23. *The number of different positions of the edge pieces is* $\binom{12}{2,2,8}$.

Proof. This proof is strictly combinatorial. We know from section 1.3.2 that any edge position is possible, as long as it is matched with an appropriate corner position. From Figure 6.5 we know that we have two identical black edge pieces, two identical white edge pieces and eight identical black-and-white edge pieces. These pieces are supposed to be placed in 12 positions.

From basic combinatorics we know that this can be done in $\binom{12}{2,2,8}$ ways. This completes the proof. □

Now that we have determined the number of different corner and edge positions, the natural thing to do is to determine whether all positions can occur together.

Lemma 6.1.24. *Every edge position can be obtained together with every corner position. The total number of different positions is* $\binom{8}{4,4} \cdot \binom{12}{2,2,8}$.

Proof. We know from Lemma 1.3.13 that every corner permutation represented by an odd permutation is allowed together with every edge position represented by an odd permutation, and that every corner permutation represented by an even permutation is allowed with every edge position represented by an even permutation. Now consider a permutation σ, it might describe the position of either corners or edges. Let corners, or edges, 1 and 2 be identical pieces. Then $\sigma \cdot (12)$ describes the same position of corners, or edges, as σ. Since σ is an arbitrary positioning of corners, or edges, we see that any positioning of corners, or edges, may be written as both even and odd permutations. Hence, any corner position is allowed with any edge position and the total number of positions possible is the number of positions for the corners multiplied by the number of positions for the edges, i.e. $\binom{8}{4,4} \cdot \binom{12}{2,2,8}$. This completes the proof. □

Now that the number of different positions are determined, we need to determine the number of different orientations that are possible.

Lemma 6.1.25. *The number of different orientations of the corner pieces is* 3^7.

Proof. From Figure 6.4 we know that the strip coloured cube have no unicoloured corner pieces. This is the same situation as with the corners of the ordinary Rubik's Cube. Hence, the statement follows from Lemma 1.3.22. □

Lemma 6.1.26. *The number of different orientations of the edge pieces is* 2^8.

Proof. From Figure 6.5 we know that the strip coloured cube have four unicoloured edge pieces. We know from section 1.3.4 that there are rotations of the cube that flip the orientation of two edges, and leave the rest of the cube unchanged. Now consider one of these rotations where one of the edge pieces that is being flipped is a unicoloured edge piece. Then the only visible difference of the cube will be one flipped edge piece. Thus, there are rotations such that one edge piece is flipped and the rest of the cube is left unchanged. There are 8 oriented edge pieces that can be flipped in two ways. Hence, the number of possible orientations of the edge pieces is 2^8. This completes the proof. □

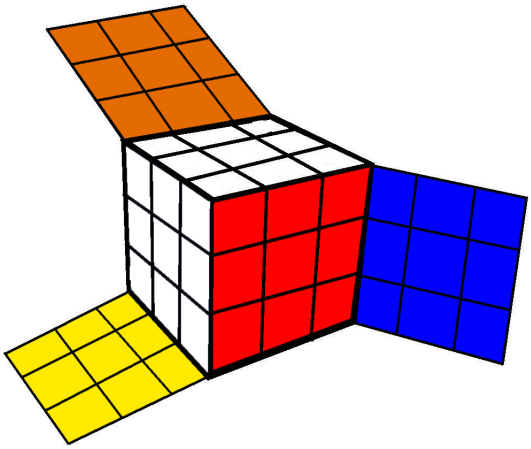


Figure 6.6: A five-coloured cube where two adjacent faces have the same colour.

We have now done all the work to determine the number of different scramblings of the strip coloured cube.

Theorem 6.1.27. *The number of different scramblings of the strip coloured cube is* $\binom{8}{4,4} \cdot \binom{12}{2,2,8} \cdot 3^7 \cdot 2^8$.

Proof. From Lemmas 6.1.24, 6.1.25 and 6.1.26 we know the numbers of these positions and orientations of corner and edge pieces. We know from section 1.3.4 that any positioning is allowed with any orientation of edges and corners, making the total number of different scramblings the product of the numbers determined in the above mentioned lemmas. This completes the proof. □

6.1.4 Other colourings with less than six colours

We have in the two previous sections realised that there is no way to form a group of the different scramblings of a black-and-white cube with the binary operator of concatenation of rotations, unless we mark identical pieces and orient unoriented pieces. The question that arises now is how many colours we need in order to form a group of the different scramblings of the cube with the above mentioned binary operator. We know that we get a group if we have six colours, namely the Rubik's Group, but can one define a group structure with less colours?

Theorem 6.1.28. *The lowest number of colours of the cube, that is greater than one, that enables one to form a group of the different scramblings of the cube with concatenation of rotations of the cube as the binary operator is six.*

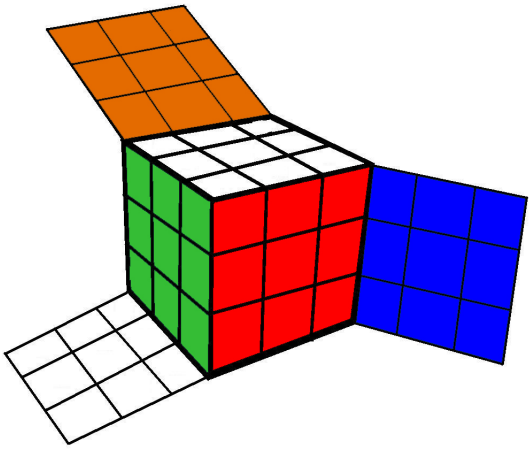


Figure 6.7: A five-coloured cube where two opposite faces have the same colour.

Proof. We know that if we have six colours, and colour each side of a cube in a unique colour, the different scramblings of this cube together with the binary operator of concatenating rotations of the cube form Rubik's Group. Now consider a cube coloured with five different colours. The two faces with the same colour will either be adjacent or opposite. First consider the situation where the two faces are adjacent. We see from Figure 6.6 that there are two faces, in this case the red and the orange, that have two adjacent faces with the same colour. Thus, there will be two pairs of edge pieces that are identical. From Lemma 6.1.2 we know that the binary operator does not yield a group for this case. Thus, this configuration does not give rise to a group.

Now consider the situation where the two faces with the same colour are opposite. We see from Figure 6.7 that all remaining faces, i.e. non-white faces, have two adjacent faces of the same colour and will thus have two identical edge pieces. In total we have four pairs of identical edge pieces. From Lemma 6.1.2 we know that the binary operator does not yield a group for this case. Hence, this configuration will not give rise to a group.

For colourings with less than five colours we realise that we will always have at least two faces that have the same colour. From the above reasoning we see that the binary operator will never be well defined for any of these configurations, and thus no colouring with less than six colours, and more than one colour, will give rise to a group structure. This completes the proof. □

Remark 6.1.29. We note that if the cube only has one colour, we have a group, since all rotations leave the cube unchanged, and thus we only have

the identity.