SOLVING RUBIK'S CUBE

BERNDT E. SCHWERDTFEGER

For Sylvia, who once wondered how
calculations might restore the magic

Abstract. Description of a strategy for solving *Rubik*'s cube using methods and concepts of finite groups, calculating the magic.

Preface

When visiting friends last summer I got hold of a *magic cube* in a fairly scrambled state. At once I felt impelled to untwist it, trying hard to recollect aged routines. When sitting in the marvelous garden, scribbling my next unscrambling turns, I attracted the curiosity of my hostess, how I could *calculate* the magic.

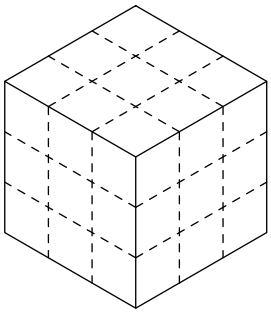
Some 30 years ago, when the magic fever was at its peak, I was infected through the regular column of Douglas Hofstadter in Scientific American [3]. I followed his advice to "use conjugates a lot" and soon had the essential *swapping* and *twisting* operators at hand, which together with the *principle of conjugacy* suffice to fix a scrambled cube.

This article describes my set of unscrambling operators together with the strategy that I follow during the pursuit. I put this into perspective to other strategies, which you may prefer, as they can be performed faster – but you have to learn much more – or they are more efficient in terms of number of turns. To go deeper you need to understand some mathematical concepts, like *groups*; some ideas are developed in the appendix.

Berlin, 22 September 2010

 version 1.1

1. The magic group



1.1. Rubik's Cube.

Let's have a closer look at *Rubik*'s Cube. It apparently consists of $3\times3\times3 = 27$ little cubes that are called *cubies*, but you immediately realize that the inner little cube is invisible and remains invisible when turning the faces. So every turn permutes

2010 *Mathematics Subject Classification.* Primary 20B25; Secondary 20B30, 20B35.

Key words and phrases. Rubik's Magic Cube, conjugacy, group structure, cubemeister, permutation groups, orbits, orders and periods, cycle.

26 cubes. But, wait a sec, the center cubes on each face do not move either: though they are rotating, the effect is indistinguishable from before the move. In fact, the construction of *Rubik*'s Magic Cube is such that the six center faces are attached to each other by an inner spindle holding them together. And the remaining small cubes are only almost cubical, having little feet toward the middle of the cube, where they are held together to their (current) neighbour when you make a turn. A really *magic* Magic Cube.

So, we only have 20 small *cubies* that are mixed up, when you play the Cube. These 20 pieces come in two flavours

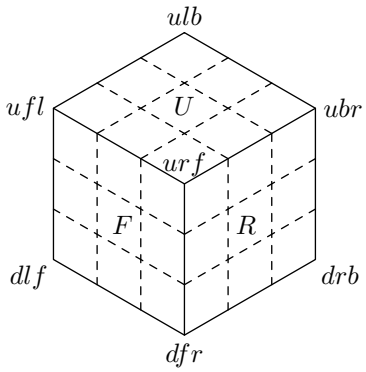
- 8 *corner* pieces with three different colours (together $3 \cdot 8 = 24$ faces)
- 12 *edge* pieces with two different colours (together $2 \cdot 12 = 24$ faces)

1.2. **Notions and notation.** Here I adopt the international standard notation as proposed by *David Singmaster* [1, 3, 7]. When you put the Cube in front of you the six faces are named *front* F, *back* B, *left* L, *right* R, *upper* U and *down* D. A *clockwise* quarter turn of a face will be denoted by the same letter, like F: a turn of the *front* to the right by 90 degrees. Attention: a clockwise direction at the *back* side B is moving the top line to the *left*! *Clockwise* means: as seen by its face. The notation for the counterclockwise direction is marked by a *dash*, like F'.

We can *combine* any moves, like F, R, U in this sequence, and write it $F \cdot R \cdot U$ and think of it as a kind of *multiplication*. We make the usual abbreviations like $F \cdot F = F^2$, $L \cdot L \cdot L = L^3$, ...etc. Remark that 4 clockwise turns of any face L, R, F, B, U, D leaves the cube identical to the previous state. The *identity* turn – *do nothing* – is denoted I, hence $U^4 = I$, as is $L^4 = R^4 = F^4 = \cdots = I$. You see that $F \cdot F' = I$ and $F' = F^3$; we also write this $F' = F^3 = F^{-1}$.

Beware, though, that the order of the *factors* in our *combined* move is important: $F \cdot R \neq R \cdot F$! Only these commutate: $F \cdot B = B \cdot F$, $R \cdot L = L \cdot R$, $U \cdot D = D \cdot U$.

The location on the cube occupied by a cubie is called a *cubicle*. The *cubicles* will be named by the position they occupy relative to their faces. The *corner* at the *u*pper, *r*ight, *f*ront position will be called urf.



The figure shows 7 corners, the corner *dbl* is hidden. Although as a cubicle $urf = rfu = fur$, the order becomes important when we consider moves and take care of the orientation at the target. We will let $urf^+ = rfu$ denote the *twist* by 120 degrees and $urf^- = fur$ the counterclockwise twist.

The move F moves the cubie in cubicle urf to the cubicle dfr and this will denoted by $urf \xrightarrow{F} rdf$, as the upper face moves to the right, the right one moves to the down face and the front face stays in front; in total F moves four cubies in the cubicles ufl, urf, dfr, dlf in a circular way

$$urf \xrightarrow{F} rdf \qquad rdf \xrightarrow{F} dlf \qquad dlf \xrightarrow{F} luf \qquad luf \xrightarrow{F} urf$$

Edge cubicles will be named similarly: the *u*pper, *r*ight *edge* will be denoted as ur, the front-right edge as fr, and so on. A *flip* is denoted $uf^+ = fu$. The *cycle* notation for F is

$$F = (urf\ rdf\ dlf\ luf)(uf\ rf\ df\ lf)$$

1.3. **Rubik's Group.** It is clear that you can perform an *infinite* number of operations, building moves from the six letters L, R, F, B, U, D in a variety of ways. The number of states that the cube can attain is *finite*, as there is only a finite number of cubies for a finite number of cubicles to be in.

Hence, a lot of operations lead to the same state, like $U^4 = I$ for example. Here is a more astonishing one: $RL^{-1}F^2B^2RL^{-1}URL^{-1}F^2B^2RL^{-1} = D$. That is, turns on the *down* face can be achieved by turns of the other five faces – isn't this *strange*?

The finite set of all states of the Cube is denoted G and it is generated by the moves R, L, F, B, U, D; in fact, as we have just seen, we could get away with one of them, we would still reach all possible states of the magic puzzle. Any two states $X, Y \in G$ can be combined to produce a new state $X \cdot Y \in G$ and any $X \in G$ has an inverse $X' \in G$ such that $X \cdot X' = I$. The state I corresponds to the unscrambled cube and is its neutral element. Hence, the set of all *states* of the magic cube, with the combination of moves as multiplication, satisfy the axioms of a group, *Rubik*'s group.

A *scrambled* cube $s \in G$ asks for a sequence of turns $t \in G$ such that applying it to s gives identity: $s \cdot t = I$. Of course, $t = s^{-1}$, but the problem is, we do not know the individual factors that have build up the state s if nobody told us, so we need to find a method. In the next section 2 on resolution methods we will see strategies for solving a scrambled cube. Some of them make use of group theory.

1.4. **Conjugacy.** The *Principle of Partial Inverses* [1, p. 21] states

> Any cubies moved by a process t will later be restored to their starting positions by t^{-1}, providing they have not been moved by any other process s in the meantime.

This principle simply formulates the fact that if s leaves a transformed cubicle $x \cdot t$ invariant, i.e. $xt \cdot s = xt$, then the *conjugate* tst^{-1} keeps x invariant: $x \cdot tst^{-1} = x$, see also section A.7 on *cycles and conjugacy* in the appendix. This simple *principle of conjugacy* economizes to remember lots of algorithms – at the cost of *efficiency* and *speed*.

1.5. **Group structure of *Rubik*'s group.** You can skip this section as the results are neither needed nor will they be used in solving *Rubik*'s cube. But they are rather instructive, as they reveal some of the hidden structure of *Rubik*'s group. We assume some familiarity with group concepts.

The group G was defined as the set of all *states* of a *Rubik*'s cube, with *combining moves* as multiplication. Now, it operates naturally on several sets (on the *right*) and can thus be understood as a subgroup of *permutation* groups. G permutes all the 48 faces of the cubies and can thus be realized inside $\mathbf{S}_{48}$. In fact, it permutes the 24 faces of the corners and those of the edges, hence

$$G \subset \mathbf{S}_{24} \times \mathbf{S}_{24} \subset \mathbf{S}_{48}$$

But the 24 corner faces can not be permuted arbitrarily, as always three of them go together sitting in the same cubicle. So the *corner* cycle of each permutation has a *twisting* part and a part $\in \mathbf{S}_8$. Similarly, the *edges* have a *flipping* part and a part $\in \mathbf{S}_{12}$.

Let us consider the larger group that we obtain, when we allow to disassemble the cube and permute the cubies individually. The permutation group we thus obtain will be called W. It is clear that we can – in W – perform any permutation of

corners and any twist per corner, hence the corner permutation part is $\mathbf{F}_3^8 \rtimes \mathbf{S}_8$, the semi-direct product of the twisting group $\mathbf{F}_3^8$ with the symmetric group on 8 corners. For the edges we obtain $\mathbf{F}_2^{12} \rtimes \mathbf{S}_{12}$, hence

$$W = (\mathbf{F}_3^8 \rtimes \mathbf{S}_8) \times (\mathbf{F}_2^{12} \rtimes \mathbf{S}_{12})$$

That the individual factors are *semi-direct* products is not very deep, but will be taken for granted in this paper.

We now have a very decent embedding $G \subset W$ and the question is what is its index $(W : G)$? This has first been determined by Anne Scott who proved

Theorem 1.1. *Let $G \subset W = (\mathbf{F}_3^8 \rtimes \mathbf{S}_8) \times (\mathbf{F}_2^{12} \rtimes \mathbf{S}_{12})$ as above. Then for $s = (u, \sigma, v, \tau) \in W$ we have $s \in G \iff$*

$$\operatorname{sig} \sigma = \operatorname{sig} \tau \tag{1}$$

$$u_1 + u_2 + u_3 + u_4 + u_5 + u_6 + u_7 + u_8 = 0 \tag{2}$$

$$v_1 + v_2 + v_3 + v_4 + v_5 + v_6 + v_7 + v_8 + v_9 + v_{10} + v_{11} + v_{12} = 0 \tag{3}$$

Corollary 1.2.

$$(W : G) = 12$$

$$|W| = 3^8 \cdot 8! \cdot 2^{12} \cdot 12! = 2^{29} \cdot 3^{15} \cdot 5^3 \cdot 7^2 \cdot 11 = 519,024,039,293,878,272,000$$

$$|G| = 3^7 \cdot 8! \cdot 2^{10} \cdot 12! = 2^{27} \cdot 3^{14} \cdot 5^3 \cdot 7^2 \cdot 11 = 43,252,003,274,489,856,000$$

The *derived* group G', generated by all *commutators* $sts^{-1}t^{-1}$, is almost all of G: $(G : G') = 2$. Instead of (1) in the theorem $s \in G'$ if $\operatorname{sig} \sigma = \operatorname{sig} \tau = +1$, hence

$$G' \simeq (\mathbf{F}_3^7 \rtimes \mathbf{A}_8) \times (\mathbf{F}_2^{11} \rtimes \mathbf{A}_{12})$$

where the factors $\mathbf{F}_3^7$ and $\mathbf{F}_2^{11}$ are to be interpreted as the *hyperplanes* defined by (2) resp. (3).

There is a more intrinsic definition of some of these groups [1, 8.3]. Let A_c be the *corner* group which leaves all edges fixed and only permutes the corners. Let A_e be the *edge* group which leaves all corners fixed and only permutes the edges. Then $G' = A_c \times A_e$. Let A_t be the *twisting* group which leaves all cubicles fixed and only twists the corners, it is a normal subgroup of A_c. Let A_f be the *flipping* group which leaves all cubicles fixed and only flips the edges, it is a normal subgroup of A_e.

Then $A_t \simeq \mathbf{F}_3^7$ and $A_c/A_t \simeq \mathbf{A}_8$ and $A_f \simeq \mathbf{F}_2^{11}$ and $A_e/A_f \simeq \mathbf{A}_{12}$.

The element $c \in A_f$ corresponding to the vector $v = (1,1,1,1,1,1,1,1,1,1,1,1)$ lies in the center and is called *superflip*.

In fact the center of G is $C(G) = \{1, c\}$

Proof. Let $c \in C$ be in the center and $c \neq 1$. Let us assume $\exists$ cubicle x with $y = x \cdot c \neq x$. Let $t \in G$ such that $x \cdot t = x$ and $y \cdot t \neq y$. Now $x \cdot t \cdot c = x \cdot c = y$ and $x \cdot c \cdot t = y \cdot t \neq y$, contradicting $t \cdot c = c \cdot t$. Hence c fixes all cubicles, but might twist or flip them. For $c = (u, 1, v, 1) \in W$ in components this means being in the center that for all $t = (u', \sigma, v', \tau) \in G$ $(u', \sigma, v', \tau) \cdot (u, 1, v, 1) = (u' + \sigma(u), \sigma, v' + \tau(v), \tau)$ equals $(u, 1, v, 1) \cdot (u', \sigma, v', \tau) = (u + u', \sigma, v + v', \tau)$, hence $\sigma(u) = u$ and $\tau(v) = v$. In particular we must have $u_1 = u_2 = \cdots = u_8$, $v_1 = v_2 = \cdots = v_{12}$, hence $u = 0$ and $v = (1,1,1,1,1,1,1,1,1,1,1,1)$ is the only non trivial solution. □

2. Resolution methods

2.1. **Strategies.** There are lots of possible strategies. Here I will give a short overview.

One method is to do it layer by layer (lower, middle, upper), sometimes with keeping one column as a shunting yard. *David Singmaster* [1, 7] has proposed such a solution in six steps

(1) The Down-face edge cubies
(2) Three Down-face corner cubies
(3) Three Middle-layer edge cubies
(4) The remaining five edge cubies
(5) Placing the final corners
(6) Untwisting the final corners

A rather different approach using *group theory* was proposed early by *Morwen Thistlethwaite* [8], which searches for least number of necessary turns. *Thislethwaite* steps through the chain of subgroups $G = G_0 \supset G_1 \supset G_2 \supset G_3 \supset 1$ where

$$\begin{aligned} G_0 &= \langle L, R, F, B, U, D\rangle \text{ the whole group} & (G_0 : G_1) &= 2,048 = 2^{11} \\ G_1 &= \langle L, R, F, B, U^2, D^2\rangle & (G_1 : G_2) &= 1,082,565 = 3^9 \cdot 5 \cdot 11 \\ G_2 &= \langle L, R, F^2, B^2, U^2, D^2\rangle & (G_2 : G_3) &= 29,400 = 2^3 \cdot 3 \cdot 5^2 \cdot 7^2 \\ G_3 &= \langle L^2, R^2, F^2, B^2, U^2, D^2\rangle & (G_3 : 1) &= 663,552 = 2^{13} \cdot 3^4 \end{aligned}$$

He proved that at most 52 turns are necessary by this method – with the help of computer algorithms. In 1992 this method was refined by German mathematician *Herbert Kociemba* [4] using the shorter group chain $G_0 \supset G_2 \supset 1$ and a two-phase algorithm $G_0 \to G_0/G_2$ and $G_2 \to 1$.

In January 1995 *Dik Winter* posted the following sequence for *superflip* in 20 moves

$$FBU^2RF^2R^2B^2U^{-1}DFU^2R^{-1}L^{-1}UB^2DR^2UB^2U$$

and a week later *Michael Reid* showed that *superflip* requires 20 moves. In July 2010 it has been proven [6] that at most 20 moves are sufficient for any $s \in G$, i.e. with 20 moves you can always fix a cube. The calculations have been performed during idle time on lots of computers donated by Google, equivalent to 35 CPU-years.

Famous speed cubemeisters, as *Jessica Fridrich* [2] or *Lars Petrus* [5], again pursue completely different strategies and do not use group theory. *Petrus* does not fix by *layer* or *corners first*. As *Petrus* puts it

> The basic problem with the layer method is a big one, and it's obvious once you realize it. When you have completed the first layer, you can do nothing without breaking it up. So you break it, do something useful, then restore it. Break it, do something, restore it. Again and again. In a good solution you do something useful all the time. The first layer is in the way of the solution, not a part of it!

Fridrich's method goes by layer, though, and she uses a large number $(120 - 150)$ of algorithms, that she knows by heart! Both perform very fast (less than 20 seconds). The world record in *speed cubing* is 4.59 seconds, achieved by South-Korean *SeungBeom Cho* at ChicaGhosts 2017 in Chicago.

2.2. **My approach: corner's first.** My strategy is neither fast nor efficient. But I can easily remember what has to be done and it still appears clear and simple to me.

I separately deal with corners and edges, doing corners first. This way only *two* simple operations – *swap* S and *twist* T – need to be performed for the corners until they are fixed. These operations mix up the edges – see table 1 for details – I don't care.

After having fixed all corners, I care about the edges, two pairs of them at a time, with only *one* operation X, which leaves corners invariant. I use only this one operation, because the *principle of conjugacy* guarantees that I can swap any other two pairs of edges as well. I do a *preparatory* move P to put the pairs of edges into position for X, do the edge swap X and thereafter restore everything else back with P^{-1}. When a preparatory process is too complicated for me to remember during my performance of PXP^{-1}, I write P down before executing X, so that I recall how to perform its inverse P^{-1}.

That is all to it. In summary:

(1) Corner cubies are placed into their home cubicles, not worrying about the orientation of the corners, with *corner swap* S
(2) Corners are *untwisted* with $T \cdot U \cdot T^{-1} \cdot U^{-1}$, $T \cdot U^2 \cdot T^{-1} \cdot U^2$ etc ...
(3) *Swap edges* with X and conjugates $P \cdot X \cdot P^{-1}$ into their home locations

Name	Operator	Cycle
corner swap S	$FRUR'U'F'$	$(urf\ ufl)^+(ubr\ ulb)^-(uf\ ru\ bu)$
corner twist T	$F'DFLDL'$	$(ufl)^+(dlf)^+(dfr\ drb\ dbl)^+(fl\ bd\ ld\ df\ dr)$
inverse twist T'	$LD'L'F'D'F$	$(ufl)^-(dlf)^-(dbl\ drb\ dfr)^-(dr\ df\ ld\ bd\ fl)$
	$TUT'U'$	$(ufl)^+(urf)^-$
	$TU^2T'U^2$	$(ufl)^+(ubr)^-$
edge swap X	$R^2L^2U^2R^2L^2D^2$	$(uf\ ub)(df\ db)$

TABLE 1. List of Operators

On occasion I make use of

$$(R^2 \cdot F^2)^3 = (uf\ df)(ur\ dr) \tag{4}$$

$$B^{-1}UFU^{-1}BU^2F^{-1}UFU^2F^{-1} = (ufl\ urf)(uf\ ul) \tag{5}$$

$$R^2F^2R^2F^2RU^{-1}R^2UFRUF^2U^{-1}F = (uf)^+ \cdot (ur)^+ \tag{6}$$

(5) is due to *Thistlethwaite*. It is a representative of the non-trivial class in G/G'. (6) is a *flip-flop*, profitably used when the edges are already in their homes, but flipped around.

APPENDIX A. BASIC CONCEPTS IN GROUP THEORY

A.1. **Groups.** A *group* G is a set of objects with a precept to compose any two objects to give another: if $s, t \in G$ are two elements, there is a well defined element, their *composition* (or *product*) $s \cdot t \in G$, satisfying the following rules

(1) for $s, t, u \in G$ we have $(s \cdot t) \cdot u = s \cdot (t \cdot u)$
(2) there is a *neutral* element $e \in G$ such that $e \cdot s = s$ for all $s \in G$
(3) to each $s \in G$ there is an $s' \in G$ giving $s' \cdot s = e$

The first rule (1) ensures that the sequence of multiplications is not important; but you have to keep the order of the factors, as in general the elements do not *commutate*: $s \cdot t = t \cdot s$ may not be valid. The element $e \in G$ of rule (2) is uniquely determined, as is the element s' in (3) for each s. This is also called the *inverse* of s and written $s' = s^{-1}$.

A *subgroup* H of a group G is a subset $H \subset G$ such that for $s, t \in H$ we also have $s \cdot t, s^{-1} \in H$. If $t \in G$ is any element and $H \subset G$ is a subgroup then the set $tHt^{-1} = \{tst^{-1} \mid s \in H\}$ is a subgroup, called *conjugate* to H.

Groups are called *abelian*[1], when the commutation rule $s \cdot t = t \cdot s$ always holds. In this case the composition often is written additively as $s + t$ and called *sum*; the neutral element is denoted by 0.

A.2. **Permutation groups.** Let X be a set and p a mapping $p : X \to X$. We have a natural *composition* of mappings $p, q : X \to X$ given by the composition map $p \cdot q : X \to X$ with $p \cdot q(x) = p(q(x))$ for all $x \in X$. The obvious neutral element is the *identity* map $i : X \to X$ given by $i(x) = x$ mapping each element to itself, as $p \cdot i = i \cdot p = p$. For a set G of maps $X \to X$ to constitute a *group* we need to have *inverse* maps p' such that $p' \cdot p = p \cdot p' = i$. This implies that the map p has to be *bijective*, i.e. both

- *injective:* whenever $p(x) = p(y)$, then $x = y$
- *surjective:* for each $x \in X$ there is an u with $p(u) = x$

If the set X is *finite* then the set $\mathbf{S}_X$ of all bijective maps is a finite group, which is called the *symmetric* group. Its elements are called *permutations* as they permute all the elements of X. The particular permutation group of the integer interval $I_n = \{1, 2, \ldots, n\} = [1, n] \cap \mathbf{Z}$ is written $\mathbf{S}_n$. For the order of $\mathbf{S}_n$ see section A.6.

The *sign* of a permutation $s \in \mathbf{S}_n$ is the number

$$\operatorname{sig} s = \prod_{1 \le i < j \le n} \frac{s(j) - s(i)}{j - i}$$

Its value is either $+1$ or -1 and the relation $\operatorname{sig}(s \cdot t) = \operatorname{sig} s \cdot \operatorname{sig} t$ holds for any $s, t \in \mathbf{S}_n$. A permutation with $\operatorname{sig} s = +1$ is called *even*, those with $\operatorname{sig} s = -1$ are called *odd*. The even permutations build the *alternate* group $\mathbf{A}_n \subset \mathbf{S}_n$.

A.3. **Operation of groups.** An *operation* of a group G on X is a map

$$G \times X \longrightarrow X$$
$$(s, x) \longmapsto s \cdot x$$

satisfying the two properties

(1) for all $s, t \in G$ and $x \in X$, we have $s \cdot (t \cdot x) = st \cdot x$
(2) if $e \in G$ is the unit element then $e \cdot x = x$ for all $x \in X$

Given an operation we define for each $s \in G$ a permutation by

$$p_s : X \longrightarrow X$$
$$p_s(x) = s \cdot x$$

Then $p_s \cdot p_t(x) = p_s(p_t(x)) = s \cdot (t \cdot x) = st \cdot x = p_{st}(x)$, hence $p_s \cdot p_t = p_{st}$. You see that $p_e = i$ is the identity by (2). The set of all p_s for $s \in G$ defines a permutation subgroup $P \subset \mathbf{S}_X$.

[1] after *Niels Henrik Abel*, 1802 – 1829

There is a similar concept of a group G operating on X on the *right*

$$X \times G \longrightarrow X$$
$$(x, s) \longmapsto x \cdot s$$

satisfying $(x \cdot s) \cdot t = x \cdot st$ and $x \cdot e = x$. This will prove to be convenient when discussing the *magic cube*.

A.4. **Orbits.** Let G operate on X on the *right*. Any subgroup $H \subset G$ of G operates on X as well.

For an $x \in X$, the set of $x \cdot s$ for all $s \in G$ is called the *orbit* of x under G and denoted $xG = \{x \cdot s \mid s \in G\} \subset X$.

Orbits are either *disjoint* or equal: if $xG \cap yG \neq \varnothing$ then $xG = yG$.

Proof. Let $z \in xG \cap yG$, say $z = x \cdot s = y \cdot t$, then by applying the operator t^{-1} we obtain $y = x \cdot st^{-1}$ and $yG = x \cdot st^{-1}G = xG$. □

The set of these orbits is denoted X/G. If G operates on the *left* it is denoted $G\backslash X$ and the individual orbits are written Gx.

We can interpret the group composition $G \times G \to G$ as *both* an operation of the group G on the set G on the *left* and on the *right*. By this interpretation we have for any subgroup $H \subset G$ the set of orbits $G/H = \{xH \mid x \in G\}$ of so called *left cosets* and $H\backslash G = \{Hx \mid x \in G\}$ of *right cosets* of H.

Another concept is the *isotropy* group $G_x = \{s \in G \mid x \cdot s = x\}$ of an element $x \in X$. If s and t leave x invariant $x \cdot s = x, x \cdot t = x$, so does their product $x \cdot st = x$ and the inverse $x \cdot s^{-1} = x$. For any $t \in G$ we have $G_{x \cdot t} = t^{-1}G_x t$, the isotropy groups along an orbit are all conjugate to each other.

Let $\pi_x : G \to xG$ be the *orbit* map $\pi_x(s) = x \cdot s$. If $\pi_x(s) = \pi_x(t)$ this means $x \cdot s = x \cdot t$ or $x \cdot st^{-1} = x$, that is $st^{-1} \in G_x$, hence $G_x s = G_x t$ and the fibers of π_x are exactly the right cosets. We conclude that $G_x\backslash G \simeq xG$ is a bijection.

A.5. **Orders and periods.** The number[2] of elements of X will be denoted $|X|$. The number $|G|$ is called the *order* of the group (if it is finite). Let $s \in G$ and $e_s : \mathbf{Z} \to G$ be the *exponential* map $e_s(n) = s^n$. The set of $n \in \mathbf{Z}$ such that $s^n = e$ is a subgroup, hence of the form $d\mathbf{Z}, d \geq 0$. The subgroup $e_s(\mathbf{Z}) = s^{\mathbf{Z}} \subset G$ is the *cyclic* group generated by s. If $d = 0$ then this cyclic group is infinite and has the same structure as $\mathbf{Z}$. If $d > 0$ then this group is finite $\{e, s, s^2, \ldots, s^{d-1}\}$ of order d with the same structure as $\mathbf{Z}/d\mathbf{Z}$, $s^d = e$ and d is called the *period* of s.

Let G be a finite group. For a subgroup $H \subset G$ the number of cosets $|G/H|$ is called the *index* $(G : H)$ of H in G. We remark that the index is also the number of *right* cosets $|G/H| = |H\backslash G|$ as taking the inverse gives a bijection

$$H\backslash G \longrightarrow G/H$$
$$Hs \longmapsto s^{-1}H$$

Each coset $C = sH$ has the same number of elements as H: $|C| = |sH| = |H|$. We can write the set G as union over all (disjoint) cosets $C = sH$

$$G = \bigcup_{C \in G/H} C$$

[2] we will use this only for *finite* sets

and get $|G| = \sum_{C\in G/H} |C| = (G : H) \cdot |H|$. In particular, the order of H *divides* the order of G, and applied to the cyclic group $H = s^{\mathbf{Z}}$ we see the period of any element s is a divisor of $|G|$.

A.6. **Order of $\mathbf{S}_n$.** We want to show that $|\mathbf{S}_n| = n! = 1 \cdot 2 \cdots n$. We have $|\mathbf{S}_1| = 1$, so let $n > 1$ and we will use induction.

Let $G = \mathbf{S}_n$ operate on $X = I_n = \{1, 2, \dots, n\}$ and pick $x = n$. We first determine the isotropy group G_x.

$s \in G_x$ says that $s(n) = n$, which implies that s permutes the elements in I_{n-1}, hence $s|I_{n-1} \in \mathbf{S}_{n-1}$. On the other side every $t \in \mathbf{S}_{n-1}$ can be uniquely extended to I_n by setting $t(n) = n$. This defines a bijective map $G_x \xrightarrow{\sim} \mathbf{S}_{n-1}$, hence $|G_x| = |\mathbf{S}_{n-1}| = (n-1)!$ by induction assumption.

Finally, the orbit of $x = n$ under $G = \mathbf{S}_n$ is $Gx = I_n$, hence $n = |Gx| = (G : G_x)$ and $|G| = (G : G_x) \cdot |G_x| = n \cdot (n-1)! = n!$.

A.7. **Cycles and conjugacy.** Let a *finite* group G operate on X on the *left*, let $s \in G$, $x \in X$ and let us inspect the orbit Hx of the cyclic group $H = s^{\mathbf{Z}}$.

Since s has a finite period, there is a smallest $l > 0$ such that $s^l \cdot x = x$ and the orbit has exactly l elements $Hx = \{x, s \cdot x, s^2 \cdot x, \dots, s^{l-1} \cdot x\}$, with $l = 1$ exactly when $s \in G_x$. If we choose another element of the orbit $y \in Hx$, the sequence in $Hy = \{y, s \cdot y, s^2 \cdot y, \dots, s^{l-1} \cdot y\}$ would be the same, but shifted by k elements for $y = s^k \cdot x$.

An ordered sequence $a_1, \dots, a_l$ with $Hx = \{a_1, \dots, a_l\}$ and $s \cdot a_i = a_{i+1}$, $i = 1, \dots, l$, $a_{l+1} = a_1$, is called a *cycle* and written in *cycle notation* as $(a_1\ a_2\ \dots\ a_l)$.

As X is the disjoint union of the orbits in $H\backslash X$ the operation of s is completely given by the cycle notation of each orbit: $s = (a_1\ a_2\ \dots\ a_l)(b_1\ \dots\ b_k)(\dots)$. In this convention 1-element orbits are usually suppressed in the notation.

For $t \in G$ the cyclic group generated by the *conjugate* element tst^{-1} is the *conjugate* group tHt^{-1}. If $(a_1\ a_2\ \dots\ a_l)$ is a cycle of s, corresponding to the orbit of x, then $(t \cdot a_1\ t \cdot a_2\ \dots\ t \cdot a_l)$ is a cycle of tst^{-1} for the orbit of $t \cdot x$, as $tHt^{-1} \cdot tx = t \cdot Hx = \{t \cdot a_1, \dots, t \cdot a_l\}$.

For an operation on the *right* and a cycle $(a_1\ a_2\ \dots\ a_l)$ for the orbit xH, the cycle for the orbit of $x \cdot t^{-1}$ under the conjugate group tHt^{-1} is $(a_1 \cdot t^{-1}\ \dots\ a_l \cdot t^{-1})$, since $xt^{-1} \cdot tHt^{-1} = xH \cdot t^{-1} = \{a_1 \cdot t^{-1}, \dots, a_l \cdot t^{-1}\}$.

References

[1] Alexander H. Frey and David Singmaster, *Handbook of Cubik Math*, Enslow Publishers, 1982. republished in 2010 by The Lutterworth Press.

[2] Jessica Fridrich, *My speed cubing page*, available at http://ws.binghamton.edu/fridrich/cube.html.

[3] Douglas R. Hofstadter, *Metamagical Themas*, Scientific American **244** (1981), no. 3, 14–26.

[4] Herbert Kociemba, *The Two-Phase-Algorithm*, http://kociemba.org/twophase.htm. Accessed December 27, 2015.

[5] Lars Petrus, *Solving Rubik's Cube for speed*, http://lar5.com/cube/index.html. Accessed February 6, 2016.

[6] Tomas Rokicki, Herbert Kociemba, Morley Davidson, and John Dethridge, *God's number is 20* (2010), http://www.cube20.org/. Accessed December 22, 2015.

[7] David Singmaster, *Notes on Rubik's Magic Cube*, Enslow Publishers, 1980, out of print.

[8] Morwen Thistlethwaite, *The 52 Move Strategy* (1981), http://www.jaapsch.net/puzzles/thistle.htm. Accessed December 27, 2015.