UNIVERSITY OF HELSINKI
Department of Mathematics and Statistics

Semidirect products and Rubik's cube

Master's thesis

Author: Nicola Bagalà

Supervisor: Johanna Rämö

Academic Year 2016-2017

HELSINGIN YLIOPISTO — HELSINGFORS UNIVERSITET — UNIVERSITY OF HELSINKI

Tiedekunta/Osasto — Fakultet/Sektion — Faculty	Laitos — Institution — Department
Faculty of Natural Sciences	Department of Mathematics and Statistics

Tekijä — Författare — Author
Nicola Bagalà

Työn nimi — Arbetets titel — Title

Semidirect products and Rubik's cube

Oppiaine — Läroämne — Subject
Mathematics

Työn laji — Arbetets art — Level	Aika — Datum — Month and year	Sivumäärä — Sidoantal — Number of pages
Master's thesis	May 2017	58

Tiivistelmä — Referat — Abstract

Given two groups, there are several ways of obtaining news ones. This work focuses on three of these ways: the direct, semidirect, and wreath products. These three products can be thought of as subsequently 'building upon' each other, since the definition of semidirect product depends on the concept of direct product, and wreath products are essentially a particular example of semidirect product.

The concepts above were explored both theoretically and practically, by means of several different examples as well as some digressions from the main topics for the benefit of interested readers. The most substantial and convoluted examples of semidirect and wreath products were given in the last section, where the algebraic structures of *Rubik's group* and of the *illegal* Rubik's group are introduced. These are the groups of, respectively, all legal and *possible* (legal or illegal) moves one can perform on Rubik's cube. An illegal move is such that it cannot be performed without taking the cube apart and reassembling it differently.

Rubik's group is generated by all legal basic moves that can be performed on Rubik's cube—for example, twisting a face of the cube left or right. This extremely large-sized group contains two particular subgroups, namely the subgroups of orientation-preserving and position-preserving moves. The first is such that any of the moves in it, if applied to the cube, will leave the orientation of all the cube's 'cubies' unchanged with respect to a labelling system priorly established on the cube itself, though they may change the position of the cubies. Similarly, the elements of the subgroup of position-preserving moves will not change the position of the cubies, but they may change their orientation. The main result proved in this work is that the legal Rubik's group is the semidirect product of the orientation-preserving and position-preserving subgroups. The method used is mainly based on, and it expands upon, that used by Charles Bandelow in his book *Inside Rubik's cube and beyond*. A second fact—that the *illegal* Rubik's group is isomorphic to a direct product of wreath products—was also proved as a secondary goal.

Avainsanat — Nyckelord — Keywords
Rubik's cube, direct product, semidirect product, wreath product, Rubik's group

Säilytyspaikka — Förvaringsställe — Where deposited
Kumpulan tiedekirjasto

Muita tietoja — Övriga uppgifter — Additional information

Contents

1 Introduction

The so-called *Rubik's cube* is a mechanical puzzle invented in 1974 by Hungarian sculptor and professor of architecture Ernő Rubik. Since its introduction on the toy market in 1980, hundreds of millions of Rubik's cubes have been sold, making it one of the world's best-selling toy and definitely one of the most well-known puzzles of all times.

Aside from being cause of severe headaches for solvers of all ages, Rubik's cube (henceforth often only 'the cube') lends itself to the application of numerous group-theoretical concepts, and has been the subject of many algebra books. The algebra of the cube involves both rather elementary notions—like permutations and groups—and more advanced ones, like semidirect products and wreath products. These two last concepts are at the core of the scope of this work.

Our main goal shall be to prove that *Rubik's group*—the group generated by all legal moves that can be performed on the cube—is the semidirect product of two of its subgroups, namely the subgroup of position-preserving and orientation-preserving moves. We will subsequently prove that Rubik's group is also isomorphic to the wreath product of two semidirect products of cyclic and symmetric groups.

We will first give a short account of some basic required concepts, for the benefit of any readers less acquainted with the subject. While direct products are not, strictly speaking, objects of our interest, they are necessary to understand both semidirect and wreath products, and will therefore be discussed in their own section. We will then discuss semidirect products and wreath products, sometimes touching topics that are not directly related to the scope of this work but may be of interest for the reader. Finally, the last section will discuss Rubik's group more in detail, defining an operation on it and eventually proceeding to proving the aforementioned claims. The interested reader will find plenty of material for further reading in the References section.

2 Preliminaries

In this section, we summarise a few key concepts whose understanding is indispensable to read this work. Readers who may need a refresher should consider reading this section before proceeding further. For a more detailed introduction to the fundamentals of abstract algebra, see for example Pinter's book [1]. For reasons of brevity, we will not give proof of any of the basic facts in this section. The interested reader can refer to any introductory algebra book.

2.1 Basic concepts

Definition 2.1. A **group** is a set G equipped with an associative binary operation $\star$ such that

- there exists an **identity element** $e \in G$ such that $a \star e = e \star a = a$ for every $a \in G$, and
- for every element $a \in G$, there is an **inverse element** a^{-1} such that $a \star a^{-1} = a^{-1} \star a = e$.

The operation $\star$ is not necessarily commutative; if it is, we say G is an **abelian** group. A subset H of G that is still a group with respect to the operation $\star$ defined on G is called a **subgroup** of G; this relation is denoted as $H \leq G$.

It is customary not to use any special symbol to indicate the operation defined on a group; thus, $a \star b$ usually becomes simply ab. The identity of a group G is often indicated as 1_G; when no danger of confusion arises, it is simply denoted as 1.

For the rest of this section, capitalised latin letters (e.g. G, H, etc.) are intended to be groups, unless otherwise specified.

Definition 2.2. If $a, x \in G$, then $xax^{-1} \in G$ is called a **conjugate** of a. If $H \leq G$, H is called a **normal** subgroup of G if $ghg^{-1} \in H$ whenever $g \in G$ and $h \in H$. If H is normal in G, we will write $H \lhd G$.

Theorem 2.1. *If $H \leq G$ and $K \lhd G$, then their product $HK = \{hk \mid h \in H, k \in K\}$ is a subgroup of G.*

Proof. Omitted. □

Definition 2.3. If $H \leq G$, the symbol Ha denotes the set of all products of the form ha, for any $h \in H$ and where $a \in G$ is fixed. This set is called a **right coset** of H in G. **Left cosets** are defined analogously. The set G/H of all (right) cosets of H in G is called the **quotient set** of G.

Theorem 2.2. *Let $H \lhd G$. For any $Ha, Hb \in G/H$, the operation*

$$(Ha)(Hb) = H(ab)$$

is well defined; the set G/H, equipped with this operation, is a group.

Proof. Omitted. □

The normality of a subgroup is equivalent to several other conditions; for example, in terms of cosets, we have $H \lhd G$ if and only if $gHg^{-1} = H$ for any $g \in G$, and $H \lhd G$ if and only if $gH = Hg$ for any $g \in G$.

Definition 2.4. Let G, H be groups. A function $f\colon G \to H$ such that $f(ab) = f(a)f(b)$ for any two elements $a, b \in G$ is called a (**group**) **homomorphism** from G onto H. If f is a bijection, we say f is an **isomorphism**. An isomorphism from G to itself is called an **automorphism**. If G is isomorphic to H, we write $G \cong H$.

Definition 2.5. If $f\colon G \to H$ is a group homomorphism, its **kernel** $K \subset G$ is the set of all $g \in G$ such that $f(g) = 1$. The kernel of f is written usually as $\ker f$.

Note that, if $f\colon G \to H$ is a homomorphism, then $f(1) = f(1 \cdot 1) = f(1)f(1)$ implies $f(1) = 1$, and thus $1 \in \ker f$. Furthermore, one can prove that $\ker f \lhd G$.

Theorem 2.3. *If f is an injective group homomorphism, $\ker f = \{1\}$.*

Proof. Omitted. □

Theorem 2.4. *Let G and H be groups, and let $f\colon G \to H$ be a group homomorphism between them. If $A \leq G$, then $f(A) \leq H$.*

Proof. Omitted. □

2.2 Isomorphism Theorems

The Isomorphism Theorems, proved by Emmy Noether in 1927, establish important relations between quotient sets. The proof of each of these theorems can be found for example in [2], pp. 35-37.

Theorem 2.5. *(First Isomorphism Theorem) Let $f : G \to H$ be a homomorphism with kernel K. Then $K \lhd G$ and $G/K \cong \operatorname{im} f$, where $\operatorname{im} f \subset H$ is the image of G under f.*

Proof. Omitted. □

Theorem 2.6. *(Second Isomorphism Theorem) Let N and T be subgroups of G such that $N \lhd G$. Then $(N \cap T) \lhd T$; furthermore, $T/(N \cap T) \cong NT/N$.*

Proof. Omitted. □

3 Direct products

Given two groups, it is possible to obtain a new one in several ways. One of the simplest ways is taking their so-called *direct product*. The interested reader may find more on this subject in [4] and [2].

3.1 External and internal direct products

Definition 3.1. If H and K are two groups, their **external direct product** $H \times K$ is the group of all ordered pairs (h, k), where $h \in H$, $k \in K$ and the group operation is given by

$$(h, k)(h'k') = (hh', kk').$$

Remark 3.1. Notice that the same $\times$ symbol is used to indicate the Cartesian product of two sets and the external direct product of two groups. This must not be source of confusion, since the set underlying the external direct product of two groups H and K is indeed their Cartesian product $H \times K$.

It is easy to see that $(1, 1)$ is the identity of $H \times K$, and that the inverse of an element (h, k) is (h^{-1}, k^{-1}). Associativity easily follows from associativity in H and K. It is worth noticing that neither H, nor K are subgroups of $H \times K$; however, their isomorphic replicas $H \times \{1\}$ and $\{1\} \times K$ are both subgroups of $H \times K$.

We will now define a different 'version' of the direct product.

Definition 3.2. Let G be a group with normal subgroups H and K such that $G = HK$ and $H \cap K = \{1\}$. Then G is said to be the **internal direct product** of H and K.

Informally speaking, the *external* direct product builds a new group out of two any other groups; an already existing group whose elements can be expressed as products of elements of two of its normal subgroups is the *internal* direct product of said subgroups.

We will now give a few examples of direct product of groups.

Example 3.1. The set $\mathbb{R}^2$, seen as the additive group $(\mathbb{R}^2, +)$, is given by the external direct product of the group $(\mathbb{R}, +)$ by itself. While $\mathbb{R} \nleq \mathbb{R}^2$, its isomorphic replica $\mathbb{R} \times \{0\}$ is a subgroup of $\mathbb{R}^2$.

Example 3.2. The external direct product of the groups $\mathbb{Z}_2$ and $\mathbb{Z}_3$ is the group $\mathbb{Z}_2 \times \mathbb{Z}_3 = \{(0_2, 0_3), (0_2, 1_3), (0_2, 2_3), (1_2, 0_3), (1_2, 1_3), (1_2, 2_3)\}$, with the normal multiplication of equivalence classes as the group operation.

Example 3.3. The 4-group $V = \{1, (12)(34), (13)(24), (14)(23)\}$ is the internal direct product of its subgroups $H = \{1, (12)(34)\}$ and $K = \{1, (13)(24)\}$. One can readily check that H and K are normal and such that $HK = V$.

Example 3.4. Let $\mu\colon G \times G \to G$ be the binary operation on the group G, i.e. $\mu(a, b) = ab$ for every $a, b \in G$. Then μ is a homomorphism from the external direct product $G \times G$ to G if and only if G is abelian; indeed,

$$\mu((a, b)(c, d)) = \mu(ac, bd) = acbd \overset{(\star)}{=} abcd = \mu(a, b)\mu(c, d), \text{ for all } a, b, c, d \in G$$

where the equality marked with $(\star)$ holds if and only if G is abelian.

One may think of the direct product as the group-equivalent of multiplication of numbers or polynomials. Just like the numbers 12 and 4 can be multiplied to give rise to the number 48, or the polynomials $x - 1$ and $x - 4$ can be multiplied into $x^2 - 5x + 4$, two groups H and K give rise to a new group $H \times K$. To push the analogy further, we can observe that, given a number (or a polynomial), it is possible to decompose it into prime factors (or irreducible polynomials): for example, $48 = 3 \times 2^4$ and $x^2 - 5x + 4 = (x - 1)(x - 2)(x + 2)$; is there any similar operation for groups as well? Let us consider an example.

Example 3.5. Let $K_4 = \{1, a, b, c\}$ be the *Klein 4-group* with the multiplication table illustrate in Table 1 below:

$\cdot$	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

Table 1: The multiplication table of the Klein 4-group.

The subgroups $A = \{1, a\}$ and $B = \{1, b\}$ are normal in K_4, their intersection contains only 1, and they are such that $AB = K_4$. In other words,

K_4 is the internal direct product of A and B. We can define an isomorphism $\phi\colon A \times B \to K_4$ as

$$\phi(\alpha, \beta) = \alpha\beta, \qquad \text{for all } \alpha \in A \text{ and } \beta \in B$$

and thus 'factor' K_4 into its two subgroups A and B. (To see why ϕ is an isomorphism, let $\alpha_1, \alpha_2 \in A$ and $\beta_1, \beta_2 \in B$, and compute

$$\begin{aligned}\phi((\alpha_1, \beta_1)(\alpha_2, \beta_2)) &= \phi(\alpha_1\alpha_2, \beta_1\beta_2) = \alpha_1\alpha_2\beta_1\beta_2 \\ &\overset{(\star)}{=} \alpha_1\beta_1\alpha_2\beta_2 = \phi(\alpha_1, \beta_1)\phi(\alpha_2, \beta_2)\end{aligned}$$

where in $(\star)$ we have made use of the fact that K_4 is abelian. To prove injectivity, let $\alpha_i \in A$ and $\beta_i \in B$, where $i = 1, 2$, and assume $\phi(\alpha_1, \beta_1) = \phi(\alpha_2, \beta_2)$. This implies $\alpha_1\beta_1 = \alpha_2\beta_2$, and thus $\beta_1 = \alpha_1^{-1}\alpha_2\beta_2$. A patient reader may attempt to substitute for all possible values of α_1, α_2, and β_2 and come to the conclusion that $(\alpha_1, \beta_1) = (\alpha_2, \beta_2)$ each time. Surjectivity is a trivial consequence of the fact K_4 is a group.)

The example above is no special case; it can be generalised to any group, as the following theorem shows.

Theorem 3.1. *Let G be a group with normal subgroups H and K. If $HK = G$ and $H \cap K = \{1\}$, then $G \cong H \times K$.*

Proof. Assume $HK = G$ and $H \cap K = \{1\}$. If $a \in G$, then by assumption $a = hk$ for some $h, k \in H, K$ respectively; the first thing we need to make sure of is that this expression for a is unique. To this end, let $a = h_1k_1$ be another such factorisation, where $h_1 \in H$ and $k_1 \in K$; then, $h_1k_1 = hk$, whence $kk_1^{-1} = h^{-1}h_1$. But now $kk_1^{-1} \in K$ and $h^{-1}h_1 \in H$, and since they are equal, they both belong to $H \cap K$. Since $H \cap K = \{1\}$ by assumption, we have $kk_1^{-1} = 1$ and $h^{-1}h_1 = 1$, and ultimately $h = h_1$, $k = k_1$ by uniqueness of inverses.

Let us now define $f\colon G \to H \times K$ by $f(a) = (h, k)$, where $a = hk$, and show that it is an isomorphism. What f does is 'pairing up' the H and K factors of a; if we consider aa', where $a' \in G$ and $a' = h'k'$, we get $f(aa') = f(hkh'k')$, and it is not clear what the H and K factors are. We can shed some light on that by considering the commutator $h'kh'^{-1}k^{-1}$. We know that $H, K \lhd G$, thus by normality $(h'kh'^{-1})k^{-1} \in K$ and also $h'(kh'^{-1}k^{-1}) \in$

H; ultimately, $h'kh'^{-1}k^{-1} \in H \cap K = \{1\}$, whence $h'kh'^{-1}k^{-1} = 1$ and thus h' and k must commute. Armed with this new fact, we now compute

$$f(aa') = f(hkh'k') = f(hh'kk') = (hh', kk') = (h, h')(k, k') = f(a)f(a').$$

This proves f is a homomorphism; to see it's also an isomorphism, we need to prove it is a bijection. Assume $f(a) = f(a')$, where $a = hk$, $a' = h'k'$, and $h, k \in H, K$ as before. Then $(h, k) = (h', k')$ and consequently $h = h'$, $k = k'$, which implies $a = a'$ and thus the injectivity of f. To prove surjectivity, let $(h, k) \in H \times K$, and let $a = hk$. Then $a \in G$, because $G = HK$, and thus $f(a) = (h, k)$. This concludes the proof. □

In essence, Theorem 3.1 says that the external and internal direct products are isomorphic, and therefore there is no need to distinguish between them, algebraically speaking; however, unlike the case of factorisation of numbers or polynomials, the group G is not equal to the direct product of its 'factors'. This fact can be better illustrated by means of the following example.

Example 3.6. Consider the group $V = \{1, (12)(34), (13)(24), (14)(23)\}$ with normal subgroups $H = \{1, (12)(34)\}$ and $K = \{1, (13)(24)\}$ from Example 3.3. All conditions of Theorem 3.1 are met, and thus $V \cong H \times K$. However, the elements of $H \times K$ are pairs of permutations, while V's only elements are individual permutations; thus, the two sets cannot be equal.

It should be noted that the 'factors' of a group in a direct product are by no means unique, except up to isomorphism. For example, consider again the Klein 4-group $K_4 = \{1, a, b, c\}$. We have seen that it is the internal direct product of its subgroups $A = \{1, a\}$ and $B = \{1, b\}$, and that $K_4 \cong A \times B$. However, $C = \{1, c\}$ is also a normal subgroup of K_4 such that $AC = K_4$, and its intersection with A is trivial. Thus, K_4 is the internal direct product of A and C. By Theorem 3.1 above, $K_4 \cong A \times C$, which means K_4 has two distinct factorisations, namely $A \times B$ and $A \times C$. While $B \neq C$, it is easy to verify that the map $\phi\colon B \to C$ defined as $\phi(1) = 1$ and $\phi(b) = c$ is an isomorphism. More generally, if $G \cong H \times K$, then $G \cong A \times B$ whenever $A \cong H$ and $B \cong K$. (If $\phi\colon A \to H$ and $\theta\colon B \to K$ are group isomorphisms, the reader can readily check that the map $\psi : A \times B \to H \times K$ defined by $\psi((a, b)) = (\phi(a), \theta(b))$ is a group isomorphism as well. It follows that $G \cong (H \times K) \cong (A \times B)$.)

The converse of Theorem 3.1 is also true: If a group is isomorphic to the external product of two other groups, it is also the internal product of two of its own normal subgroups, as shown in the following theorem. The proof is based on that found in [9].

Theorem 3.2. *If $G \cong G_1 \times G_2$, then there exist normal subgroups H_1 and H_2 of G such that $G = H_1H_2$ and $H_1 \cap H_2 = \{1\}$.*

Proof. If $G \cong G_1 \times G_2$, then there exists an isomorphism $\phi\colon G_1 \times G_2 \to G$. We can then define

$$H_1 = \phi(G_1 \times \{1\}) = \{\phi(g_1, 1) \,|\, g_1 \in G_1\}$$

$$H_2 = \phi(\{1\} \times G_2) = \{\phi(1, g_2) \,|\, g_2 \in G_2\}$$

Using the fact ϕ is an isomorphism, we can easily show that $H_1 \lhd G$. The inverse of $\phi(g_1, 1) \in G$ is $\phi(g_1^{-1}, 1)$; if $\phi(g_1, 1), \phi(g', 1) \in H_1$, then

$$\phi(g_1^{-1}, 1)\phi(g', 1) = \phi(g_1^{-1}g', 1) \in H_1,$$

because $g_1^{-1}g' \in G_1$. Therefore, by the subgroup criterion, $H_1 \leq G$.

Let now $g \in G$. Then there exists $h \in G_1$ such that $\phi(h, 1) = g$. Since isomorphisms map inverses to inverses, if $\phi(g_1, 1) \in H_1$ we have

$$g\phi(g_1, 1)g^{-1} = \phi(h, 1)\phi(g_1, 1)\phi(h^{-1}, 1) = \phi(hg_1h^{-1}, 1) \in H_1,$$

because $hg_1h^{-1} \in G_1$. Therefore, $H_1 \lhd G$. Similarly, one can prove $H_2 \lhd G$.

To complete the proof, we need to show that $H_1 \cap H_2 = \{1\}$ and that $H_1H_2 = G$. To prove the former, assume $x \in H_1 \cap H_2$. Then $x \in H_1$, and thus there is $(a, 1) \in G_1 \times \{1\}$ such that $\phi(a, 1) = x$. Similarly, $x \in H_2$ implies the existence of $(1, b) \in \{1\} \times G_2$ such that $\phi(1, b) = x$. Thus, $\phi(a, 1) = \phi(1, b)$, and since ϕ is a bijection, we must conclude $(a, 1) = (1, b)$ and $a = b = 1$. Therefore, $x = \phi(1, 1) = 1$, and $H_1 \cap H_2 = \{1\}$.

Finally, to prove $G = H_1H_2$, let $g \in G$. Since ϕ is a surjection, there exists $(a, b) \in G_1 \times G_2$ such that $\phi(a, b) = g$. Therefore,

$$g = \phi(a, b) = \phi(a, 1)\phi(1, b) \in H_1H_2.$$

This implies $G \subset H_1H_2$ and ultimately $G = H_1H_2$. □

Example 3.7. Consider again Example 3.2. Define $f\colon \mathbb{Z}_2 \times \mathbb{Z}_3 \to \mathbb{Z}_6$ as $f(x_2, y_3) = (3x - 2y)_6$ for all $x, y \in \mathbb{Z}$[1]. The values of this function can be written out as

$$f(0_2, 0_3) = 0_6,\ f(0_2, 1_3) = 4_6,\ f(0_2, 2_3) = 2_6,$$

$$f(1_2, 0_3) = 3_6,\ f(1_2, 1_3) = 1_6,\ f(1_2, 2_3) = 5_6.$$

By visual inspection of the values above, we can tell that f is a bijection. For all $x, y, a, b \in \mathbb{Z}$, the following computation proves f is a homomorphism:

$$f((x_2, y_3)(a_2, b_3)) = f(xa_2, yb_3) = (3xa - 2yb)_6 \tag{3.1}$$

$$\begin{aligned} &f(x_2, y_3)f(a_2, b_3) = (3x - 2y)_6(3a - 2b)_6 = ((3x - 2y)(3a - 2b))_6 \\ &= (9xa + 6xb - 6ya + 4yb)_6 = (9xa)_6 + (6xb)_6 - (6ya)_6 + (4yb)_6 \\ &= (3xa + 6xa)_6 - (2yb)_6 = (3xa)_6 - (2yb)_6 = (3xa - 2yb)_6 \end{aligned} \tag{3.2}$$

In (3.2) we have made use of the fact that any integer multiple of 6 is equal to $0 \pmod 6$ and that any integer multiple of 4 is equal to $-2 \pmod 6$. Since the final results in (3.1) and (3.2) are equal, we can conclude that f is a bijective homomorphism and thus an isomorphism between $\mathbb{Z}_2 \times \mathbb{Z}_3$ and $\mathbb{Z}_6$.

Given this fact, according to Theorem 3.2, there should be subgroups of the additive group $\mathbb{Z}_6$ such that $\mathbb{Z}_6$ is their internal direct product; indeed, $\langle 2_6 \rangle \lhd \mathbb{Z}_6$ and $\langle 3_6 \rangle \lhd \mathbb{Z}_6$ are two such groups. If we write them out as $\langle 2_6 \rangle = \{0_6, 2_6, 4_6\}$ and $\langle 3_6 \rangle = \{0_6, 3_6\}$ for clarity, it is immediate to see that they only have the identity 0_6 in common, they are normal, and $\langle 2_6 \rangle \langle 3_6 \rangle = \mathbb{Z}_6$. Notice how $\langle 2_6 \rangle \cong \mathbb{Z}_2$ and $\langle 3_6 \rangle \cong \mathbb{Z}_3$, as one would expect by how H_1 and H_2 were defined in Theorem 3.2.

Theorem 3.3. *If $A \lhd H$ and $B \lhd K$, then $A \times B \lhd H \times K$, and*

$$(H \times K)/(A \times B) \cong (H/A) \times (H/B).$$

[1] To obtain the formula for f, for each pair $(x_2, y_3) \in \mathbb{Z}_2 \times \mathbb{Z}_3$ consider the linear congruences $z \equiv_2 x$ and $z \equiv_3 y$. The Chinese remainder theorem (see e.g. [1], pp 232-234) guarantees the existence of a solution, which can be computed as $z = 3xm_2 + 2ym_1$, where $m_1, m_2 \in \mathbb{Z}$ are solutions to Bézout's identity $2m_1 + 3m_2 = 1$ (see e.g. [11], pp 17-18).

Proof. From the assumption, it follows that $A \times B \subset H \times K$. If $(a, b), (c, d) \in A \times B$, then $(a, b)(c, d)^{-1} = (a, b)(c^{-1}, d^{-1}) = (ac^{-1}, bd^{-1}) \in A \times B$ because $ac^{-1} \in A$ and $bd^{-1} \in B$. Thus, by the subgroup criterion, $A \times B \leq H \times K$. Proving that this subgroup is normal is just a matter of brutal computation: since A and B are normal in H and K respectively, we see that, for any $(a, b) \in A \times B$ and $(h, k) \in H \times K$,

$$(h, k)(a, b)(h, k)^{-1} = (h, k)(a, b)(h^{-1}, k^{-1}) = (hah^{-1}, kbk^{-1}) \in A \times B$$

and thus $A \times B \lhd H \times K$.

Let now $\phi\colon H \times K \to (H/A) \times (K/B)$ be defined by $\phi(h, k) = (Ah, Bk)$. If we could show that ϕ is a surjective homomorphism and that $\ker \phi = A \times B$, then our second claim would follow from the First Isomorphism Theorem. It is easy to see that ϕ is indeed a homomorphism: if $(h, k), (h', k') \in H \times K$, then

$$\begin{aligned} \phi((h, k)(h', k')) &= \phi(hh', kk') = (Ahh', Bkk') \\ &= (AhAh', BkBk') \\ &= (Ah, Bk)(Ah', Bk') \\ &= \phi(h, k)\phi(h', k'). \end{aligned}$$

To prove surjectivity, let x be any element of $(H/A) \times (K/B)$. Then x is a pair of cosets of A and B in H and K respectively, which means there exist $h \in H$ and $k \in K$ such that $x = (Ah, Bk)$. Thus, $(h, k) \in H \times K$ is such that $\phi(h, k) = x$, which proves ϕ is a surjective map. Note that this implies $\operatorname{im} \phi = (H/A) \times (H/B)$. Now, if $(x, y) \in \ker \phi$, then $\phi(x, y) = (Ax, By) = (A, B)$, which implies $x \in A$ and $y \in B$. Thus $\ker \phi \subset A \times B$. On the other hand, if $(a, b) \in A \times B$, then $\phi(a, b) = (Aa, Bb) = (A, B)$, therefore $A \times B \subset \ker \phi$. Ultimately, $\ker \phi = A \times B$; so, by the First Isomorphism Theorem, $(H \times K)/\ker \phi = (H \times K)/(A \times B) \cong \operatorname{im} \phi = (H/A) \times (H/B)$. $\square$

Corollary 3.1. *If $G = H \times K$, then $G/(H \times 1) \cong K$.*

Proof. It is easy to see that $H \lhd H$ and $\{1\} \lhd K$, so by Theorem 3.3 we have

$$\begin{aligned} (H \times K)/(H \times \{1\}) &\cong (H/H) \times (K/\{1\}) \\ &= \{H\} \times \{\{k\} \mid k \in K\} \\ &= \{(H, \{k\}) | k \in K\} \cong K. \end{aligned}$$

To see why the last step is true, define $\psi\colon \{(H,\{k\})|k \in K\} \to K$ as $\psi(H,\{k\}) = k$. This function is obviously a homomorphism, since for all $k_1, k_2 \in K$

$$\begin{aligned}\psi((H,\{k_1\})(H,\{k_2\})) &= \psi(H,\{k_1\}\{k_2\}) = \psi(H,\{k_1k_2\}) \\ &= k_1k_2 = \psi(H,\{k_1\})\psi(H,\{k_2\}).\end{aligned}$$

(Notice that $\{k_1\}$ and $\{k_2\}$ are cosets of $\{1\}$, i.e. $\{k_1\} = k_1\{1\}$ and $\{k_2\} = k_2\{1\}$. Therefore $\{k_1\}\{k_2\} = k_1\{1\}k_2\{1\} = k_1k_2\{1\} = \{k_1k_2\}$.) Moreover, if $k \in K$ then $\psi(H,\{k\}) = k$, and $\psi(H,\{k_1\}) = \psi(H,\{k_2\})$ leads inevitably to $k_1 = k_2$ for all $k_1, k_2 \in K$. Thus, ψ is a bijection, and ultimately an isomorphism. □

3.2 Direct products of an arbitrary number of groups

While thus far we have dealt with the direct product of only two groups, there is no reason we could not consider the direct product of any number of groups. The countable case is simple. Let $G = G_1 \times \cdots \times G_n$ be the direct product of n groups. We define a product between any two elements of G in the usual component-wise fashion:

$$(g_1, \ldots, g_n)(h_1, \ldots, h_n) := (g_1h_1, \ldots, g_nh_n),$$

for all $(g_1, \ldots, g_n), (h_1, \ldots, h_n) \in G$. Since every G_i, where $i = 1, \ldots, n$, is a group, we know $g_ih_i \in G_i$, and thus $(g_1h_1, \ldots, g_nh_n) \in G$. Thus, G is closed with respect to the given operation.

The element $(1_{G_1}, \ldots, 1_{G_n})$ is in G, being an n-tuple of identities of each G_i, and it works as identity for G, since

$$(1_{G_1}, \ldots, 1_{G_n})(g_1, \ldots, g_n) = (1_{G_1}g_1, \ldots, 1_{G_n}g_n) = (g_1, \ldots, g_n),$$

$$(g_1, \ldots, g_n)(1_{G_1}, \ldots, 1_{G_n}) = (g_11_{G_1}, \ldots, g_n1_{G_n}) = (g_1, \ldots, g_n)$$

for every $(g_1, \ldots, g_n) \in G$.

If $(g_1, \ldots, g_n) \in G$, then so is $(g_1^{-1}, \ldots, g_n^{-1})$, and

$$(g_1, \ldots, g_n)(g_1^{-1}, \ldots, g_n^{-1}) = (g_1g_1^{-1}, \ldots, g_ng_n^{-1}) = (1_{G_1}, \ldots, 1_{G_n}),$$

$$(g_1^{-1}, \ldots, g_n^{-1})(g_1, \ldots, g_n) = (g_1^{-1}g_1, \ldots, g_n^{-1}g_n) = (1_{G_1}, \ldots, 1_{G_n}),$$

whence every $(g_1, \ldots, g_n) \in G$ has an inverse element. Ultimately, G is a group for any $n \in \mathbb{N}$.

We indicate the Cartesian product of n groups $G_1, \ldots, G_n$ as

$$\prod_{i=1}^{n} G_i,$$

and when the number of the G_i's is countably infinite,

$$\prod_{i=1}^{\infty} G_i.$$

Although it may be more difficult to visualise, we can take the direct product of an *uncountable* amount of groups as well. This will require a more general definition.

Definition 3.3. Let $\{H_\lambda\}$ be a family of groups H_λ, where λ belongs to an index set Λ. Let us consider the set F of all functions f defined on Λ such that $f(\lambda) \in H_\lambda$ for all $\lambda \in \Lambda$, and define a product on F as

$$(fg)(\lambda) = f(\lambda)g(\lambda)$$

for each $\lambda \in \Lambda$ and $f, g \in F$. Then F, equipped with the above operation, is called the **complete direct product** of the groups H_λ.

Example 3.8. Let $G_x = \mathbb{Z}_3$ for all $x \in \mathbb{R}$. Then

$$F = \prod_{x \in \mathbb{R}} G_x = \left\{ f \colon \mathbb{R} \to \bigcup_{x \in \mathbb{R}} G_x \mid f(x) \in G_x, \text{ for all } x \in \mathbb{R} \right\}$$

is the complete direct product of the groups G_x; the group operation is defined as $(f + g)(x) = f(x) + g(x)$ for all $f, g \in F$ and all $x \in \mathbb{R}$. An example of an element of this group is the function f such that

$$f(x) = \begin{cases} 0_3, \text{ if } x \leq -1 \\ 1_3, \text{ if } x \in (-1, 1) \\ 2_3, \text{ if } x \geq 1 \end{cases}$$

whose inverse is the function f^{-1} such that

$$f^{-1}(x) = \begin{cases} 0_3, \text{ if } x \leq -1 \\ 2_3, \text{ if } x \in (-1, 1) \\ 1_3, \text{ if } x \geq 1 \end{cases}$$

It is easy to see that, for any $x \in \mathbb{R}$, $(f + f^{-1})(x) = 0_3$, as expected. To prove that F is a group, for each $f \in F$ and each $z \in \mathbb{Z}_3$ consider the sets

$$F_z^f = \{x \in \mathbb{R} \,|\, f(x) = z\}\,;$$

in other words, each F_z^f is the subset of $\mathbb{R}$ on which f assumes value $z \in \mathbb{Z}_3$. For every $x \in F_z^f$, the function $g \in F$ defined as $g(x) = -z$ is such that $(f + g)(x) = 0_3 = (g + f)(x)$; since $\mathbb{R} = \bigcup_{z \in \mathbb{Z}_3} F_z^f$, then $(f + g)(x) = 0_3 = (g + f)(x)$ for all $x \in \mathbb{R}$, whence $g = f^{-1}$. It is easy to check that F is closed under addition, and the function i such that $i(x) = 0_3$ for every $x \in \mathbb{R}$ is in F. Consequently, F is a group.

Definition 3.3 expands the notion of direct product to allow for uncountably many factors. An element in a finite direct product of the form $H_1 \times H_2 \times \ldots H_n$, where $n < \infty$, is a sequence $(h_1, h_2, \ldots, h_n)$ where $h_i \in H_i$; if the number of the H_i's is countably infinite with index set $\mathbb{N}$, then we have an infinite sequence

$$(h_1, h_2, \ldots, h_m, h_{m+1}, \ldots).$$

If the index set Λ is $\mathbb{Z}$, for example, then the elements of the direct product of $|\mathbb{Z}|$ groups would be sequences of the form

$$(\ldots, h_{-m-1}, h_{-m}, \ldots, h_0, h_1, \ldots, h_m, h_{m+1}, \ldots),$$

unbounded both from above *and* below. However, in the most general case of infinite direct product, we must account for the possibility that the index set Λ may be uncountable, in which case discrete sequences turn into functions of a continuous variable. In this new setting, the condition $f(\lambda) \in H_\lambda$ means loosely speaking that at 'place λ' of the function there is an element from the group H_λ, in analogy with the discrete case.

Proposition 3.1. *The complete direct product in Definition 3.3 is a group with respect to the given operation.*

Proof. If $f, g \in F$ and $\lambda \in \Lambda$, then by definition $fg(\lambda) = f(\lambda)g(\lambda) \in H_\lambda$, implying that $fg\colon \Lambda \to \bigcup_{\lambda\in\Lambda} H_\lambda$. Therefore, F is closed with respect to its binary operation. Associativity follows trivially from associativity in each H_λ. Let $i\colon \Lambda \to \bigcup_{\lambda\in\Lambda} H_\lambda$ be such that $i(\lambda) = 1_{H_\lambda}$ for every $\lambda \in \Lambda$. Clearly $i \in F$ and $f(\lambda)i(\lambda) = f(\lambda)1_{H_\lambda} = f(\lambda)$ for every $\lambda \in \Lambda$, since $f(\lambda) \in H_\lambda$. Similarly, $i(\lambda)f(\lambda) = f(\lambda)$. Thus, F has an identity element. Finally, if $f \in F$, define a function $g\colon \Lambda \to \bigcup_{\lambda\in\Lambda} H_\lambda$ such that $g(\lambda) = (f(\lambda))^{-1}$ for all $\lambda \in \Lambda$. Then $fg(\lambda) = f(\lambda)(f(\lambda))^{-1} = 1_{H_\lambda} = i(\lambda)$, and similarly $gf(\lambda) = i(\lambda)$, whence $g = f^{-1}$.Ultimately, F is a group. □

In the case of an uncountable index set, we cannot define the direct product in the normal way, and we must define it as above instead. Nonetheless, we can anyway make use of the notation

$$\prod_{\lambda\in\Lambda} H_\lambda$$

regardless of the cardinality of Λ.

4 Semidirect products

We will now construct a generalised version of the direct product; like the direct product itself, this generalisation as well comes into two equivalent fashions. Before proceeding to the construction, we will give a brief account of the concept of *action* of a group, which our construction will rely on.

4.1 Group actions

Definition 4.1. Let G and H be two groups. If there exists a homomorphism ϕ from G into $\mathrm{Aut}\, H$, we say that G **acts** on H via ϕ. We will call ϕ a (**group**) **action** of G on H.

Remark 4.1. To avoid cumbersome notation, if $\phi(g) \in \mathrm{Aut}\, H$ is an automorphism of H (where $g \in G$ and ϕ is an action of G on H) we will sometimes write it as ϕ_g. So, for example, the image of $h \in H$ under $\phi(g)$ will be written as $\phi_g(h)$, rather than $\phi(g)(h)$.

If we made use of Definition 4.1 as it is, proving that a map ϕ is a group action of group G on group H could be quite laborious and tedious, because we would have to prove, among other things, that ϕ_g is a bijection from H to itself for every $g \in G$. However, the following lemma will make things easier.

Lemma 4.1. *Let G and H be groups. Then a map $\phi : G \to H^H$ is an action as described in Definition 4.1 if and only if*

(i) $\phi_{gf} = \phi_g \phi_f$ *for every* $g, f \in G$,

(ii) $\phi_{1_G} = \mathrm{id}_H$, *and*

(iii) ϕ_g *is an endomorphism of H (i.e. a homomorphism between H and itself) for every* $g \in G$.

Proof. Let ϕ be as in Definition 4.1. Properties (i) and (ii) follow directly from the fact ϕ is a homomorphism. By definition of ϕ, the map ϕ_g is in $\mathrm{Aut}\, H$ and thus it is a homomorphism between H and itself, which is what property (iii) says.

Conversely, assume properties (i)-(iii) hold. From property (iii), we know that for any $g \in G$ the map ϕ_g is a homomorphism from H to itself. For any $h \in H$ and any $g \in G$, from (i) and (ii) we get

$$h = \mathrm{id}_H(h) = \phi_{1_G}(h) = \phi_{g^{-1}g}(h) = \phi_{g^{-1}}(\phi_g(h)),$$

which shows that ϕ_g is a bijection for any $g \in G$. Thus we can redefine ϕ as $\phi : G \to \mathrm{Aut}\, H$. This fact, combined with (i), proves that ϕ is a homomorphism from G into $\mathrm{Aut}\, H$. Ultimately, ϕ is an action as intended in Definition 4.1. □

Whenever we need to prove a map is an action in the sense of Definition 4.1, it will suffice to prove it satisfies Lemma 4.1.

Example 4.1. Perhaps the most elementary example of action is the *trivial action*, defined between any two groups G and H by means of the homomorphism $\phi(g) = \mathrm{id}_H$ for every $g \in G$.

Example 4.2. Let V be a vector space over the field of real numbers $\mathbb{R}$. The set V is a group with respect to vector addition ('+'), and $\mathbb{R} \setminus \{0\}$ is a group with respect to the usual product. It is easy to see that scalar multiplication defined as $\theta_r \colon V \to V$, $\theta_r(\mathbf{v}) = r\mathbf{v}$, where $r \in \mathbb{R} \setminus \{0\}$, is an action θ of $\mathbb{R} \setminus \{0\}$ on V. In order to verify this, all we need to do is checking that properties (i)-(iii) of Lemma 4.1 hold. For arbitrary $r \in \mathbb{R}$ and $\mathbf{v}, \mathbf{w} \in V$, we have

$$\theta_r(\mathbf{v} + \mathbf{w}) = r(\mathbf{v} + \mathbf{w}) = r\mathbf{v} + r\mathbf{w} = \theta_r(\mathbf{v}) + \theta_r(\mathbf{w}),$$

which proves property (iii). For any $r, s \in \mathbb{R}$ and $\mathbf{v} \in V$, we have

$$\theta_{rs}(\mathbf{v}) = rs\mathbf{v} = \theta_r(s\mathbf{v}) = \theta_r(\theta_s(\mathbf{v})) = \theta_r\theta_s(\mathbf{v}),$$

which proves property (i). Finally, $\theta_1(\mathbf{v}) = 1\mathbf{v} = \mathbf{v}$ for any $\mathbf{v} \in V$, i.e. $\theta_1 = \mathrm{id}_V$, which proves property (ii). Ultimately, θ defines an action of $\mathbb{R} \setminus \{0\}$ on V.

Example 4.3. If G is a group, we can define an action ϕ of G on itself by means of conjugation: $\phi_g(x) = gxg^{-1}$, where $g, x \in G$. Indeed, property (iii) of Lemma 4.1 holds for any $g, x, y \in G$, because

$$\phi_g(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = \phi_g(x)\phi_g(y),$$

and so does property (i), since for any $x, y, g \in G$,

$$\phi_{xy}(g) = xyg(xy)^{-1} = xygy^{-1}x^{-1} = \phi_x(\phi_y(g)) = \phi_x\phi_y(g).$$

Since $\phi_{1_G}(x) = 1_G x 1_G = x$ for any $x \in G$, we conclude that $\phi_{1_G} = \mathrm{id}_G$.

Example 4.4. If H is a group and $G \leq \operatorname{Aut} H$, then $\theta\colon G \hookrightarrow \operatorname{Aut} H$ such that $\theta_g(h) = g(h)$ for all $h \in H$ defines an action of G on H. Indeed, if $g_1, g_2 \in G$ and $h \in H$, then $\theta_{g_1 g_2}(h) = g_1 g_2(h) = g_1(g_2(h)) = g_1(\theta_{g_2}(h)) = \theta_{g_1}(\theta_{g_2}(h)) = \theta_{g_1}\theta_{g_2}(h)$. Thus θ is a group homomorphism from G into $\operatorname{Aut} H$, and it is by Definition 4.1 an action of G on H.

We can now proceed with the construction of *semidirect products*.

4.2 External and internal semidirect products

Theorem 4.1. *Let G and H be groups, and let ϕ be an action of G on H. Let L be the set of all pairs of the form (h, g), where $h \in H$ and $g \in G$ (i.e, $L = H \times G$). If we equip L with the operation defined as*

$$(h, g)(h', g') = (h\phi_g(h'), gg'),$$

then L forms a group.

Proof. Let $h, h' \in H$ and $g, g' \in G$. Since ϕ_g is an endomorphism of H for every $g \in G$, we know that $h\phi_g(h') \in H$, and trivially $gg' \in G$, because G is a group. Thus, $(h\phi_g(h'), gg') \in L$, and L is closed under the given operation.

We will now verify that the operation defined on L is associative. Let $g, u, x \in G$ and $h, v, y \in H$. Then, thanks to associativity in H and G and to the properties of ϕ, we have

$$\begin{aligned}[(h, g)(v, u)](y, x) &= (h\phi_g(v), gu)(y, x) = (h\phi_g(v)\phi_{gu}(y), gux) \\ &= (h\phi_g(v)\phi_g(\phi_u(y)), g(ux)) = (h\phi_g(v\phi_u(y)), g(ux)) \\ &= (h, g)(v\phi_u(y), ux) = (h, g)[(v, u)(y, x)].\end{aligned}$$

This proves associativity; we still need to prove the existence of an identity and the existence of the inverse of every element. If $(h, g) \in L$, then $(h, g)(1_H, 1_G) = (h\phi_g(1_H), g) = (h1_H, g) = (h, g)$, and similarly we have $(1_H, 1_G)(h, g) = (h, g)$; thus $(1_H, 1_G)$ is the identity. We also see that every element (h, g) has inverse $((\phi_{g^{-1}}(h))^{-1}, g^{-1})$, for

$$((\phi_{g^{-1}}(h))^{-1}, g^{-1})(h, g) = ((\phi_{g^{-1}}(h))^{-1}\phi_{g^{-1}}(h), g^{-1}g) = (1_H, 1_G), \text{ and}$$

$$\begin{aligned}(h, g)((\phi_{g^{-1}}(h))^{-1}, g^{-1}) &= (h\phi_g((\phi_{g^{-1}}(h))^{-1}), gg^{-1}) = (h\phi_g(\phi_{g^{-1}}(h^{-1})), 1_G) \\ &= (h\phi_{gg^{-1}}(h^{-1}), 1_G) = (h\,\mathrm{id}_H(h^{-1}), 1_G) = (1_H, 1_G).\end{aligned}$$

Ultimately, L is a group under the given operation. □

We can now formally define the semidirect product.

Definition 4.2. If G and H are groups and ϕ is an action of G on H, then the set L of all pairs of the form (h, g), where $h \in H$ and $g \in G$, equipped with binary operation

$$(h, g)(h', g') = (h\phi_g(h'), gg') \tag{4.1}$$

is a group, called the **external semidirect product** of G and H with respect to the action ϕ.

Example 4.5. Consider the groups V and $\mathbb{R} \setminus \{0\}$ and the action θ of Example 4.2. The set $L = V \times \mathbb{R} \setminus \{0\}$ forms a group with respect to the operation

$$(\mathbf{v}, r)(\mathbf{w}, s) = (\mathbf{v} + \theta_r(\mathbf{w}), rs) = (\mathbf{v} + r\mathbf{w}, rs)$$

and it is in fact the external semidirect product of V and $\mathbb{R} \setminus \{0\}$, as per Theorem 4.2.

Example 4.6. The set $L = H \times G$, where H, G are groups and $G \leq \operatorname{Aut} H$ as in Example 4.4, is the external semidirect product of H and G when equipped with the following operation, defined by the action $\theta \colon G \hookrightarrow \operatorname{Aut} H$ from the same example:

$$(h_1, g_1)(h_2, g_2) = (h_1\theta_{g_1}(h_2), g_1g_2) = (h_1g_1(h_2), g_1g_2),$$

for all $h_1, h_2 \in H$ and all $g_1, g_2 \in G$.

Example 4.7. Let $T = \mathbb{Z}_4 \times \mathbb{Z}_3$. Define a map $\theta \colon \mathbb{Z}_4 \to \operatorname{Aut} \mathbb{Z}_3$ as follows:

$$\theta(x) = \theta(3x) := \mathrm{sw}_{\mathbb{Z}_3}, \quad \theta(0x) = \theta(2x) := \mathrm{id}_{\mathbb{Z}_3},$$

where $\mathrm{sw}_{\mathbb{Z}_3}$ swaps around 1_3 and 2_3; in other words, θ maps even multiples of elements of $\mathbb{Z}_4$ to the identity map of $\mathbb{Z}_3$, and odd multiples of elements of $\mathbb{Z}_4$ to an automorphism of $\mathbb{Z}_3$ that maps 0_3 to 0_3, 1_3 to 2_3 and vice-versa. (Notice that there exist only two automorphisms on $\mathbb{Z}_3$: the identity $\mathrm{id}_{\mathbb{Z}_3}$ and $\mathrm{sw}_{\mathbb{Z}_3}$. This is because automorphisms map identity to identities.) We know that $\mathbb{Z}_3 = \langle 1_3 \rangle$ and $\mathbb{Z}_4 = \langle 1_4 \rangle$; since 1_4 generates $\mathbb{Z}_4$, any element in $\mathbb{Z}_4$ is of the form $n1_4$, where $n \in \mathbb{Z}$. Thus, the proof that θ is a homomorphism if straightforward. Let $k, l \in \mathbb{Z}$. Then:

$$\theta(k1_4)\theta(l1_4) = \begin{cases} \mathrm{id}_{\mathbb{Z}_3}\,\mathrm{id}_{\mathbb{Z}_3} = \mathrm{id}_{\mathbb{Z}_3} = \theta((k+l)1_4), k, l \text{ even} \\ \mathrm{id}_{\mathbb{Z}_3}\,\mathrm{sw}_{\mathbb{Z}_3} = \mathrm{sw}_{\mathbb{Z}_3} = \theta((k+l)1_4), k \text{ even}, l \text{ odd} \\ \mathrm{sw}_{\mathbb{Z}_3}\mathrm{sw}_{\mathbb{Z}_3} = \mathrm{id}_{\mathbb{Z}_3} = \theta((k+l)1_4), k, l \text{ odd} \\ \mathrm{sw}_{\mathbb{Z}_3}\,\mathrm{id}_{\mathbb{Z}_3} = \mathrm{sw}_{\mathbb{Z}_3} = \theta((k+l)1_4), k \text{ odd}, l \text{ even} \end{cases}$$

Since $\theta((k+l)1_4) = \theta(k1_4 + l1_4)$, we have that θ is a homomorphism. If we equip T with the operation

$$(x, y)(x', y') = (x\theta_y(x'), yy')$$

given in Definition 4.2, then T is the external semidirect product of $\mathbb{Z}_4$ and $\mathbb{Z}_3$ with respect to θ. (Example adapted from [2], p. 171.)

As it turns out, if a group L is the external semidirect product of two groups G and H, the latter ones have 'counterparts' as subgroups of L.

Proposition 4.1. *Let L be the semidirect product of H and G. For $g \in G$ and $h \in H$, define*

$$\gamma\colon G \to L, \quad \gamma(g) = (1_H, g)$$
$$\eta\colon H \to L, \quad \eta(h) = (h, 1_G);$$

set

$$\bar{G} = \{\gamma(g) \mid g \in G\} \text{ and } \bar{H} = \{\eta(h) \mid h \in H\}.$$

Then, γ is an isomorphism from G onto $\bar{G}$, η is an isomorphism from H onto $\bar{H}$, and we have

$$\bar{H} \lhd L = \bar{G}\bar{H}, \quad \bar{G} \cap \bar{H} = \{(1_G, 1_H)\}.$$

Proof. By the definition of the group operation on L, we see that, for any $g, g' \in G$

$$\gamma(gg') = (1_H, gg') = (1_H\phi_g(1_H), gg') = (1_H, g)(1_H, g') = \gamma(g)\gamma(g'),$$

and similarly $\eta(hh') = \eta(h)\eta(h')$, for any $h, h' \in H$. Thus, both γ and η are homomorphisms, and considering their obvious bijectivity, they are isomorphisms. Thus, $\bar{G} = \gamma(G)$ and $\bar{H} = \eta(H)$ are both subgroups of L, and one can easily see that $\bar{H}\bar{G} = L$. It is equally easy to see that $\bar{H} \cap \bar{G} =$

$\{(1_H, 1_G)\}$. To see how $\bar{H} \lhd L$, it suffices to observe that, if $(h', 1_G) \in \bar{H}$, then, for any $h \in H$ and $g \in G$

$$\begin{aligned}(h,g)(h',1_G)(h,g)^{-1} &= (h\phi_g(h'),g)((\phi_{g^{-1}}(h))^{-1},g^{-1}) \\ &= (h\phi_g(h')\phi_g((\phi_{g^{-1}}(h))^{-1}),gg^{-1}) \\ &= (h\phi_g(h'(\phi_{g^{-1}}(h))^{-1}),1_G) \\ &= (h\phi_g(h'\phi_{g^{-1}}(h^{-1})),1_G) \\ &= (h\phi_g(h')h^{-1},1_G) \in \bar{H},\end{aligned}$$

since $h\phi_g(h')h^{-1} \in H$.

□

Proposition 4.1 allows us to identify the groups G, H with subgroups of their external semidirect product L; in this sense, G and H can be seen as subgroups of L itself. As we are going to see, the semidirect product can also be defined in terms of actual subgroups of L. This kind of semidirect product is called the *internal semidirect product*, and it is isomorphic to the external one, which we will prove shortly.

Definition 4.3. A group G is said to be an **internal semidirect product** of two subgroups H and K if $H \lhd G$, $H \cap K = \{1\}$, and $G = HK$; to say G is an internal semidirect product of H and K, we write $G = H \rtimes K$.

Example 4.8. Let S_n be the group of all permutations over n elements. Then S_n is an internal semidirect product of A_n by Q, where A_n is the subgroup of all even permutations of S_n and $Q = \{1, (12)\}$. Before proving this fact, we will remind the reader of a few properties of permutations.

A permutation is *even* when it can be expressed as the product of an even number of transpositions, and similarly, a permutation is *odd* when it can be expressed as the product of an odd number of transpositions. For example, in S_4, the permutation (123) is even, because $(123) = (12)(32)$.

The *sign* $\operatorname{sgn}(\alpha)$ of a permutation α is 1 if and only if α is even, and -1 if and only if α is odd. The inverse of a permutation has the same sign as the permutation itself. If $\sigma, \rho \in S_n$, then $\operatorname{sgn}(\sigma\rho) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\rho)$.

The cardinality of A_n is $|A_n| = \frac{n!}{2}$, where $n! = |S_n|$. (See for example [3], p. 268, 10.4.6.) Additionally, it is easy to see that $A_n \lhd S_n$. For any $\alpha \in A_n$, $\operatorname{sgn}(\alpha) = 1$ by definition. If $\sigma \in S_n$, then from the properties of the sign function it follows that $\operatorname{sgn}(\sigma\alpha\sigma^{-1}) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\alpha)\operatorname{sgn}(\sigma^{-1}) = \operatorname{sgn}(\sigma) \cdot 1 \cdot \operatorname{sgn}(\sigma) = (\operatorname{sgn}(\sigma))^2 = 1$, whence $\sigma\alpha\sigma^{-1} \in A_n$ for every $\alpha \in A_n$.

We can now prove that S_n is the internal semidirect product of A_n by Q. Since $Q = \{(1), (12)\}$, we know $Q \leq S_n$. Since $A_n \lhd S_n$, we know from Theorem 2.1 that $A_nQ \leq S_n$. Since $A_n \cap Q = \{(1)\}$, we see that

$$\begin{aligned} A_nQ &= \{aq \in S_n \mid a \in A_n, q \in Q\} = \{a(1) \mid a \in A_n\} \cup \{a(12) \mid a \in A_n\} \\ &= A_n \cup A_n(12). \end{aligned}$$

Suppose now $x \in A_n \cap A_n(12)$. Then $x \in A_n(12)$, and thus there exists $a \in A_n$ such that $x = a(12)$. From this, it follows that $a^{-1}x = (12)$. However, $x \in A_n$ as well by assumption, whence $\operatorname{sgn}(x) = 1$. Permutation a is in A_n as well, and therefore $\operatorname{sgn}(a) = 1 = \operatorname{sgn}(a^{-1})$. Consequently, $\operatorname{sgn}((12)) = \operatorname{sgn}(a^{-1}x) = \operatorname{sgn}(a^{-1})\operatorname{sgn}(x) = 1 \cdot 1 = 1$, which implies (12) is even. This is a contradiction, because (12) is a single transposition and as such it is odd by definition. Therefore, $A_n \cap A_n(12) = \varnothing$. From this, it follows that $|A_nQ| = |A_n \cup A_n(12)| = |A_n| + |A_n(12)| = \frac{n!}{2} + \frac{n!}{2} = n!$. Thus, A_nQ is a subgroup of S_n with the same cardinality as S_n, and therefore it can only be S_n itself. Ultimately, $S_n = A_nQ$, where $A_n \lhd S_n$ and $A_n \cap Q = \{(1)\}$, which means S_n is the internal direct product of A_n and Q.

Example 4.9. We will show that the dihedral group D_{2n} is the internal semidirect product of two of its subgroups: the subgroup of rotations of a regular n-gon, and the subgroup generated by a single reflection of the same regular n-gon .

If $D_{2n} = \langle a, x\rangle$, where a generates the subgroup $\langle a\rangle$ of rotations and x generates the subgroup $\langle x\rangle$, then we know that $a^n = e$ and $x^2 = e$, where e is the identical symmetry. From the algebra of symmetries, we know that $\{e\} = \langle a\rangle \cap \langle x\rangle$; we also know that, if x is a reflection and a a rotation, then

$$xa = a^{n-1}x. \tag{4.2}$$

Being D_{2n} the group of all symmetries of a regular n-gon, it contains all and only the rotations and reflections of the n-gon itself; this fact, combined with the fact that $\{e\} = \langle a\rangle \cap \langle x\rangle$, allows us to deduce $|\langle a\rangle\langle x\rangle| = |D_{2n}|$. Since $\langle a\rangle\langle x\rangle \leq D_{2n}$, it follows $\langle a\rangle\langle x\rangle = D_{2n}$. Finally, from (4.2) we obtain $xax^{-1} = a^{n-1}xx^{-1} = a^{n-1} \in \langle a\rangle$; thus, $\langle a\rangle$ is normal. The conditions of Definition 4.3 are all met, thus $D_{2n} = \langle a\rangle \rtimes \langle x\rangle$. (For a more detailed account of dihedral groups, see for example [4]. A shorter introduction to the topic can be found in [8].)

If G is the internal semidirect product of groups K and Q, where $K \lhd G$, the subgroup Q is sometimes referred to as a *complement* of K.

Definition 4.4. If $G = K \rtimes Q$, where $KQ = G$, $K \lhd G$, and $K \cap Q = \{1\}$, Q is called a **complement** of K.

A subgroup K of a group G does not necessarily have a complement, and even if it does, the complement is unique only up to isomorphism; in other words, a subgroup can and generally does have multiple possible complements all isomorphic to each other. This can easily be seen by observing that, if Q is any complement of a subgroup K, then

$$Q \cong Q/\{1\} = Q/(K \cap Q) \overset{(\star)}{\cong} KQ/K = G/K,$$

where in $(\star)$ we have made use of the Second Isomorphism Theorem. Since all complements are isomorphic to the quotient group G/K, they all are isomorphic to each other.

Example 4.10. Subgroups $H = \{1, (12)(34)\}$ and $K = \{1, (13)(24)\}$ of the Klein 4-group $V = \{1, (12)(34), (13)(24), (14)(23)\}$ in Example 3.3 are complements of each other: This is because $V = KH = HK$, $K \cap H = \{1\}$, and *both* K and H are normal in V.

Example 4.11. Example 4.10 might tempt us to think that all complements are normal, and thus that, if K is a complement of H, then H is a complement of K. However, complements need not be normal subgroups. For example, consider $K = \{(1), (123), (132)\}$ and $H = \{(1), (12)\}$ as subgroups of S_3. $K \lhd S_3$, $K \cap H = \{(1)\}$, and $KH = S_3$, therefore K is a complement of H, but H is not normal in S_3. This implies H is not a complement of K.

There are several conditions that are equivalent to the definition of internal semidirect product, as proved in the following lemma.

Proposition 4.2. *If K is a normal subgroup of a group G, the following statements are equivalent:*

i) G is the internal semidirect product of subgroups $K \lhd G$ and $Q \leq G$, where $K \cap Q = \{1\}$ (i.e., K has a complement Q in G);

ii) there exists a subgroup $Q \leq G$ such that every $g \in G$ has a unique expression $g = ax$, where $a \in K$ and $x \in Q$;

iii) there exists a homomorphism $s\colon G/K \to G$ *such that* $vs = \mathrm{id}_{G/K}$*, where* $v\colon G \to G/K$ *is the canonical surjection;*

iv) there exists a homomorphism $\pi\colon G \to G$ *such that* $\ker\pi = K$ *and* $\pi(x) = x$ *for every* $x \in \mathrm{im}\,\pi$*. (The map* π *is called a* ***retraction*** *of* G*, while* $\mathrm{im}\,\pi$ *is called a* ***retract*** *of* G*.)*

Proof. We proceed by proving the chain of implications $i) \Rightarrow ii) \Rightarrow iii) \Rightarrow iv) \Rightarrow i)$.

$i) \Rightarrow ii)$ Let Q be a complement of K in G, and let $g \in G$. By assumption, $KQ = G$, therefore there exist $a \in K$ and $x \in Q$ such that $g = ax$. If $g = by$ is a second such factorisation, where $b \in K$ and $y \in Q$, then $ax = by$ and $xy^{-1} = a^{-1}b$. The left-hand term is in Q, and the right-hand one is in K; since they are equal, they both are in $K \cap Q = \{1\}$. Ultimately, $a = b$ and $x = y$, proving that the factorisation of g is unique.

$ii) \Rightarrow iii)$ By assumption, for each $g \in G$ there exist unique $a \in K$ and $x \in Q$ such that $g = ax$; therefore, if $Kg \in G/K$, we have $Kg = Kax = Kx$, since $a \in K$. Thus, by the uniqueness of this factorisation, we can define a function $s\colon G/K \to G$ such that $s(Kg) = x$, and prove it meets the conditions expressed in $iii)$. If $Kg, Kh \in G/K$, where the factorisation $h = by$ ($b \in K, y \in Q$) is unique, then

$$\begin{aligned} s(KgKh) = s(KaxKby) = s(KxKy) &\overset{(\star)}{=} s(Kxy) = s(K1_Gxy) = xy \\ &= s(Kg)s(Kh), \end{aligned}$$

where in $(\star)$ we have used the normality of K; this proves s is a homomorphism. Additionally,

$$vs(Kg) = vs(Kax) = vs(Kx) = v(x) = Kx = Kax = Kg,$$

i.e. $vs = \mathrm{id}_{G/K}$.

$iii) \Rightarrow iv)$ Let us define $\pi\colon G \to G$ as $\pi = sv$, where $s\colon G/K \to G$ and the map $v\colon G \to G/K$ is the canonical surjection. We will need to prove two things, namely that π is a retraction of G, and that $\ker\pi = K$.
For the first part, let $x \in \mathrm{im}\,\pi$. Then $x = \pi(g)$, for some $g \in G$. Now

$$\begin{aligned} \pi(x) = \pi(\pi(g)) = sv(sv(g)) &= s(vs)v(g) \\ &= s(\mathrm{id}_{G/K})v(g) = sv(g) = \pi(g) = x. \end{aligned}$$

Thus, π is a retraction of G.
Let us now show that $\ker \pi = K$. Since $vs = \mathrm{id}_{G/K}$ by assumption, we know s is an injection. Now, let $g \in \ker \pi$. Then $1_G = \pi(g) = sv(g) = s(Kg)$. Since s is an injective group homomorphism, its kernel is trivial, and therefore $Kg = K$, which implies $g \in K$. This proves $\ker \pi \subset K$. For the reverse inclusion, notice first that $K \subset \ker v$, for if $k \in K$, then $v(k) = Kk = K = 1_{G/K}$. Now, if $a \in K$,

$$\pi(a) = sv(a) = s(1_{G/K}) = s(K) = s(K1_G1_G) = 1_G,$$

which implies $a \in \ker \pi$ and therefore $K \subset \ker \pi$.

$iv) \Rightarrow i)$ We will need to show that K has a complement in G, i.e that there exists $Q \leq G$ such that $K \cap Q = \{1\}$ and $KQ = G$. To this end, let $Q = \mathrm{im}\, \pi$. (Note that this is not, in general, the same π as in the previous step.) Since π is a retraction of G, if $g \in Q$ we have $\pi(g) = g$; on the other hand, if $g \in K$, then $\pi(g) = 1$, since $\ker \pi = K$. It follows that, if $g \in K \cap Q$, then $g = \pi(g) = 1$, i.e. $K \cap Q = \{1\}$.
For the second part, let us start by observing that, since π is a retraction of G and a homomorphism, if $g \in G$ we have

$$\pi(g\pi(g^{-1})) = \pi(g)\pi(\pi(g^{-1})) = \pi(g)\pi(g^{-1}) = \pi(gg^{-1}) = \pi(1) = 1,$$

which implies that $g\pi(g^{-1}) \in \ker \pi$. Since $\ker \pi = K$, $g\pi(g^{-1}) \in K$. Also, $\pi(g) \in Q$, and thus $g\pi(g^{-1})\pi(g) \in KQ$. However,

$$g\pi(g^{-1})\pi(g) = g\pi(g^{-1}g) = g \cdot 1 = g,$$

proving that $G = KQ$.

□

4.3 Isomorphism between semidirect products

In order to prove, as promised, that the external and internal semidirect products are isomorphic, we will need to make use of the following lemma.

Lemma 4.2. *Let G be the internal semidirect product of its subgroups H and K, where $H \lhd G$. Define the map $\theta \colon K \to \mathrm{Aut}\, H$ so that the function θ_x conjugates elements of H by x (for example, $\theta_x(h) = xhx^{-1}$ for any $x \in K$ and $h \in H$). Then θ is an action of K on H.*

Proof. Since the codomain of θ is $\mathrm{Aut}\, H$ by definition, it will suffice to check property (i) of Lemma 4.1, i.e. that θ is a homomorphism. For every $a \in H$ and any x, y in K, we have

$$\begin{aligned}\theta_{xy}(a) &= \gamma_{xy}(a) = xya(xy)^{-1} \\ &= xyay^{-1}x^{-1} = x(yay^{-1})x^{-1} \\ &= \gamma_x(\gamma_y(a)) = \theta_x(\theta_y(a)) \\ &= \theta_x\theta_y(a),\end{aligned}$$

which proves the claim. □

Now we can finally prove that the external and internal semidirect products are isomorphic to each other.

Theorem 4.2. *Let G be an internal semidirect product of two subgroups H and K such that $H \lhd G = HK$ and $H \cap K = \{1\}$. Let $\theta\colon K \to \mathrm{Aut}\, H$ be defined in terms of conjugation as in Lemma 4.2, so that $\theta_u(h) = uhu^{-1}$ for any $u \in K$ and $h \in H$. Then θ is an action of K on H, and the external semidirect product of H and K with respect to θ is isomorphic to G.*

Proof. Lemma 4.2 proves θ is an action of K on H. If L is the external semidirect product of H and K with respect to θ, we can define a function $f\colon L \to G$ such that $(h, k) \to hk$, where $(h, k) \in L$ and $hk \in G$ (by assumption that $G = HK$). We need to show that f is a bijective homomorphism.

To see that f is a homomorphism, we compute

$$\begin{aligned}f((h,k)(v,u)) &= f(h\theta_k(v), ku) = h\theta_k(v)ku \\ &= hkvk^{-1}ku = hkvu \\ &= f(h,k)f(v,u).\end{aligned}$$

where $k, u \in K$ and $h, v \in H$.

To prove the bijectivity of f, we notice first that, if $g \in G$, then by assumption there exist $h \in H$ and $k \in K$ such that $hk = g$. Since $(h, k) \in L$, we have that $g = hk = f(h, k) \in f(L)$. Since g was arbitrary, it follows that $G \subset f(L)$. By definition of f, we also have $f(L) \subset G$, ultimately leading to $f(L) = G$, which shows that f is a surjection.

Suppose now that $(h, k) \in \ker f$: Then $f(h, k) = hk = 1$, which implies $h = k^{-1}$. In turn this means that $h, k \in H \cap K = \{1\}$. It follows that $\ker f$ contains 1 as its only element, which implies f is an injection. □

Since the external and internal semidirect products are isomorphic, we may choose as operational definition that of internal semidirect product, drop the adjective *internal*, and write the semidirect product G of groups K and Q as $G = K \rtimes Q$.

5 Wreath products

The direct product and the (external) semidirect product are two ways to obtain a new group from two given ones. A third, slightly more convoluted way is the so-called *wreath product*, which we will now proceed to illustrate.

5.1 General wreath product

Thus far we have made use of the concept of action of a group on another group. This concept is a special case of the notion of action of a group on a *set*. We will need this generalisation in our definition of the wreath product.

Definition 5.1. Let G be a group, let X be any set, and let ρ be a homomorphism from G into the symmetric group $\Sigma(X)$ of X—i.e., the group of bijections of X. We call ρ an **action** of G on X and we say that G acts on X via the homomorphism ρ. The pair (X, ρ) is sometimes referred to as a G**-set**.

Remark 5.1. To see why Definition 4.1 is, as claimed, a special case of Definition 5.1, let us consider the action ρ of a group G on another group H. The map ρ is a homomorphism from G to $\operatorname{Aut} H$; since $\operatorname{Aut} H \subset \Sigma(H)$, we have that $\rho : G \to \Sigma(H)$ is a homomorphism from G to $\Sigma(H)$ as well. Since the group H is obviously also a set, we have that ρ is an action of the group G on the *set* H. In other words, every group action is an action.

If (X, ρ) is a G-set and $g \in G$, then each element of G determines a permutation $\rho(g)$on X. As we did before, to avoid cumbersome notation we will sometimes write ρ_g instead of $\rho(g)$.

Just like we did in our discussion of semidirect products, whenever we will need to check if a given map is an action, instead of checking if the map meets the conditions of Definition 5.1, we can make use of the following lemma.

Lemma 5.1. *Let G be a group and let X be a set. Then a map $\rho\colon G \to X^X$ is an action as described in Definition 5.1 if and only if*

(i) $\rho_{gh} = \rho_g \rho_h$ *for every* $g, h \in G$*, and*

(ii) $\rho_{1_G} = \mathrm{id}_X$

Proof. If ρ is as in Definition 5.1, then both properties (i) and (ii) follow from the properties of group homomorphisms. Conversely, assume (i) and (ii) hold. Just as in the proof of Lemma 4.1, these properties imply that, for any $g \in G$ and $x \in X$,

$$x = \mathrm{id}_X(x) = \rho_{1_G}(x) = \rho_{g^{-1}g}(x) = \rho_{g^{-1}}(\rho_g(x)).$$

This means ρ_g is a bijection for every $g \in G$; combined with (i), this shows that $\rho\colon G \to \Sigma(X)$ is an action as intended in Definition 5.1.

□

Example 5.1. Let $G = \{1, -1\}$ and let $X = \mathbb{R}$. The set G is a group if equipped with the normal multiplication of real numbers, which we can use to induce an action ρ of G on X. This action maps 1 to the identity function on X, and -1 to the 'inv' function on X—that is, the function that maps $x \in X$ to its inverse $-x$. Formally,

$$\rho\colon G \to \Sigma(X), \quad \rho(g) = \rho_g \in \Sigma(X),$$

where, for $x \in X$,

$$\rho_g(x) = \begin{cases} \mathrm{id}_X(x) = x, & \text{if } g = 1 \\ \mathrm{inv}(x) = -x, & \text{if } g = -1. \end{cases}$$

To prove ρ is a homomorphism, notice that we can write $\rho_g(x) = gx$. Thus, if $g, h \in G$, then

$$\rho_{gh}(x) = ghx = g(h(x)) = \rho_g(h(x)) = \rho_g(\rho_h(x)) = \rho_g\rho_h(x).$$

Ultimately, ρ is an action of G on X.

Example 5.2. Let $n > 0$, let $G = GL_n(\mathbb{C})$—the group of all invertible $n \times n$ complex matrices—and let $X = M_n(\mathbb{C})$—the set of all $n \times n$ complex matrices. (Notice this is not a group, for not all its elements have an inverse.) Define $\rho\colon G \to \Sigma(X)$ as $\rho_g(A) = gA$ for each $g \in G$, $A \in X$. Clearly, ρ is a homomorphism, for

$$\rho_{gh}(A) = ghA = g(hA) = \rho_g(hA) = \rho_g(\rho_h(A)).$$

Additionally, $\rho_{1_G}(A) = 1_G A = A$ for all $A \in X$, whence $\rho_{1_G} = \mathrm{id}_X$. By Lemma 5.1, ρ is an action.

We can now proceed to introduce the wreath product.

Definition 5.2. Let G and H be groups, and let (X, μ) be an H-set. Let B be the set of all functions from X to G. If $b, b' \in B$, define their product and the action of H on B as follows:

$$bb'(x) = b(x)b'(x), \quad \text{and}$$
$$\phi\colon H \to \operatorname{Aut} B, \quad (\phi_h(b))(x) = b(\mu_h(x)),$$

where $x \in X$ and $h \in H$. The semidirect product of B and G with respect to the action just defined is called the **general wreath product** of G and H.

Remark 5.2. Notice how B in Definition 5.2 is nothing but the complete direct product of G with itself. (See Definition 3.3.)

We can make the above definition more specific, limiting ourselves to the case when X is finite. We will make use of this simplified definition in our next examples. This definition has been adapted from [10].

Definition 5.3. Let $X = \{1, 2, \ldots, t\}$ be a finite set with $|X| = t$. Let G, H be groups, and let μ be an action of H on X. Define G^t to be the direct product of G with itself t times; elements of G^t are thus of the form $\bar{g} = (g_1, \ldots, g_t)$. The **wreath product** of G and H is defined as the semidirect product $G \wr_t H$ = $G^t \rtimes H$ with respect to the action ϕ of H on G^t derived from the action of H on X as follows:

$$\phi_h(\bar{g}) = \phi_h(g_1, \ldots, g_t) = (g_{\mu_h(1)}, \ldots, g_{\mu_h(t)}), \qquad \text{for all } \bar{g} \in G^t$$

where $h \in H$.

Before we proceed further, let us show that ϕ is indeed an action of H on G^t. Notice that, since both H and G^t are groups, we need to prove that ϕ is an action as intended in Definition 4.1; on the other hand, μ was defined as an action of a group on a *set*, and thus according to Definition 5.1. Let us first prove that, given any $h \in H$, ϕ_h is a homomorphism from G^t to itself (condition (iii) of Lemma 4.1). If $\bar{g} \in G^t$, then obviously $\phi_h(\bar{g}) \in G^t$ as well, since it is merely a rearrangement of t elements of G. Additionally, if $h \in H$ and $\bar{g}, \bar{f} \in G^t$ then

$$\begin{aligned}\phi_h(\bar{g}\bar{f}) &= \phi_h((g_1, \ldots, g_t)(f_1, \ldots, f_t)) \\ &= \phi_h(g_1 f_1, \ldots, g_t f_t) \overset{(\star)}{=} (g_{\mu_h(1)} f_{\mu_h(1)}, \ldots, g_{\mu_h(t)} f_{\mu_h(t)}) \\ &= (g_{\mu_h(1)}, \ldots, g_{\mu_h(t)})(f_{\mu_h(1)}, \ldots, f_{\mu_h(t)}) = \phi_h(\bar{g})\phi_h(\bar{f}).\end{aligned}$$

To see why the step marked as $(\star)$ is true, consider that each $g_i f_i$ is simply an element of G obtained as the product of g_i and f_i. If we agree to write

$$\gamma_i := g_i f_i,\ i = 1, \ldots, t,$$

then we can rewrite $\phi_h(g_1 f_1, \ldots, g_t f_t)$ as $\phi_h(\gamma_i, \ldots, \gamma_t)$. By definition of ϕ_h, we have

$$\phi_h(\gamma_1, \ldots, \gamma_t) = (\gamma_{\mu_h(1)}, \ldots, \gamma_{\mu_h(t)}).$$

From the notation we adopted it follows $\gamma_{\mu_h(i)} = g_{\mu_h(1)} f_{\mu_h(1)}$ for $i = 1, \ldots, t$, ultimately yielding

$$(\gamma_{\mu_h(1)}, \ldots, \gamma_{\mu_h(t)}) = (g_{\mu_h(1)} f_{\mu_h(1)}, \ldots, g_{\mu_h(t)} f_{\mu_h(t)}).$$

As for condition (ii) of Lemma 4.1, we see that, since $\mu_{1_H} = \mathrm{id}_X$ by Lemma 5.1,

$$\begin{aligned} \phi_{1_H}(\bar{g}) = \phi_{1_H}(g_1, \ldots, g_t) &= (g_{\mu_{1_H}(1)}, \ldots, g_{\mu_{1_H}(t)}) \\ &= (g_{\mathrm{id}_X(1)}, \ldots, g_{\mathrm{id}_X(t)}) = (g_1, \ldots, g_t = \bar{g}, \end{aligned}$$

for all $\bar{g} \in G^t$, proving that $\phi_{1_H} = \mathrm{id}_{G^t}$.

Now we only need to show that condition (i) of Lemma 4.1 is met, that is that ϕ is a homomorphism. This follows easily from the fact μ is a homomorphism:

$$\begin{aligned} \phi_{hk}(\bar{g}) = \phi_{hk}(g_1, \ldots, g_t) &= (g_{\mu_{hk}(1)}, \ldots, g_{\mu_{hk}(t)}) \\ &= (g_{\mu_h \mu_k(1)}, \ldots, g_{\mu_h \mu_k(t)}) = \phi_h(g_{\mu_k(1)}, \ldots, g_{\mu_k(t)}) \\ &= \phi_h \phi_k(g_1, \ldots, g_t) = \phi_h \phi_k(\bar{g}). \end{aligned}$$

Remark 5.3. It is worth pointing out how Definition 5.2 is a generalised version of Definition 5.3. In the former, X can be a set of any cardinality, as opposed to the finite-version X in the latter definition. Similarly, Definition 5.3 makes use of a finite direct product of G with itself, while Definition 5.2, by considering the set of all functions $X \to G$, is essentially using a direct product of G with itself of arbitrary size—i.e., a complete direct product. The two actions denoted as ϕ are in fact the same: The one in Definition 5.2 works with arbitrarily long, potentially uncountable indexed families of elements of G, whereas that of Definition 5.3 deals with finite t-tuples of elements of G.

Example 5.3. Let $G = \mathbb{Z}_m$, $H = S_n$, $X = \{1, 2, \ldots, n\}$, and let the map $\mu\colon S_n \to \Sigma(X)$ be the natural action of S_n on X. Let us define the action $\phi\colon S_n \to \operatorname{Aut} \mathbb{Z}_m^n$ of S_n on $G^n = \mathbb{Z}_m^n$ as

$$\phi_\sigma(x_1, x_2, \ldots, x_n) = (x_{\mu_\sigma(1)}, x_{\mu_\sigma(2)}, \ldots, x_{\mu_\sigma(n)}),$$

for all $x_i \in \mathbb{Z}_m$ and $\sigma \in S_n$. The wreath product of G by H is then the semidirect product $G \wr_n H = \mathbb{Z}_m^n \rtimes S_n$ with respect to ϕ. In simple terms, the result of this particular wreath product is the shuffling of n-tuples of elements of the cyclic group $\mathbb{Z}_m$, that is a group of permutations over $\mathbb{Z}_m^n$; for this reason, it is called the *generalised symmetric group*.

To better visualise the situation, let $m = 2$ and $n = 3$—that is,

$$\begin{aligned} G &= \mathbb{Z}_2 = \{0_2, 1_2\}, \\ H &= S_3 = \{(1), (1,2,3), (3,2,1), (1,2), (1,3), (2,3)\}, \\ X &= \{1, 2, 3\}. \end{aligned}$$

The wreath product is then $G \wr_3 H = \mathbb{Z}_2^3 \rtimes S_3$; to emphasise its group structure, recall the underlying set is $\mathbb{Z}_2^3 \times S_3$, and the group operation is defined as in (4.1), in the definition of semidirect product:

$$(x, \sigma)(y, \rho) = (x + \phi_\sigma(y), \sigma\rho), \quad x, y \in \mathbb{Z}_2^3,\ \sigma, \rho \in S_3.$$

The elements of $G \wr_3 H$ are of the form $((x, y, z), \sigma)$, where $x, y, z \in \mathbb{Z}_2$ and $\sigma \in S_3$, for a total of 48 elements. As an example, let $a = ((1_2, 1_2, 0_2), (12))$ and $b = ((1_2, 0_2, 1_2), (23))$ be elements of $G \wr_3 H$. Then, keeping in mind that the end result of the action μ_σ is simply that of shuffling around an n-tuple of elements of $\mathbb{Z}_2$, we get

$$\begin{aligned} ab &= ((1_2, 1_2, 0_2), (12))((1_2, 0_2, 1_2), (23)) \\ &= ((1_2, 1_2, 0_2) + \phi_{(12)}(1_2, 0_2, 1_2), (12)(23)) \\ &= ((1_2, 1_2, 0_2) + (0_2, 1_2, 1_2), (132)) \\ &= ((1_2, 0_2, 1_2), (132)). \end{aligned}$$

(Recall that the group operation in $\mathbb{Z}_2^3$ is based on the addition of congruence classes.)

Example 5.4. Let $G = \mathbb{R}$, $H = S_n$, $X = \{1, 2, \ldots n\}$. Define an action μ of H on X in the usual way, i.e. $\mu_\sigma(x) = \sigma(x)$ for every $x \in X$ and every $\sigma \in H$.

This action extends naturally to an action ϕ of H on G^n in the same way as before, i.e.

$$\phi_\sigma(\bar{x}) = (x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)})$$

for all $\bar{x} \in G^n$. The wreath product of G and H is now $G \wr_n H = \mathbb{R}^n \rtimes S_n$, with respect to the action ϕ. Again, we notice the set underlying this group is $\mathbb{R}^n \times S_n$, and the group operation is given by

$$(\bar{x}, \sigma)(\bar{y}, \rho) = (\bar{x} + \phi_\sigma(\bar{y}), \sigma\rho),$$

for every $\bar{x}, \bar{y} \in \mathbb{R}^n$, $\sigma, \rho \in S_n$, and where $+$ denotes the usual vector addition operation.

5.2 Twisted wreath product

We conclude this section with a brief account of a variant of the wreath product called the *twisted wreath product*.

Let A and G be two groups, and let $H \leq G$. Let also ϕ be an action of H on A—that is, $\phi\colon H \to \operatorname{Aut} A$; finally, let B be the set of all functions $b\colon G \to A$ such that, for any $h \in H$, we have

$$b(hx) = \phi_h(b(x)), \quad \text{for all } x \in G. \tag{5.1}$$

Let us now define a product on B as follows:

$$b_1 b_2(x) = b_1(x) b_2(x), \tag{5.2}$$

for $b_1, b_2 \in B$ and all $x \in G$. In other words, given two functions in B, their product $b_1 b_2$ is simply another function in B obtained as the pointwise product of b_1 and b_2 in A. The product we just defined satisfies (5.1): given $b_1, b_2 \in B$ and $x \in G, h \in H$, we have

$$\begin{aligned} b_1 b_2(hx) &= b_1(hx) b_2(hx) = \phi_h(b_1(x))\phi_h(b_2(x)) \\ &= \phi_h(b_1(x) b_2(x)) = \phi_h(b_1 b_2(x)), \end{aligned}$$

therefore $b_1 b_2 \in B$, and thus B is closed with respect to the operation in (5.2). As a matter of fact, B is a group: The reader will recognise it as the complete direct product of the group A with itself. (See Definition 3.3.) The group B is called the *base group* of the twisted wreath product.

Now we will define the action of G on B. Let $u \in G$ and $b \in B$. Define $\eta\colon G \to B^B$ so that

$$(\eta_u(b))(x) = b(xu), \quad \text{for all } x \in G. \tag{5.3}$$

To show that this is indeed an action, we can make use of Lemma 4.1. Let us first show condition (i) of Lemma 4.1, i.e. let us show that η is a homomorphism. Keeping in mind that the operation on B^B is function composition, we easily see that, for all $u, v, x \in G$ and $b \in B$,

$$\begin{aligned}(\eta_u\eta_v(b))(x) &= (\eta_u(\eta_v(b)))(x) = (\eta_v(b))(xu) \\ &= b(xuv) = b(x(uv)) = (\eta_{uv}(b))(x)\end{aligned}$$

which proves condition (i). To prove condition (ii), let $x \in G$ and $b \in B$ be arbitrary and compute

$$(\eta_{1_G}(b))(x) = b(x1_G) = b(x).$$

This shows that $\eta_{1_G} = \mathrm{id}_B$. To prove condition (iii), we need to show that η_u is a homomorphism from B to itself. Now, for all $u, x \in G$ and $h \in H$ we have

$$(\eta_u(b))(hx) = b(hxu) = \phi_h(b(xu)) = \phi_h((\eta_u(b))(x)),$$

therefore $\eta_u(b) \in B$, since it satisfies (5.1). Finally,

$$(\eta_u(b_1b_2))(x) = b_1b_2(xu) = b_1(xu)b_2(xu) = (\eta_u(b_1))(x)(\eta_u(b_2))(x).$$

Ultimately, η is an action.

We are now ready to give the following definition:

Definition 5.4. Let B, G, H, A, η, ϕ be as in the construction above. Then, the semidirect product W of B and G with respect to η is called **twisted wreath product**.

Put in terms of what Theorem 4.1 says, $W = B \rtimes G$, where $B \times G$ is the underlying set, every $w \in W$ is of the form (b, g) with $b \in B$, $g \in G$, and the product between two elements of W is defined as $(b, g)(b', g') = (b\eta_g(b'), gg')$.

6 Rubik's cube group

The final section of this work will discuss *Rubik's group* in terms of semidirect and wreath products. We will first lay down the fundamentals of the cube's algebra and define an operation on the cube's group.

6.1 Basics of Rubik's cube algebra

Rubik's cube consists of six faces, each of which consists of nine coloured squares called *facets*, typically white, red, orange, blue, green, and yellow. Facets can be located in the centre of a face, on its corners, or on its edges (i.e. between two corners). Each face can be rotated by $360°$ clockwise and anticlockwise, and so can the 'slice' between two opposite faces. This configuration allows to change the position and orientation of each facet, with the exception of the centre facets, which do not move at all. (Strictly speaking, one could for example keep two side faces fixed and move the slice between them, so that its centre facet would effectively move; however, this is for all intents and purpose the same as keeping the centre slice fixed and moving the two side faces. Thus, one can—and it is generally more convenient to do so—consider the cube fixed in space so that the centre facets serve as a reference and stay put where they are.) A *solved* cube is such that on each face all facets are of the same colour.

A *basic move* rotates one of the six faces of the cube by $90°$; the set of basic moves can be described using the so-called *Singmaster notation*. Define the *front* face of the cube to be that directly in front of the observer, and consequently define the remaining faces as *back*, *up*, *down*, *left*, and *right*. The elements of the basic moves set are then $\boldsymbol{F}$, $\boldsymbol{B}$, $\boldsymbol{U}$, $\boldsymbol{D}$, $\boldsymbol{L}$, $\boldsymbol{R}$, defined in the following way:

Basic move	Inverse
$\boldsymbol{F}$: front face 90° clockwise	$\boldsymbol{F'}$: front face 90° anticlockwise
$\boldsymbol{B}$: back face 90° clockwise	$\boldsymbol{B'}$: back face 90° anticlockwise
$\boldsymbol{U}$: up face 90° clockwise	$\boldsymbol{U'}$: up face 90° anticlockwise
$\boldsymbol{D}$: down face 90° clockwise	$\boldsymbol{D'}$: down face 90° anticlockwise
$\boldsymbol{L}$: left face 90° clockwise	$\boldsymbol{L'}$: left face 90° anticlockwise
$\boldsymbol{R}$: right face 90° clockwise	$\boldsymbol{R'}$: right face 90° anticlockwise

It is also useful to consider a 'neutral move' $\boldsymbol{E}$ such that no 'cubie' (the

tiny cubes the cube is made of) is moved.

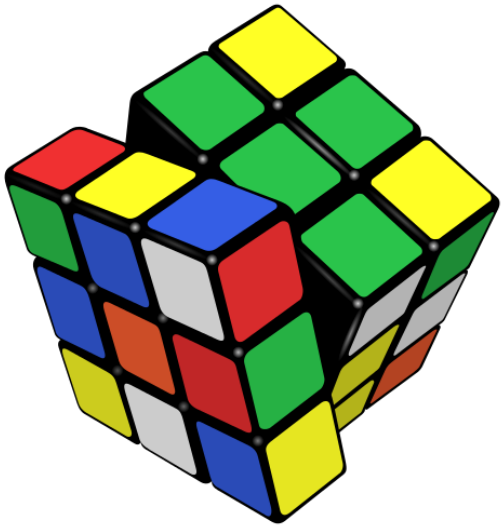


Figure 6.1: Rubik's cube. (Image credit: Wikipedia user Booyabazooka)

We call a combination of basic moves a *move*. The group G of all legal moves that can be performed on the cube is therefore generated by all basic moves, i.e $G = \langle \boldsymbol{F}, \boldsymbol{B}, \boldsymbol{U}, \boldsymbol{D}, \boldsymbol{L}, \boldsymbol{R} \rangle$. Each $g \in G$ induces a certain state of the cube. We can think of any state of the cube as a permutation over the set of its 54 facets. The group of all such permutations is S_{54}, but this is not the group of *legal* states of the cube. A legal state is induced only by means of a legal move $g \in G$, and as we have seen, by means of legal moves alone, for all intents and purposes the six centre facets do not move at all. Therefore, the group P of legal cube states induced by all $g \in G$ cannot be larger than S_{48}. Additionally, legal moves can only move corner facets to corner positions, and edge facets to edge positions. Ultimately, this means that P must be a proper subgroup of S_{48}. As we will see, G and P are isomorphic, so for simplicity's sake we can always refer to G alone. We call G the *Rubik's cube group* or simply *Rubik's group*. The cardinality of G is $|G| = 43.252.003.274.489.856.000$; nonetheless, Rubik's cube can be solved in as little as 26 moves starting from any legal state.[6]

6.2 Defining an operation on Rubik's group

6.2.1 Numbering and labelling of the cube. Cube states.

We shall begin by establishing a labelling system on the cube, as done by Christoph Bandelow [6]. Assume that the cube, in its initial (solved) configuration, is in a fixed location in space. For our purposes, we can assume no inner layer movements. (That is, as said before, we assume any layer of the cube between two other layers does not move in any way, and thus the centre facets stay put where they are.) Further imagine the cube is lodged in an incorporeal 'scaffolding' which does not impede the cube's movements in any way. We can visualise this scaffolding as nine cubical boxes ('cubicles') fixed together in a cubical shape, so that each box contains a cubie from the cube.

Let us now number the corner cubies from 1 to 8, and the edge cubies from 1 to 12. We write the same numbers on the corresponding cubicles in the scaffolding. Our numbering proceeds in ascending order left to right, top to bottom and front to back, as shown in Figure 6.2.1. After a move is performed on the cube, the numbers on the cubies will be scrambled, but the numbers on the scaffolding will remain in their original positions.

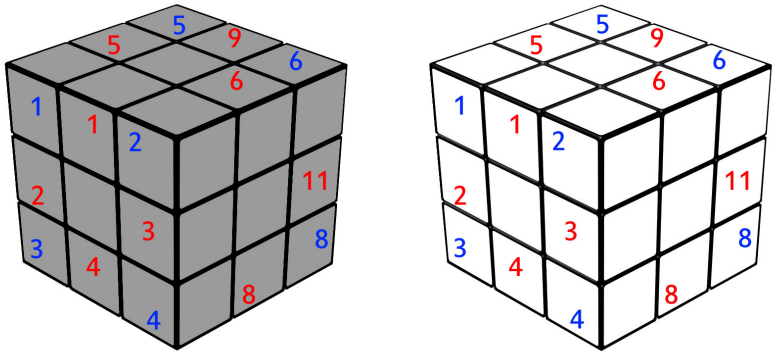


Figure 6.2: The numbering system on Rubik's cube. The gray cube is the 'scaffolding', to be imagined superimposed on the actual, white cube. Blue numbers indicate corner cubies and cubicles; red numbers indicate edge cubies and cubicles. Some numbers not possible to show have been left out. (Image credit: http://www.tipsquirrel.com. Retouched.)

With this system in place, for any arbitrary state of the cube we can

define the location of any corner cubie by an element of the symmetric group S_8— i.e., after performing permutation $\rho \in S_8$ on the corner cubies, corner cubie i will be in corner cubicle $\rho(i)$. Similarly, edge cubie j ends up in corner cubicle $\sigma(j)$ after performing permutation $\sigma \in S_{12}$.

Now that we have a way of describing the location of each corner and edge cubie, we need a system to describe their orientations. We shall mark the scaffolding of the cube in such a way that, for each corner cubie, a side touching one of the three facets of that cubie is marked by a blue cross; for each edge cubie, a side touching one of the two facets of the cubie will be marked by a red cross. Notice these marks are made *only* on the scaffolding, not on the facets of the cubies themselves. We will then mark the facets of each corner cubie with $0, 1, 2$ clockwise with 0 located beneath each blue cross, and the facets of each edge cubie with 0 and 1, with 0 in the corresponding position of the red cross marked on the scaffolding.

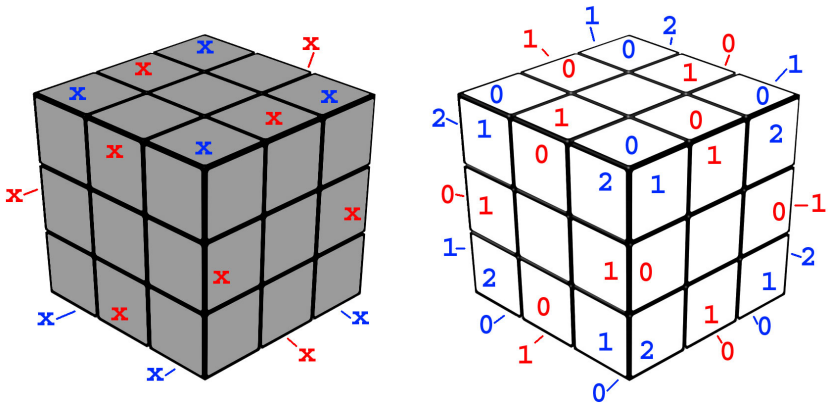
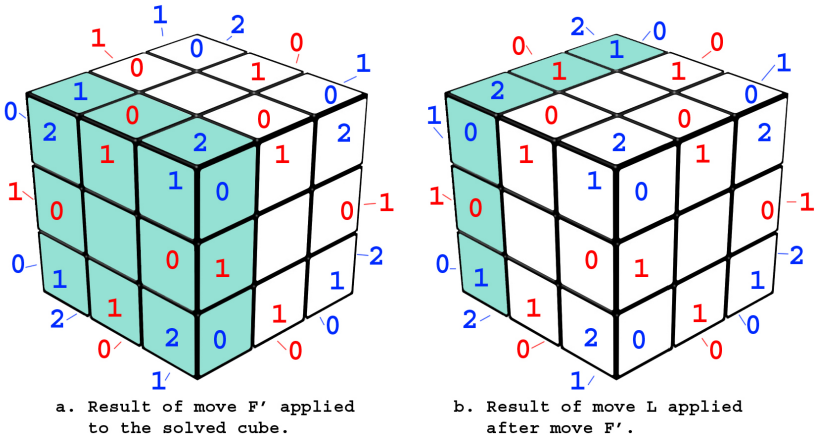


Figure 6.3: The labelling system on Rubik's cube. The gray cube is the 'scaffolding', to be imagined superimposed on the actual, white cube. The crosses always indicate the initial location of a 0, i.e. the correct orientation of a cubie. Lines indicate marks on non-visibile facets. Some marks not possible to show have been left out. (Image credit: http://www.tipsquirrel.com. Retouched.)

Given any cube state, the orientation of corner and edge cubies can now be represented as an 8-tuple $x = (x_1, \ldots, x_8) \in X = \{0, 1, 2\}^8$ and a 12-tuple $y = (y_1, \ldots, y_{12}) \in Y = \{0, 1\}^{12}$ respectively, where x_i denotes the facet of the i^{th} corner cubie lying in its current cubicle under the blue cross, and similarly y_j denotes the facet of the j^{th} edge cubie lying in its current

cubicle under the red cross.

Example 6.1. If the cube is in its solved state, then the labels are as in Figure 6.3. In this case, we have $x = (0, \ldots, 0)$ and $y = (0, \ldots, 0)$, i.e. $x_i = 0$ for all $i = 1, \ldots, 8$ and $y_j = 0$ for all $j = 1, \ldots, 12$. If we perform basic moves ***F'*** and ***L*** in a sequence—that is, we twist the front face anticlockwise and the left face clockwise—the resulting vectors will be $x = (1, 2, 1, 2, 2, 0, 1, 0)$ and $y = (0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$.



a. Result of move F' applied to the solved cube.

b. Result of move L applied after move F'.

Figure 6.4: Move ***F'*** on the solved cube produces the cube state in **a**. Subsequently applying move ***L*** results in the cube state in **b**. Cubies that have been moved are highlighted in dark cyan. Notice that, when rotating a cube face, one must first look directly at said face, and then rotate clockwise (or anticlockwise.) (Image credit: http://www.tipsquirrel.com. Retouched.)

We will sometimes refer to x_i (respectively, y_j) as the *value* of cubie i (respectively, cubie j). If $x_i = 0$ (respectively, $y_j = 0$), we say corner cubie i (respectively, edge cubie j) is *correctly oriented*, and *incorrectly oriented* otherwise. We can now give a formal definition of a cube *state*.

Definition 6.1. A **state** of Rubik's cube is a quadruplet (ρ, σ, x, y) such that $\rho \in S_8$, $\sigma \in S_{12}$, $x \in X = \{0, 1, 2\}^8$, and $y \in Y = \{0, 1\}^{12}$. The set of all states is indicated as $P^\star$.

To clarify, if $p = (\rho, \sigma, x, y)$ is a state of the cube, the permutation ρ indicates in which corner cubicle each corner cubie is located; so, for example, if $\rho = (1243)$, we know that corner cubie 1 is located in corner cubicle $\rho(1) = 2$. Similarly, σ indicates the cubicle where each edge cubie is

currently located. The current orientation of corner cubies is given by the vector x, so that its x_i coordinate *always* indicates the orientation of cubie i, wherever it may be located. In a similar fashion, vector y tells us the orientation of edge cubies in their *present* location. The cube's solved state is $I = (1, 1, 0, 0)$, because all cubies are in their original cubicle (e.g., corner cubie 1 is in corner cubicle 1, and so on) and they all are oriented so that the side marked with 0 looks toward the blue (or red for edge cubies) cross on the scaffolding.

Example 6.2. If the cube is in its solved state and we perform move ***F***—twist of the front face clockwise—then the cube's new state will be $p = (\rho, \sigma, x, y)$, where

$$\begin{aligned}
\rho &= (1243),\\
\sigma &= (1342),\\
x &= (2, 1, 1, 2, 0, 0, 0, 0),\\
y &= (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0).
\end{aligned}$$

6.2.2 Group structure of P. Isomorphism between P and G.

Not all states in $P^\star$ are legal states of the cube; some of them would require taking the cube apart and reassembling it into a configuration that would not be achievable by means of legal moves, such as swapping a corner with another corner. The set of all *legal* states, indicated as P, is such that each element can be obtained from the solved state of the cube by means of legal moves (i.e. basic moves and their combinations).

Let us stress once more that Rubik's cube group G is *not* the same thing as P. The set P is the set of legal states of the cube, while G is the group of *moves* that produce those states. One can think of every $g \in G$ as a function $g\colon P \to P$ that takes in a legal state and returns another legal state. However, it is possible to define a group operation on P and show that $G \cong P$. Given $p \in P$, we see that the map

$$\xi\colon G \to P, \quad \xi(g) = g(I) \tag{6.1}$$

where $I \in P$ is the solved state of the cube, is a bijection. Indeed, if we let $p \in P$, then by the very definition of P there exists a combination of legal moves $g \in G$ such that $g(I) = p$, which proves surjectivity; if we further assume $\xi(g) = \xi(h)$ for some $g, h \in G$, we get $g(I) = h(I)$. Since G is a

group, we know that g has inverse g^{-1}; if we apply it to the last equality, we obtain $g^{-1}(g(I)) = g^{-1}(h(I))$, whence $I = g^{-1}(h(I))$. Since G is a group, we know that g^{-1} must be the inverse of h. Thus, $g^{-1}h = 1_G$ implies $h = g$. Thus, ξ is a bijection.

For any $p, q \in P$, the bijectivity of ξ allows us to define the product

$$pq = \xi(\xi^{-1}(p)\xi^{-1}(q)).$$

Once this product is defined, it is easy to see that ξ is a homomorphism. Let $p, q \in P$ and $g, h \in G$ be such that $p = \xi(g)$ and $q = \xi(h)$. Then

$$\xi(g)\xi(h) = pq = \xi(\xi^{-1}(p)\xi^{-1}(q)) = \xi(gh).$$

Now it is equally simple to check that the product we just defined on P is a group operation. Assume $p, q, r \in P$ and $g, h, i \in G$ are such that $p = \xi(g)$, $q = \xi(h)$, and $r = \xi(i)$. Then

$$\begin{aligned}(pq)r &= \xi(\xi^{-1}(p)\xi^{-1}(q))\xi(i) = \xi(gh)\xi(i) = \xi(ghi) = \xi(g)\xi(hi) \\ &= p(\xi(\xi^{-1}(q)\xi^{-1}(r))) = p(qr),\end{aligned}$$

which shows the product on P is associative. The very definition of this product also shows that P is closed with respect to it. If $j = \xi(1_G)$, then $pj = \xi(\xi^{-1}(p)\xi^{-1}(j)) = \xi(g1_G) = \xi(g) = p$, and similarly $jp = p$, whence $j = 1_P$. Finally, $p\xi(g^{-1}) = \xi(g)\xi(g^{-1}) = \xi(gg^{-1}) = \xi(1_G) = 1_P$, therefore $\xi(g^{-1}) = p^{-1}$. Ultimately, P is a group with respect to the given product.

We now know that both G and P are groups, and that they are isomorphic thanks to the map ξ. We can therefore identify P with G and and element $g \in G$ with the corresponding state $\xi(g) = p = (\rho, \sigma, x, y) \in P$.

6.2.3 Twist constants

The product of P has so far been defined in terms of product in G—i.e., composition of moves. However, in order to prove the main results of this section, we will need a shift in perspective and see this same product in terms of product of states. This product will require combining the permutations and orientation vectors of two different states. As the reader may imagine, to combine permutations it will be enough to take the normal permutation product; however, combining orientation vectors will not prove to be equally easy, and will require the concept of *twist constants*,

which we will now introduce. (It is highly recommended that the reader tries the following for themselves, with their own Rubik's cube marked accordingly.)

If s is any cube state, we write

$$s = (\rho^s, \sigma^s, x^s, y^s),$$

where ^{s} is not an exponent, but merely an index to conveniently identify components of s.

For simplicity's sake, in this discussion we will work only with corner cubies and cubicles. The reasoning can easily be extended to edge cubie and cubicles.

Consider now the cube in its solved state $I = (\rho^I, \sigma^I, x^I, y^I)$ and let $b \in G$ be a basic move. We know we can identify b with the cube state $s = (\rho^s, \sigma^s, x^s, y^s)$ it produces; so, for simplicity's sake, let us allow a slight abuse of notation and say $b = (\rho^b, \sigma^b, x^b, y^b)$. When the cube is in its initial state, we have $x^I = (0, 0, 0, 0, 0, 0, 0, 0)$, i.e. $x^I_i = 0$ for $i = 1, \ldots, 8$.

Now consider, for example, the cubie located in cubicle 2 (which, in the solved state, is cubie 2) and let $b = \boldsymbol{R}$. (Remember $\boldsymbol{R}$ is the basic move that twists the right face of the cube 90 degrees clockwise.) We see that $\rho^{\boldsymbol{R}} = (2684)$, so when we first rotate the right side of the cube clockwise, cubie 2 moves from cubicle 2 to cubicle 6, and the facet of cubie 2 pointing toward the mark of cubicle 6 is marked with a 2; in other words, $x^{\boldsymbol{R}}_2 = 2$. Notice that $x^{\boldsymbol{R}}_2 = 2 = 0 + 2 = x^I_2 + 2$; it appears as if move $\boldsymbol{R}$ has added 2 to the value of cubie 2. We might be tempted to think that perhaps $\boldsymbol{R}$ adds 2 to the value of every cubie it moves, but it is easy to see that this is not the case. For example, after performing $\boldsymbol{R}$ on the solved cube, the value of cubie 4 changed from $x^I_4 = 0$ to $x^{\boldsymbol{R}}_4 = 1$, so in this case $\boldsymbol{R}$ seems to have added 1 to the value of cubie 4. However, if we perform $\boldsymbol{R}$ again—i.e., if we rotate the right face of the cube clockwise again—cubie 4 will move from cubicle 2 to cubicle 6, and it will show 0 toward the mark of its current cubicle, i.e. $x^{\boldsymbol{RR}}_4 = 0$. We notice that $x^{\boldsymbol{RR}}_4 = 0 = 3 = 1 + 2 = x^{\boldsymbol{R}}_4 + 2 \pmod 3$. So, $\boldsymbol{R}$ added 1 to the value of cubie 4 while this was in cubicle 4, but it added 2 to the value of cubie 4 when this was in cubicle 2. It seems move $\boldsymbol{R}$ adds different constants to the value of a cubie depending on the cubie's current location. If we keep performing $\boldsymbol{R}$ over and over, we see that the pattern repeats: The cubie currently located in cubicle 2 will be moved to cubicle 6, and its value will increase by $2 \pmod 3$. Similarly,

if we perform for example move $\boldsymbol{L'}$ over and over, we see that the value of the cubie located in cubicle 1 is increased by 1 each time. By trying this exercise with several other cubicles and moves, the reader can easily convince themselves that there is a different constant associated to each cubicle and each move. (This result will be proved later on, in Theorem 6.1.) The constants depend on how we have numbered the facets of the cube: Had we proceeded anticlockwise rather than clockwise, the same constants would be tied to different cubicles and moves.

As we have seen, the same move b involving the same corner cubicle i always increments the value of the cubie located in cubicle i by the same constant. To find out the value of a specific constant, we can simply subtract the old value of a cubie from its new value. More accurately, if i is a corner cubicle, for example, and n is the cubie currently located in i, the constant κ_i^b of cubicle i associated with basic move b can be computed as

$$\kappa_i^b = x_n^b - x_n^p \text{ (mod 3)},$$

where (mod 3) ensures that the value of the constant will always be 0, 1, or 2. (Edge cubies can only have two values, so in that case we would have (mod 2).)

Example 6.3. Let the cube be in its solved state. Corner cubies 1 and 2 are currently located in cubicles 1 and 2 respectively, and have both value 0. If we perform move $\boldsymbol{L'}$ on the cube, the value of cubie 1 will change from $x_1^I = 0$ to $x_1^{\boldsymbol{L'}} = 1$. To find out the constant relevant to this case, we compute $\kappa_1^{\boldsymbol{L'}} = x_1^{\boldsymbol{L'}} - x_1^I = 1 - 0 = 1$. We can verify this is correct by performing $\boldsymbol{L'}$ multiple times and observing how the value of any cubie located in cubicle 1 increases by 1 each time. Similarly, performing $\boldsymbol{R}$ we see that $\kappa_2^{\boldsymbol{R}} = x_2^{\boldsymbol{R}} - x_2^I = 2 - 0 = 2$, and if we do it over and over again, we see that this constant is added to the value of whichever cubie is located in cubicle 2.

Example 6.4. Let the cube be on its solved state. If we perform move $\boldsymbol{F}$, cubie 1 will move to cubicle 2 and assume value $x_1^{\boldsymbol{F}} = 2$. If we now perform move $\boldsymbol{R}$, cubie 1 will assume value $x_1^{\boldsymbol{FR}} = 1$, in agreement with our expectations, since

$$x_1^{\boldsymbol{FR}} = x_1^{\boldsymbol{F}} + \kappa_2^{\boldsymbol{R}} = 2 + 2 = 1 \text{ (mod 3)}.$$

We have said that the constant for cubicle i and basic move b can be computed as the difference between the value of the cubie that was in cubicle i prior to performing b, and the value that the same cubie has after performing b. If, as we have said, the constants are always the same regardless of how scrambled the cube may be, then computing the constant for cubicle i and basic move b should always yield the same result, no matter which cubie happens to be located in cubicle i. In other words, if cubie n is located in cubicle i, the constant for cubicle i and basic move b is $x_n^b - x_n^p \pmod 3$. If later on cubie m is in cubicle i, the constant can be computed as $x_m^b - x_m^p \pmod 3$, and we expect that $x_n^b - x_n^p = x_m^b - x_m^p \pmod 3$. Therefore, we can make things simple for ourselves and compute the constants with respect to the solved state. In the solved state of the cube, every cubie is in its original cubicle and its value is zero, which means that the constant for cubicle i and basic move b is simply the new value of cubie i after we performed b:

$$\kappa_i^b = x_i^b - x_i^I = x_i^b - 0 = x_i^b \pmod 3,$$

The huge advantage of this method is that, in order to find out the *all* constants of *any* legal move m, it is enough to perform m on the solved cube and make note of the resulting values of the cubies.

Example 6.5. Let the cube be in its solved state. If we perform move ***F***, for each corner cubicle i the constant $\kappa_i^{\boldsymbol{F}}$ is computed as

$$\kappa^{\boldsymbol{F}} = x_i^{\boldsymbol{F}} - x_i^I = x_i^{\boldsymbol{F}} - 0 = x_i^{\boldsymbol{F}}.$$

These constants are nothing but the components of the orientation vector

$$x^{\boldsymbol{F}} = (2, 1, 1, 2, 0, 0, 0, 0)$$

resulting after move ***F*** has been performed on the solved cube. For move ***R***, the constants of corner cubicles are the components of orientation vector

$$x^{\boldsymbol{R}} = (0, 2, 0, 1, 0, 1, 0, 2).$$

To find out the constants for move ***FR***, we perform ***F*** and ***R*** in succession on the solved cube and obtain vector

$$x^{\boldsymbol{FR}} = (1, 2, 1, 2, 0, 1, 0, 2).$$

We can now give a formal definition of the constants, for both corners and edges.

Definition 6.2. Let the cube be in its solved state. Let b be a basic move, and let i, j be a corner and edge cubicle respectively. The **corner twist constant** κ_i^b of corner cubicle i with respect to basic move b is defined as the value x_i^b that cubie i has after move b has been performed on the solved cube. Similarly, the **edge twist constant** ϵ_j^b of edge cubicle j with respect to basic move b is defined as the value y_j^b that cubie j has after move b has been performed on the solved cube.

We have claimed that the twist constants depend only on our labelling system, and that each pair made by a basic move and a cubicle will have a unique constant, regardless of the cubie currently located in the cubicle or of the value of such cubie. It is now time to formally prove this claim.

Theorem 6.1. *Given a labelling system on Rubik's cube, each twist constant is specific to each pair composed by a basic move and a cubicle, and it is the same regardless of the specific cubies or their values.*

Proof. We start our proof from the case of corner cubies. Let b be a basic move. If $b = \boldsymbol{U}$ or $b = \boldsymbol{D}$ (or their inverses), the claim is trivial: If the corner cubies in the up face show values $v_1, \ldots, v_4$, rotating the up face around will change the position of the cubies on this face, but it will not change the values $v_1, \ldots, v_4$ in any way. Move $b = \boldsymbol{U}$ also does not affect cubies on the down face. Therefore, no matter which cubies are located where on these faces or what values they have, the corner twist constant for basic move $\boldsymbol{U}$ is $\kappa_i^{\boldsymbol{U}} = 0$, for $i = 1, \ldots, 8$. An entirely analogous reasoning shows that $\kappa_i^{\boldsymbol{D}} = 0$, for $i = 1, \ldots, 8$.

Now imagine we could walk on the cubies. In our clockwise labelling system, each time we move from a cubie facet in the clockwise direction the number displayed on the facet we are currently on differs from the previous one by $1 \pmod 3$. So, for example, if the facet we are on displays 2, by moving one more facet on the same cubie in the clockwise direction we will land on a facet displaying $2 + 1 = 0 \pmod 3$. Since we cannot really walk ourselves on the cubies, we will do something different. Given a specific corner cubie, imagine that any blue cross on the scaffolding indicates our position on the cubie itself. For example, if the cube is in its solved state, cubie 1 is in cubicle 1, and the blue cross of cubicle 1 indicates the 0-facet

of cubie 1—that facet is our current position. If we perform $\boldsymbol{F}$, cubie 1 will end up in cubicle 2, and the blue cross of cubicle 2 will indicate the 2-facet of cubie 1. This is our new position: For all intents and purposes, this is the same as if we had walked on cubie 1 all the way from facet 0 to facet 2. Each basic move will make us 'walk away' a different number of facets from our starting facet depending on the cubicle where the cubie is currently located. For example, if we perform $\boldsymbol{F}$ on the solved cube, we will move two facets from facet 0 on cubie 1 (i.e., the value of cubie 1 will change from 0 to 2), but only one facet from facet 0 on cubie 4 (i.e., the value of cubie 4 will change from 0 to 1). This fact is the very meaning of the twist constants, and we shall make use of it in our proof.

We shall write our reasoning only for the front face—i.e., for move $\boldsymbol{F}$ and its inverse. The reasoning is completely analogous for all the other side faces and easily leads to the same conclusions. (For brevity's sake, we shall omit '(mod 3)' wherever there is no danger of confusion.) Move $\boldsymbol{F}$ leaves cubicles from 5 to 8 unaffected, whence $\kappa_i^{\boldsymbol{F}} = 0$ for $i = 5, \ldots 8$, regardless of the specific cubies in those cubicles or their values. On the other hand, given any cubie in cubicle 1, $\boldsymbol{F}$ makes us 'walk two facets away' from the current value-facet of the cubie; in other words, if cubie n is currently in cubicle 1 and x_n is its current value, its new value will be $x_n^{\boldsymbol{F}} = x_n + 2 \pmod 3$, yielding corner twist constant $\kappa_1^{\boldsymbol{F}} = 2$. It is easy to see that we would get the same result if we performed $\boldsymbol{F'}$ instead, whence $\kappa_1^{\boldsymbol{F'}} = 2$ too. By symmetry, this result applies to corner cubicle 3 as well, yielding $\kappa_3^{\boldsymbol{F}} = \kappa_3^{\boldsymbol{F'}} = 2$. However, move $\boldsymbol{F}$ only 'walks us away' one facet in the clockwise direction from the value-facet of a cubie in cubicle 2. This means that given value x_m for cubie m in cubicle 2, its new value after move $\boldsymbol{F}$ will be $x_m^{\boldsymbol{F}} = x_m + 1 \pmod 3$, yielding corner twist constant $\kappa_2^{\boldsymbol{F}} = 1$ (An analogous reasoning shows that $\kappa_2^{\boldsymbol{F'}} = 1$.) Symmetry allows us to deduce $\kappa_4^{\boldsymbol{F}} = \kappa_4^{\boldsymbol{F'}} = 1$. Notice once more that the reasoning above is independent of the cubies and their values; all that matters is how many 'steps' we take from the current value-facet to the new value-facet of a cubie with each basic move we perform, and this number depends on the position of each specific cubicle. This proves the claim for corner twist constants.

In the case of the edge twist constants, things are simpler: In order to always be beneath a red cross after a move has been performed, we only need to 'walk' one facet at most—in other words, each possible (basic) move adds 1 or 0 modulo 2 to an edge cubie's value. Let the cube be in an arbitrary legal state. If we perform $\boldsymbol{F}$ or its inverse, only edge cubies located in

edge cubicles $1, 2, 3, 4$ will be affected; all other edge cubies are unaffected, whence the edge twist constant $\epsilon_j^F = 0$ for $j = 5, \ldots, 12$. Similarly, $\epsilon_j^{F'} = 0$ for $j = 5, \ldots, 12$. The symmetric, alternating fashion in which we have numbered edge cubies and labelled edge cubicles makes it so that, when we perform $\boldsymbol{F}$ on the cube, all edge cubies on the front face will change value: if the value is 0, it will become 1 and vice-versa, yielding twist constant $\epsilon_j^F = 1$, for $j = 1, \ldots, 4$; similarly, $\epsilon_j^{F'} = 1$ for $j = 1, \ldots, 4$. Thus the edge twist constants are always 1 for all cubicles affected by a given basic move b, and 0 otherwise. An analogous reasoning proves the claim for the remaining basic moves.

Ultimately, all twist constants depend only on the labelling system and each pair of basic moves and cubicles. □

6.2.4 Product of states

Let $b, d \in G$ be two basic moves. We know we can think of them as the states they induce on the cube, which we indicate as $b = (\rho^b, \sigma^b, x^b, y^b)$ and $d = (\rho^d, \sigma^d, x^d, y^d)$ respectively. In order to define the product bd in terms of product of states, we can proceed as follows. Permutations can be applied subsequently in a natural way, so that the corner and edge permutations of bd are simply $\rho^d\rho^b$ and $\sigma^d\sigma^b$, respectively. (Recall that, in a product of permutations, the order of execution is right-to-left. Therefore, if we perform move bd, we are performing b first and d then, leading to the corner permutation $\rho^d\rho^b$.) As said earlier, the composition of vectors x^b and x^d (or y^b and y^d) is a bit more complicated. The situation at the starting position is the following:

$$\begin{aligned} x^I &= (0, 0, 0, 0, 0, 0, 0, 0), \\ y^I &= (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0); \end{aligned}$$

if we perform b on the cube, the new value of each cubie is obtained adding the appropriate twist constant to the old value of the cubie:

$$\begin{aligned} x_i^b &= x_i^I + \kappa_i^b = 0 + \kappa_i^b = \kappa_i^b \\ y_j^b &= y_j^I + \epsilon_j^b = 0 + \epsilon_j^b = \epsilon_j^b, \end{aligned}$$

for all corner and edge cubies i, j affected by move b.

If we then perform move d, for each corner cubie i its new value will be obtained by adding to its current value the appropriate twist constant of

the cubicle where it is currently located—i.e, where it ended up after performing move b. The location of cubie i after performing move b is therefore $\rho^b(i)$. Thus, the twist constant to be added is $\kappa^d_{\rho^b(i)} = x^d_{\rho^b(i)}$. Analogously, one finds that for edge cubies the appropriate constant is $\epsilon^d_{\sigma^b(j)} = y^d_{\sigma^b(j)}$. If we define

$$\begin{aligned} x^d_{\rho^b} &:= (x^d_{\rho^b(1)}, \ldots, x^d_{\rho^b(8)}) \\ y^d_{\sigma^b} &:= (y^d_{\sigma^b(1)}, \ldots, y^d_{\sigma^b(12)}) \end{aligned} \tag{6.2}$$

we see that the vectors x^{bd} and y^{bd}—which represent the cubie orientations after move bd has been performed—can be expressed as

$$\begin{aligned} x^{bd} &= (x^b_1 + x^d_{\rho^b(1)}, \ldots, x^b_8 + x^d_{\rho^b(8)}) = x^b + x^d_{\rho^b} \\ y^{bd} &= (y^b_1 + y^d_{\sigma^b(1)}, \ldots, y^b_{12} + y^d_{\sigma^b(12)}) = y^b + y^d_{\sigma^b}. \end{aligned}$$

Ultimately, the product of basic moves b and d is defined as

$$bd = (\rho^b, \sigma^b, x^b, y^b)(\rho^d, \sigma^d, x^d, y^d) = (\rho^d\rho^b, \sigma^d\sigma^b, x^b + x^d_{\rho^b}, y^b + y^d_{\sigma^b}).$$

Since all legal moves can be expressed as the product of basic moves, this definition naturally extends to the product of any two legal moves. To see why this is true, consider the following basic moves:

$$\begin{aligned} b &= (\rho^b, \sigma^b, x^b, y^b), \\ c &= (\rho^c, \sigma^c, x^c, y^c), \\ d &= (\rho^d, \sigma^d, x^d, y^d). \end{aligned}$$

We need to make sure that the product bcd is still a state in P. The first step is computing bc; by definition, this is just

$$(\rho^b, \sigma^b, x^b, y^b)(\rho^c, \sigma^c, x^c, y^c) = (\rho^c\rho^b, \sigma^c\sigma^b, x^b + x^c_{\rho^b}, y^b + y^c_{\sigma^b}),$$

This quadruplet does not describe the situation after a single basic move, and since the product of states was defined for basic moves only, it might break down when we try to compute $(bc)d$. However, if we proceed in our calculation, we obtain

$$\begin{aligned} (bc)d &= (\rho^c\rho^b, \sigma^c\sigma^b, x^b + x^c_{\rho^b}, y^b + y^c_{\sigma^b})(\rho^d, \sigma^d, x^d, y^d) \\ &= (\rho^d\rho^c\rho^b, \sigma^d\sigma^c\sigma^b, (x^b + x^c_{\rho^b}) + x^d_{\rho^c\rho^d}, (y^b + y^c_{\sigma^b}) + y^d_{\sigma^c\sigma^b}). \end{aligned}$$

We see that the result is in P: The first two terms are permutations, as they are supposed to be; the term $(x^b + x^c_{\rho^b})$ is a vector in C_3^8, and so is $x^d_{\rho^c\rho^d}$, thus their sum is also in C_3^8. Similarly, we have $(y^b + y^c_{\sigma^b}) + y^d_{\sigma^c\sigma^b} \in C_2^{12}$. Also recall that $x^d_{\rho^c\rho^d}$ is simply the vector x^d describing the orientation of the corner cubies after basic move d has been performed on the solved cube, although its components are scrambled according to permutation $\rho^c\rho^d$ to account for the location of the cubies once bd has been performed. Simply put, the expression

$$(x^b + x^c_{\rho^b}) + x^d_{\rho^c\rho^d}$$

means that the values of the corner cubies after move bc (which are listed in $(x^b + x^c_{\rho^b})$) is being increased by the corner twist constants related to move d and to the current locations of the cubies (these constants are the components of $x^d_{\rho^c\rho^d}$), leading to the correct new value of each corner cubie. The reasoning is entirely analogous for edge cubies—i.e. for the expression $(y^b + y^c_{\sigma^b}) + y^d_{\sigma^c\sigma^b}$. We can extend our reasoning and conclude that if the product $b_1 \cdots b_n$ is in P and accurately describes the state of the cube after moves $b_1, \ldots, b_n$ have been performed, the same is true of the product $b_1 \cdots b_{n+1}$ after moves $b_1, \ldots, b_{n+1}$ have been performed. Since any combination of non-basic moves is a product of basic moves, we see that the product of any number k of non-basic moves $\boldsymbol{M}_1, \ldots, \boldsymbol{M}_k$ is in P and accurately describes the state of the cube after $\boldsymbol{M}_1, \ldots, \boldsymbol{M}_k$ have been performed.

Remark 6.1. One might wonder if the product of states we just defined is compatible with the map ξ defined in (6.1)—in other words, if ξ still behaves as a homomorphism when the product between elements of P is carried out as product of states. The answer is yes. If we agree to define

$$\xi(gh) = gh(I) = (\rho^{gh}, \sigma^{gh}, x^{gh}, y^{gh}) := (\rho^h\rho^g, \sigma^h\sigma^g, x^g + x^h_{\rho^g}, y^g + y^h_{\sigma^g}),$$

where $\xi : G \to P$ is as in (6.1), then we have that

$$\begin{aligned}\xi(gh) = gh(I) &= (\rho^{gh}, \sigma^{gh}, x^{gh}, y^{gh}) := (\rho^h\rho^g, \sigma^h\sigma^g, x^g + x^h_{\rho^g}, y^g + y^h_{\sigma^g}) \\ &= (\rho^g, \sigma^g, x^g, y^g)(\rho^h, \sigma^h, x^h, y^h) = \xi(g)\xi(h),\end{aligned}$$

and for any $g \in G$,

$$\xi(1_G) = \xi(gg^{-1}) = \xi(g)\xi(g^{-1}) = \xi(g)\xi(g)^{-1} = I.$$

6.3 Semidirect product

Let us consider the following two subgroups of G:

$$G_O := \{(\rho^g, \sigma^g, x^g, y^g) \in G \,|\, x^g = 0, y^g = 0\}$$
$$G_P := \{(\rho^g, \sigma^g, x^g, y^g) \in G \,|\, \rho^g = 1, \sigma^g = 1\}.$$

Note that we are still persisting in our abuse of notation; what we mean by $g = (\rho^g, \sigma^g, x^g, y^g) \in G$ is in fact that move $g \in G$ induces a legal cube state (i.e., an element of P) which we indicate as $(\rho^g, \sigma^g, x^g, y^g)$ to avoid cumbersome notation. This is made possible by the fact G and P are isomorphic. Elements of G_O preserve the orientation of the cubies, though they may change their position; similarly, elements of G_P preserve the position of the cubies, but not necessarily their orientation. To better visualise this, suppose the cube is in a certain state $s = (\rho^s, \sigma^s, x^s, y^s)$, and let $g \in G_O$ and $h \in G_P$. The states g, h will be of the form

$$g = (\rho^g, \sigma^g, 0, 0)$$

$$h = (1, 1, x^h, y^h)$$

and their product with s will give rise to, respectively

$$sg = (\rho^s, \sigma^s, x^s, y^s)(\rho^g, \sigma^g, 0, 0) = (\rho^g \rho^s, \sigma^g \sigma^s, x^s, y^s)$$

$$sh = (\rho^s, \sigma^s, x^s, y^s)(1, 1, x^h, y^h) = (\rho^s, \sigma^s, x^s + x^h_{\rho^s}, y^s + y^h_{\sigma^s}).$$

We see that in state sg, the orientation of the cubies is the same as in state s, and in state sh their position is the same as it was in state s. In particular, if $s = I$, this means that in state sg, the cubies will be correctly oriented, albeit possibly in the wrong cubicles, and in state sh the cubies will be in their correct cubicle although their orientation may be incorrect.

Our goal is to prove that the Rubik's cube group is the semidirect product of G_O and G_P. To this end, we will need two propositions and one lemma.

Lemma 6.1. *If $g = (\rho^g, \sigma^g, x^g, y^g) \in G$, its inverse is given by*

$$g^{-1} = ((\rho^g)^{-1}, (\sigma^g)^{-1}, -x^g_{(\rho^g)^{-1}}, -y^g_{(\sigma^g)^{-1}}),$$

where $-x^g = (-x^g_1, \ldots, -x^g_8)$ and $-y^g = (-y^g_1, \ldots, -y^g_{12})$.

Proof. The proof is a just matter of computation:

$$\begin{aligned}
&(\rho^g, \sigma^g, x^g, y^g)((\rho^g)^{-1}, (\sigma^g)^{-1}, -x^g_{(\rho^g)^{-1}}, -y^g_{(\sigma^g)^{-1}}) \\
&= ((\rho^g)^{-1}\rho^g, (\sigma^g)^{-1}\sigma^g, x^g - x^g_{(\rho^g)^{-1}\rho^g}, y^g - y^g_{(\sigma^g)^{-1}\sigma^g}) \\
&= (1, 1, x^g - x^g, y^g - y^g) \\
&= (1, 1, 0, 0) \\
&= 1_G,
\end{aligned}$$

whence indeed $g^{-1} = ((\rho^g)^{-1}, (\sigma^g)^{-1})$ as claimed. A similar computation shows that $g^{-1}g = 1_G$. □

Proposition 6.1. *The set G_P is a normal subgroup of G.*

Proof. It is obvious that $G_P \subset G$. If $g, h \in G_P$, then

$$\begin{aligned}
g &= (1, 1, x^g, y^g), \\
h &= (1, 1, x^h, y^h),
\end{aligned}$$

and $gh = (1, 1, x^g + x^h, y^g + y^h)$, whence $gh \in G_P$. The identity element of G, that is $1_G = (1, 1, 0, 0)$, is obviously in G_P. If $g = (1, 1, x^g, y^g) \in G_P$, then by Lemma 6.1 $g^{-1} = (1, 1, -x^g, -y^g)$ is in G_P. This proves that $G_P \leq G$.

To prove that $G_P \lhd G$, let $g \in G$ and $h \in G_P$. Then

$$\begin{aligned}
ghg^{-1} &= (\rho^g, \sigma^g, x^g, y^g)(1, 1, x^h, y^h)((\rho^g)^{-1}, (\sigma^g)^{-1}, -x^g_{(\rho^g)^{-1}}, -y^g_{(\sigma^g)^{-1}}) \\
&= (\rho^g, \sigma^g, x^g + x^h_{\rho^g}, y^g + y^h_{\sigma^g})((\rho^g)^{-1}, (\sigma^g)^{-1}, -x^g_{(\rho^g)^{-1}}, -y^g_{(\sigma^g)^{-1}}) \\
&= ((\rho^g)^{-1}\rho^g, (\sigma^g)^{-1}\sigma^g, x^g + x^h_{\rho^g} - x^g_{(\rho^g)^{-1}\rho^g}, y^g + y^h - y^h_{(\sigma^g)^{-1}\sigma^g}) \\
&= (1, 1, x^h_{\rho^g}, y^h_{\sigma^g}) \in G_P.
\end{aligned}$$

□

Remark 6.2. There is a less formal but more intuitive way of seeing why Proposition 6.1 is true. If $g, h \in G_P$, both of them will not change the position of any cubicle, and thus neither will their combination. This means $gh \in G_P$. By definition, the identity 1_G will leave every cubie in whichever cubicle it is located, thus $1_G \in G_P$. If $g \in G_P$, performing it will not change the location of any cubie; if g^{-1} changed the location of some cubies, then

the combination gg^{-1} would not be the identity, which is impossible by definition. Therefore, $g^{-1} \in G_P$ and $G_P \leq G$. Let now $g \in G$ and $h \in G_P$. If g leaves all cubies where they are, then by the above so does g^{-1}; we know h does not change the position of any cubies, and therefore ghg^{-1} also leaves all cubies where they are hence $ghg^{-1} \in G_P$. On the other hand, if g does change the location of some cubies, then g^{-1} will put them back where they were, and ultimately $ghg^{-1} \in G_P$ again. Thus, $G_P \lhd G$.

Proposition 6.2. *The set G_O is a subgroup of G.*

Proof. Again, obviously $G_O \subset G$. Since $1_G = (1, 1, 0, 0)$, in particular we have $1_G \in G_O$. Let $g, h \in G_O$ be defined as

$$g = (\rho^g, \sigma^g, 0, 0),$$
$$h = (\rho^h, \sigma^h, 0, 0).$$

Then

$$gh = (\rho^g, \sigma^g, 0, 0)(\rho^h, \sigma^h, 0, 0) = (\rho^h \rho^g, \sigma^h \sigma^g, 0, 0) \in G_O,$$

and $g^{-1} = ((\rho^g)^{-1}, (\sigma^g)^{-1}, 0, 0) \in G_O$. Ultimately, $G_O \leq G$. □

Remark 6.3. A more intuitive way of understanding why Proposition 6.2 is true is the following. The identity 1_G preserves all orientations by definition and thus it belongs to G_O. If $g, h \in G_O$, then both preserve all orientations, and so will their product. If $g \in G_O$ preserves all orientations, so must g^{-1}, for if it did not, then $gg^{-1} = 1_G$ would not preserve some orientations either, which is a contradiction. Therefore, $G_O \leq G$.

We are now ready to prove the main result of this section.

Theorem 6.2. *The Rubik's cube group G is the semidirect product of the subgroup of position-preserving moves and the subgroup of orientation-preserving moves. In other words,*

$$G = G_O \rtimes G_P.$$

Proof. By proposition 6.1, we know that $G_P \lhd G$. If $g \in G_O \cap G_P$, then we know that $\rho^g = 1$, $\sigma^g = 1$, $x^g = 0$ and $y^g = 0$. Thus, $g = (1, 1, 0, 0) = 1_G$. Finally, for any $g = (\rho^g, \sigma^g, x^g, y^g) \in G$, we see that

$$g_O = (\rho^g, \sigma^g, 0, 0) \in G_O \quad \text{and}$$
$$g_P = (1, 1, x^g_{(\rho^g)^{-1}}, y^g_{(\sigma^g)^{-1}}) \in G_P$$

are such that

$$\begin{aligned} g_O g_P &= (\rho^g, \sigma^g, 0, 0)(1, 1, x^g_{(\rho^g)^{-1}}, y^g_{(\sigma^g)^{-1}}) \\ &= (\rho^g, \sigma^g, x^g, y^g) = g, \end{aligned}$$

whence $G = G_O G_P$. This concludes the proof. □

6.4 Wreath product

In our discussion of Rubik's cube, we have dealt primarily with the *legal* Rubik's cube group, i.e. the group G arising from legal moves alone, which we have seen to be isomorphic to the group P of legal states of the cube. However, we have also seen that P is a subset of $P^\star$, the set of all *possible* states of the cube, legal or illegal. The only way to rearrange the cube into an illegal state $s \in P^\star \setminus P$ is to take the cube apart and reassemble it in state s. The set $P^\star$ is therefore strictly larger than P, because it contains as elements states that are not contained in P, such as states where two adjacent corners are swapped around. We will henceforth refer to $P^\star$ as the *illegal Rubik's group*; the aim of this section is to show that $P^\star$ is isomorphic to a direct product of wreath products—and thus that it is indeed a group.

6.4.1 The groups P_C and P_E, and their relation to $P^\star$

Let us start by considering the set $P_C \subset P^\star$ of all possible states (legal or illegal) of the corner cubies. Elements of P_C describe all possible orientations of all corner cubies in any location they may be, disregarding edge cubies entirely. In other words, we define the set P_C as

$$P_C = \{c \in P^\star \mid c = (\rho^c, 1, x^c, 0)\}.$$

Since the edge permutation and the edge orientation vector are always 1 and 0 respectively for any $c \in P_C$, we may leave them out and write simply $c = (x^c, \rho^c)$. Note that we have swapped the positions of the permutation and the orientation vector. This change of order does not influence our reasoning, and it is useful in that it better suits the definition of external semidirect product, which we will need shortly.

We know that the group of all possible permutations over 8 corner cubies is S_8, and that the set of all their possible orientations is $X_3^8 = \{0, 1, 2\}^8$. Thus, if $c = (x^c, \rho^c) \in P_C$, then $c \in X_3^8 \times S_8$ as well, which means that

$P_C \subset X_3^8 \times S_8$. On the other hand, if we take any pair $(x, \rho) \in X_3^8 \times S_8$, this pair describes a possible state (legal or not) of the corner cubies, and therefore it is an element of P_C. Thus, $P_C = X_3^8 \times S_8$. An entirely analogous reasoning allows to define the set P_E of all possible states of edge cubies as

$$P_E = \{e \in P^\star \mid c = (1, \sigma^e, 0, y^e)\}$$

and conclude that $P_E = X_2^{12} \times S_{12}$. Exactly as we did for P_C, we can more conveniently write an element $(1, \sigma^e, 0, y^e)$ of P_E as (y^e, σ^e).

One might wonder whether P_C and P_E are groups with respect to the same operation we defined on the legal Rubik's group G. To verify if this is the case, let (x^c, ρ^c) and (x^d, ρ^d) be any two states of the corner cubies. Their product in terms of the same operation defined on G is

$$(x^c, \rho^c)(x^d, \rho^d) = (x^c + x^d_{\rho^c}, \rho^d \rho^c). \tag{6.3}$$

Similarly, if (y^e, σ^e) and (y^f, σ^f) are any two elements of P_E, we can define a binary operation as

$$(y^e, \sigma^e)(y^f, \sigma^f) = (y^e + y^f_{\sigma^e}, \sigma^f \sigma^e). \tag{6.4}$$

The reader may have noticed the similarity between (6.3), (6.4) and the operation defined in Theorem 4.1 for semidirect products. This is no accident. The following lemma will show that (6.3) relies on an action of S_8 on X_3^8, and that P_C is thus their semidirect product. This, in turn, will imply that P_C is the wreath product of X_3 and S_8.

Lemma 6.2. *The group P_C is the wreath product of X_3 with S_8. In other words, $P_C = X_3 \wr_8 S_8 = X_3^8 \rtimes S_8$.*

Proof. All we need to do is show that the conditions of Definition 5.3 are met. Let $X = \{1, \ldots, 8\}$. Both X_3^8 and S_8 are groups; the next ingredient we need is an action μ of S_8 on X. By Definition 5.1, μ must be a homomorphism $S_8 \to \Sigma(X)$; however, $\Sigma(X) = S_8$, therefore it suffices to choose $\mu = \mathrm{id}_{S_8}$. In order to obtain the semidirect product of X_3^8 with S_8, we need an action of the latter on the former. From Definition 5.3 and the discussion that follows it, we know that $\phi : S_8 \to \mathrm{Aut}\, X_3^8$ is a group action of S_8 on X_3^8

if we define it as

$$\begin{aligned}\phi_\rho(x) = \phi_\rho(x_1, \ldots, x_8) &= (x_{\mu_\rho(1)}, \ldots, x_{\mu_\rho(8)}) = (x_{\mathrm{id}_{S_8}(\rho)(1)}, \ldots, x_{\mathrm{id}_{S_8}(\rho)(8)}) \\ &= (x_{\rho(1)}, \ldots, x_{\rho(8)}) \overset{(\star)}{=} x_\rho, \quad \text{for any } \rho \in S_8,\ x \in X_3^8.\end{aligned} \tag{6.5}$$

(Notice that in $(\star)$ we made use of the notation described in (6.2)).

By Definition 4.2, the set $P_C = X_3^8 \times S_8$ equipped with operation

$$(x^c, \rho^c)(x^d, \rho^d) = (x^c + \phi_{\rho^c}(x^d), \rho^d\rho^c), \quad c, d \in P_C,\ x^c, x^d \in X_3^8,\ \rho^c, \rho^d \in S_8,$$

is the semidirect product $X_3^8 \rtimes S_8$, as desired. Notice that, by (6.5), we have $\phi_{\rho^c}(x^d) = x^d_{\rho^c}$, whence

$$(x^c, \rho^c)(x^d, \rho^d) = (x^c + \phi_{\rho^c}(x^d), \rho^d\rho^c) = (x^c + x^d_{\rho^c}, \rho^d\rho^c),$$

showing that indeed (6.3) relies on an action of S_8 on X_3^8. □

We come to similar conclusions about (6.4) and P_E.

Lemma 6.3. *The group P_E is the wreath product of X_2 with S_{12}. In other words, $P_E = X_2 \wr_{12} S_{12} = X_2^{12} \rtimes S_{12}$.*

Proof. The proof is entirely analogous as the proof of Lemma 6.2. □

The main claim of this section is now trivial to prove.

Theorem 6.3. *The illegal Rubik's cube group $P^\star$ is isomorphic to the direct product of wreath products $X_3 \wr_8 S_8$ and $X_2 \wr_{12} S_{12}$.*

Proof. We have that

$$P^\star = \{(\rho, \sigma, x, y) \,|\, \rho \in S_8, \sigma \in S_{12}, x \in X_3^8, y \in X_2^{12}\}$$

and

$$(X_3 \wr_8 S_8) \times (X_2 \wr_{12} S_{12}) = \{((x, \rho), (y, \sigma)) \,|\, \rho \in S_8, \sigma \in S_{12}, x \in X_3^8, y \in X_2^{12}\};$$

the group operation on P^* is the same as on G—concatenation of moves, or equivalently, product of states.

Define $\lambda\colon (X_3 \wr_8 S_8) \times (X_2 \wr_{12} S_{12}) \to P^\star$ in such a way that

$$\lambda((x, \rho), (y, \sigma)) = (\rho, \sigma, x, y).$$

Then λ is obviously bijective. Let $\phi\colon S_8 \to \operatorname{Aut} X_3^8$ be the action of S_8 on X_3^8, and $\psi\colon S_{12} \to \operatorname{Aut} X_2^{12}$ the action of S_{12} on X_2^{12}. Then, if $((x,\rho),(y,\sigma))$ and $((x',\rho'),(y',\sigma'))$ are any two elements of $(X_3 \wr_8 S_8) \times (X_2 \wr_{12} S_{12})$, we have

$$\begin{aligned}
&\lambda(((x,\rho),(y,\sigma))((x',\rho'),(y',\sigma'))) = \lambda((x,\rho)(x',\rho'),(y,\sigma)(y',\sigma')) \\
&= \lambda((x+\phi_\rho(x'),\rho'\rho),(y+\psi_\sigma(y'),\sigma'\sigma)) = (\rho'\rho,\sigma'\sigma,x+\phi_\rho(x'),y+\psi_\sigma(y')) \\
&\overset{(*)}{=} (\rho'\rho,\sigma'\sigma,x+(x'_{\rho(1)},\dots,x'_{\rho(8)}),y+(y'_{\sigma(1)},\dots,y'_{\sigma(12)})) \\
&= (\rho'\rho,\sigma'\sigma,x+x'_\rho,y+y'_\sigma) = (\rho,\sigma,x,y)(\rho',\sigma',x',y') \\
&= \lambda((x,\rho),(y,\sigma))\lambda((x',\rho'),(y',\sigma')),
\end{aligned}$$

where in $(*)$ we have written out the result of the actions ϕ and ψ, and used the notation

$$\begin{aligned}
(x'_{\rho(1)},\dots,x'_{\rho(8)}) &:= x'_\rho \\
(y'_{\sigma(1)},\dots,y'_{\sigma(8)}) &:= y'_\sigma.
\end{aligned}$$

This concludes the proof. □

In the proof above we have said that the product of states we defined on the legal Rubik's group (or on P_C and P_E) is a group operation on $P^\star$ as well. Indeed, it is not difficult to see that all the properties of a group operation hold for the product of states on $P^\star$. This makes G, P_C, and P_E proper subgroups of $P^\star$ with respect to the product of states. Ultimately, this operation is equivalent to concatenation of moves (legal or not). If we consider the set $G^\star$ of all possible moves—legal or illegal—that can be performed on the cube, it is easy to convince oneself that it is a group under concatenation. We can thus extend the map ξ appeared in (6.1) to obtain

$$\xi^\star\colon G^\star \to P^\star;$$

the same reasoning used in section 6.2.2 shows that $\xi^\star$ is a group isomorphism.

The interested reader may find more about the algebra of Rubik's cube in [6], [5], and [7].

References

[1] C. C. Pinter *A Book of Abstract Algebra*, second edition, Dover publications, 2010

[2] J. J. Rotman *An Introduction to the Theory of Groups*, fourth edition, Springer-Verlag, 1995

[3] W. R. Scott *Group Theory*, Prentice-Hall, Inc., 1964

[4] M. Suzuki *Group Theory I*, Springer-Verlag, 1982

[5] D. Joyner *Adventures in Group Theory: Rubik's Cube, Merlin's Machine, and Other Mathematical Toys*, Johns Hopkins, 2008

[6] C. Bandelow *Inside Rubik's cube and beyond* , Birkhäuser Boston, 1982

[7] J. Häsä *Ryhmäteoreettinen näkökulma Rubikin kuutioon*, Helsingin Yliopiston Matematiikan ja tilastotieteen laitos, 2008
https://www.cs.helsinki.fi/u/jhasa/kurssit/rubik_s12/materiaali_rubik12.pdf
Last consulted in December 2016

[8] K. Conrad, *Dihedral groups*, University of Connecticut, 2016
http://www.math.uconn.edu/ kconrad/blurbs/grouptheory/dihedral.pdf
Last consulted in December 2016

[9] K. Elce, *Direct products*, California State University, 2009
http://www.csus.edu/indiv/e/elcek/m210a/directprodn.pdf
Last consulted in December 2016

[10] L. Daniels, *Group Theory and the Rubik's Cube*, Lakehead University, 2014
https://www.lakeheadu.ca/sites/default/files/uploads/77/docs/Daniels_Project.pdf
Last consulted in December 2016

[11] M. Welleda Baldoni, Ciro Ciliberto, G.M. Piacentini Cattaneo *Elementary Number Theory, Cryptography and Codes*, Springer, 2009