University *of Ljubljana*
Faculty *of Mathematics and Physics*

DISCRETE MATHEMATICS 2

ANTONIO MONTERO

Office 5.17
FMF - University of Ljubljana

1. Permutation groups

Informally speaking, a permutation of a collection of objects is just a way of (linearly) order the objects. Permutations are often thought either as purely combinatorial objects, usually in counting problems, or as one of the first examples in a first class of group theory. In these first sections we will look at the interplay between these two approaches. We will use permutations to understand combinatorial problems and the other way around, we will use counting techniques to understand group theoretical properties of permutations. In this section we first review some basic properties of permutations.

Let X be a set, a *permutation* of X is a bijection $\sigma : X \to X$. Observe that the *identity* $\varepsilon_X : X \to X$, defined by $\varepsilon_X(x) = x$ for every $x \in X$, is a permutation (if there is no ambiguity we often write ε instead of ε_X). Moreover, if σ and τ are permutations of X, then so σ^{-1} and $\tau \circ \sigma$ are. That implies that the set of permutations of X, denoted S_X, is a group with the composition as operation. This group is called the *symmetric group on* X. We usually omit the symbol $\circ$ and simply write $\tau\sigma$.

In this course we will mostly work with finite sets. If $|X| = n$ we will think of X either as the set $[n] := \{1, \dots, n\}$ or as the set $\mathbb{Z}_n$ of integers modulo n, as convenient. In either situation we write S_n instead of S_X (see Exercise 1.1).

If $\sigma \in S_n$, then it is convenient (particularly for small values of n) to represent σ with a $2 \times n$ matrix where the entries of the first row are the elements of $[n]$ and we write $\sigma(x)$ below every element x. For example the equation

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 4 & 2 \end{bmatrix}$$

E-mail address: antonio.montero@fmf.uni-lj.si.

means that σ is such that $\sigma(1) = 3$, $\sigma(2) = 1$, $\sigma(3) = 5$, $\sigma(4) = 4$ and $\sigma(5) = 2$. Observe that this representation is not unique, the following matrices also represent the permutation σ described above.

$$\sigma = \begin{bmatrix} 3 & 1 & 2 & 5 & 4 \\ 5 & 3 & 1 & 2 & 4 \end{bmatrix} = \begin{bmatrix} 5 & 4 & 3 & 2 & 1 \\ 2 & 4 & 5 & 1 & 3 \end{bmatrix}.$$

Matrix representation of permutations allows us to find inverses and operate permutations easily. The inverse of a permutation σ is just the permutation given by swapping the rows of any representation of σ. For the example above:

$$\sigma^{-1} = \begin{bmatrix} 3 & 1 & 5 & 4 & 2 \\ 1 & 2 & 3 & 4 & 5 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 4 & 3 \end{bmatrix}$$

We can find a matrix representation for $\tau\sigma$ by considering the first and third row of a $3 \times n$ matrix M where the first two rows come from a matrix representation of σ and the third one is given by writing $\tau(y)$ below every element y in the second row. For example, if

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 4 & 2 \end{bmatrix}, \quad \tau = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 2 & 5 \end{bmatrix}, \tag{1.1}$$

then

$$M = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 4 & 2 \\ 1 & 4 & 5 & 2 & 3 \end{bmatrix}, \quad \tau\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 5 & 2 & 3 \end{bmatrix}$$

Keep in mid that since we are thinking of permutations as functions, our convention is to evaluate them from right to left, that is $\tau\sigma$ means we apply first σ and then τ. Other authors (notably, those of [1]) use the other convention. Usually the choice of one or another has little to none theoretical implications but one has to be careful when doing explicit computations. For example, observe that for the permutations used above

$$\sigma\tau = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 1 & 2 \end{bmatrix} \neq \tau\sigma.$$

Another common way of represent a permutation is as a product of disjoint cycles. We say that a permutation $\tau \in S_n$ is a *k-cycle* if there are k different elements $x_1, \ldots, x_k \in [n]$ such that $\tau(x_i) = x_{i+1}$ for $1 \leqslant i \leqslant k-1$ and $\tau(x_k) = x_1$ and $\tau(y) = y$ for every other element $y \in X$. In this case we write

$$\tau = (x_1\, x_2\, \cdots x_k)$$

A 2-cycle is called a *transposition*. Notice that there is not a unique way of writing a cycle (see Exercise 1.3)

Example 1.1. The permutation

$$\gamma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{bmatrix}$$

is the 3-cycle (1 2 3). The permutations σ and τ defined in Equation (1.1) can be written as

$$\sigma = (1\,3\,5\,2), \quad \tau = (1\,4\,2\,3).$$

Proposition 1.2. *Every permutation $\sigma \in S_n$ can be written as a product of disjoint cycles. Moreover, this way of writing a permutation is unique up to the order in which the cycles appear and the inclusion or not of* 1*-cycles, which represent fixed points of σ.*

Proof. See Exercises 1.3 to 1.5. □

Proposition 1.2 is also true when we consider permutations of a infinite set X but there might be infinite cycles (see Exercise 1.7) and possibly infinitely many of them. In this case the definition of product is just formal and should be reinterpreted suitably.

If $\gamma = (x_1 \cdots x_k)$ is a cycle, then we can convince ourselves that γ^{-1} is the cycle $(x_x \cdots x_1)$. Recall that if $\gamma_1, \ldots, \gamma_r$ are elements of a group, then $(\gamma_1 \cdots \gamma_r)^{-1} = \gamma_r^{-1} \cdots \gamma_1^{-1}$. These two observations give us a way of finding the inverse of a permutation written as a product of cycles: just write each cycle in reverse order and then write the product of the reversed cycles also in reverse order. The example below should show the idea

$$((2\,4\,5\,7)(1\,3\,6))^{-1} = (1\,3\,6)^{-1}(2\,4\,5\,7)^{-1} = (6\,3\,1)(7\,5\,4\,2)$$

If we have two permutations written as product of cycles we can compute its product is just the permutation given by concatenating the corresponding cycles. Observe that in general, this is not an expression as disjoint cycles, but we can compute one as follows. First, pick a random element and trace its image along the cycles. Keep in mind that we evaluate permutation form right to left. For example, consider the expression (1 2)(4 5)(1 5 3)(2 4) and pick the number 1, by tracking its image along the cycle we see that 1 goes to 4:

$$\underbrace{\overbrace{(1\,2)}^{4\to4}\overbrace{(4\,5)}^{5\to4}\overbrace{(1\,5\,3)}^{1\to5}\overbrace{(2\,4)}^{1\to1}}_{1\to4} = (1\,4\cdots$$

Then we need to track the image of 4, which we see that it is 1 and hence, the first cycle is complete.

$$\underbrace{\overbrace{(1\,2)}^{2\to1}\overbrace{(4\,5)}^{2\to2}\overbrace{(1\,5\,3)}^{2\to2}\overbrace{(2\,4)}^{4\to2}}_{4\to1} = (1\,4)\cdots$$

Now pick another symbol, say 2 and proceed similarly:

$$\overbrace{\underbrace{(1\,2)}_{5\to 5}\underbrace{(4\,5)}_{4\to 5}\underbrace{(1\,5\,3)}_{4\to 4}\underbrace{(2\,4)}_{2\to 4}}^{2\to 5} = (1\,4)(2\,5\cdots$$

If we continue this way, we can see that

$$(1\,2)(4\,5)(1\,5\,3)(2\,4) = (1\,4)(2\,5\,3).$$

Observe that the fact that we omit fixed points when writing a permutation as product of cycles disjoint cycle allow us to abuse notation a do not specify on which set a given permutation acts. For example, the permutation $(2\,3)(4\,7\,5)$ can be regarded as a permutation in S_7, in S_8 or in S_{2022}. In fact, with no further information, this could even be a permutation on the set of natural numbers or even a permutation on the set $\{2, 3, 4, 5, 7\}$. For these reason we should adopt some conventions. We always assume that a permutation act on a set $[n]$ for some $n \in \mathbb{N}$, that is, we shall avoid thinking of a permutation such as $(2\,3)(4\,7\,5)$ acting on a smaller set than $[7]$. Moreover, if $k \leqslant n$ we might regard the group S_k as the subgroup of S_n consisting of the permutations that fix every number m with $k < m \leqslant n$. Unless it is explicitly specified, we should keep symmetric groups on infinite sets out of the game.

If $\sigma = \gamma_1 \cdots \gamma_k$ is a permutation written as a product of disjoint cycles (including 1-cycles), the *cycle-type* of σ is the tuple $[a_1, \ldots, a_k]$ where the number a_i is the length of the cycle γ_k. Observe that if $\sigma \in S_n$, then $a_1 + \cdots + a_k = n$. Of course, we might safely omit the entries with value 1 from the cycle type and say, for example, that the permutation $(2\,3)(3\,7\,5)$ has cycle-type $[2, 3]$.

The following is a straight forward observation:

Proposition 1.3. *Let $\sigma \in S_n$ and assume that σ has cycle type $[a_1, \ldots, a_k]$, then the order of σ is* $\operatorname{lcm}(a_1, \ldots, a_k)$.

Proof. Just observe that if $\sigma = \gamma_1 \cdots \gamma_k$ is written as a product of disjoint cycles then

$$\sigma^r = \gamma_1^r \cdots \gamma_k^r = \varepsilon \Leftrightarrow a_i | r \text{ for all } i \in \{1, \ldots, k\}. \quad \square$$

These first results describe some tools to work with permutations. Now we turn our attention to some group-theoretical properties of permutations.

Two elements σ, τ in a group Γ are *conjugate* if there exists $\mu \in \Gamma$ such that $\sigma = \mu\tau\mu^{-1}$. Observe that this notion defines an equivalence relation in Γ. The equivalence classes are called *conjugacy classes* of Γ.

Proposition 1.4. *Let $n \in \mathbb{N}$ and let σ and τ two permutations in S_n. Then σ and τ are conjugate if and only if σ and τ have the same cycle-type.*

Proof. See Exercise 1.6. $\square$

Definition 1.5. A *permutation group* is a subgroup of a symmetric group.

Let us now show a more group-theoretical property.

Theorem 1.6. *Let $n \in \mathbb{N}$. The group S_n can be generated by the set of transpositions. This is*

$$S_n = \langle (x\ y) : x, y \in [n] \rangle$$

Proof. Just observe that if $(x_1\ \cdots\ x_k)$ is a k-cycle, then

$$(x_1\ \cdots\ x_k) = (x_1\ x_2)(x_2\ x_3)\cdots(x_{k-2}\ x_{k-1})(x_{k-1}\ x_k).$$

□

Theorem 1.6 shows that every permutation can be written as a product of transpositions. However, there is no a unique way of writting a permutation as product of transposition, for example:

$$(2\ 1)(2\ 4)(2\ 3) = (2\ 3\ 4\ 1) = (1\ 2)(2\ 4)(4\ 3)(2\ 4)(4\ 3).$$

As shown in the example above, not even the number of transpositions required is constant. However we shall prove that parity of the number of transpositions depends only on the given permutation and not on a particular way of writing it as a product of transpositions. First we prove the following lemma.

Lemma 1.7. *Let $n \in \mathbb{N}$ and assume that $\gamma_1, \ldots, \gamma_r$ is a family of transpositions such that*

$$\gamma_r \cdots \gamma_1 = \varepsilon.$$

Then r is even.

Proof. We will prove this by induction over r. First observe that $r \geqslant 2$, otherwise we would have $\varepsilon = (x\ y)$ for some pair $\{x, y\} \subseteq [n]$, which is impossible. If $r = 2$ there is nothing to prove. Assume that if $2 \leqslant k < r$ and that $\delta_1, \ldots, \delta_k$ is a family of transpositions with $\delta_k \cdots \delta_1 = \varepsilon$, then k is even. Let $\gamma_1, \ldots, \gamma_r$ be a family of r transpositions that satisfy $\gamma_r \cdots \gamma_1 = \varepsilon$.

Define $\alpha_1 = \gamma_1$ and consider the product $\gamma_2\alpha_1 = \gamma_2\gamma_1$. Observe that there must be 4 elements $x, y, w, z \in [n]$ such that one of the following holds:

$$\gamma_2\alpha_1 = \begin{cases} (x\ y)(x\ y), \\ (x\ z)(x\ y), \\ (w\ z)(x\ y). \end{cases}$$

In the first case, $\gamma_2\alpha_1 = \gamma_2\gamma_1\varepsilon$, which implies that $\gamma_3, \cdots, \gamma_r$ satisfy the inductive hypothesis. In other words, $r - 2$ is even and so it is r,

If $\gamma_2\alpha_1 = (x\ z)(x\ y) = (x\ y\ z) = (x\ y)(y\ z)$. In this case define $\alpha_2 = (x\ y)$ and $\beta_1 = (y\ z)$. If $\gamma_2\gamma_1 = (w\ z)(x\ y) = (x\ y)(w\ z)$ then take $\alpha_2 = (x\ y)$ and $\beta_1 = (w\ z)$. Notice that in any case

$$\varepsilon = \gamma_r \cdots \gamma_2\gamma_1 = \gamma_r \cdots \gamma_3\alpha_2\beta_1.$$

Observe also that α_2 moves x but β_1 does not.

Proceed again but now with the product $\gamma_3\alpha_2$. If $\gamma_3 = \alpha_2$ then we apply the inductive hypothesis to the family $\beta_1, \gamma_4 \cdots, \gamma_{r-1}, \gamma_r$ and we are done. If not, then proceed as before to build a new pair of transpositions α_3, β_2 that satisfy $\gamma_3\alpha_2 = \alpha_3\beta_2$, the permutation α_3 moves x but β_2 does not.

Keep going this way. In the i-th iteration of this process we have constructed $(i-1)$ permutations $\beta_1, \ldots \beta_{i-1}$ such that all of them fix x and a permutation α_i such that α_i moves x. These permutations satisfy that

$$\varepsilon = \gamma_r \cdots \gamma_1 = \gamma_r \cdots \gamma_{i+1}\alpha_i\beta_{i-1} \cdots \beta_1.$$

We have to analyse the possibilities for the product $\gamma_{i+1}\alpha_i$. If $\gamma_{i+1} = \alpha_i$ we apply the inductive hypothesis to the family of transpositions $\beta_1, \ldots, \beta_{i-1}, \gamma_{i+2}, \ldots, \gamma_r$.

If the previous condition is never satisfied after r iterations of the process we have a family of transpositions $\beta_1, \cdots, \beta_{r-1}, \alpha_r$ such that $\beta_i(x) = x$ for every $1 \leqslant i \leqslant r-1$ and $\alpha_r(x) \neq x$. However, these transpositions satisfy that

$$\varepsilon = \gamma_r \cdots \gamma_1 = \alpha_r\beta_{r-1} \cdots \beta_1,$$

which is obviously a contradiction. It follows that at some point $\alpha_i = \gamma_{i+1}$, and by the inductive hypothesis $r-2$ is even and so it is r. □

An immediate consequence of the previous result is the next theorem.

Theorem 1.8. *Let $n \in \mathbb{N}$ and $\sigma \in S_n$. Assume that σ is written as a product of transpositions, say $\sigma = \gamma_r \cdots \gamma_1$. Then the parity of r depends only on σ and not on the particular choice of the transpositions.*

Proof. Assume that

$$\beta_s \cdots \beta_1 = \sigma = \gamma_r \cdots \gamma_1$$

are two ways of writing σ with $\beta_1, \ldots, \beta_s, \gamma_1, \ldots, \gamma_r$ transpositions. Observe that

$$\begin{aligned} \varepsilon &= \left(\beta_s \cdots \beta_1\right)\left(\gamma_r \cdots \gamma_1\right)^{-1} \\ &= \beta_s \cdots \beta_1\gamma_1 \cdots \gamma_r. \end{aligned}$$

Lemma 1.7 implies that $r + s$ is even or equivalently, that r and s have the same parity. □

A permutation σ is called *even* if whenever σ is written as a product of transpositions, then number of transposition is even. Otherwise σ is called *odd*.

The set A_n consisting of all the even permutations in S_n is a subgroup (see Exercise 1.12) of S_n and it is called the *alternating group* on n symbols. Theorem 1.8 allows us to define a group homomorphism $\operatorname{sgn} : S_n \to \{1, -1\}$ where

$$\operatorname{sgn}(\sigma) = (-1)^r$$

whenever σ can be written as a product of r transpositions.

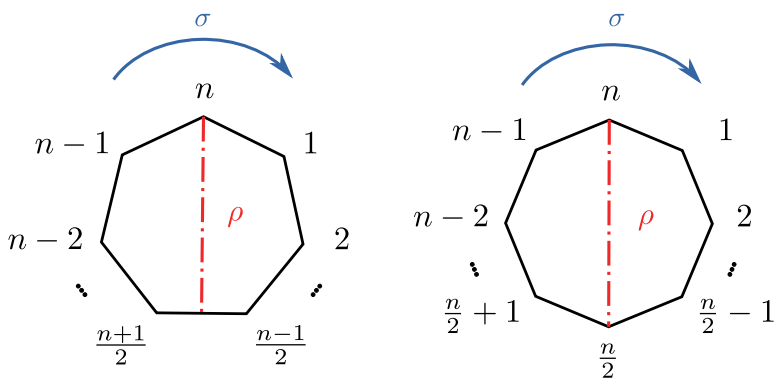


FIGURE 1. The action of D_n

As usuall, two subgroups Γ and Δ of S_n are conjugate if there exists a permutation $\mu \in S_n$ such that

$$\Gamma = \mu\Delta\mu^{-1}\,\{\mu\delta\mu_{-1} : \delta \in \Delta\}$$

There are two important subgroups of S_n that we should introduce now. The *cyclic group* C_n is a group generated by a permutation of order n. Usually we think of C_n as the permutation group generated by the n-cycle $(1\ 2\ \ldots\ n)$ (cf. Exercise 1.16) The *dihedral group* on n symbols D_n is the subgroup of S_n generated by the permutations σ and ρ where

$$\sigma = (1\ \cdots n)$$

$$\rho = \begin{cases} (1 \quad n-1)(2 \quad n-2)\cdots\left(\frac{n}{2}-1 \quad \frac{n}{2}+1\right) & \text{if } n \text{ is even,} \\ (1 \quad n-1)(2\cdots n-2)\cdots\left(\frac{n-1}{2} \quad \frac{n+1}{2}\right) & \text{if } n \text{ is odd.} \end{cases} \tag{1.2}$$

The group D_n can be seen as the permutations of the vertices of a n-cycle that preserve neighbours (see Figure 1)

Example 1.9 (The 15-puzzle[1])**.** The *15-puzzle* consist of a set of squared tiles such that the tiles fit in a box arranged in a 4×4 grid leaving a *blank* space (see Figure 2a). A valid movement of the puzzle is given by sliding one adjacent tile to the blank space or, equivalently, moving the blank space to an adjacent tile.

A position P of the puzzle is *solvable* if the blank space is at the bottom-right corner of the box, and it can be taken to the *solved* position S (Figure 2a) by a sequence of valid movements. Obviously, if we can go from a position P to the position S by a sequence of movements, by applying the same movements in reversed order we can go from S to P, so we can think of the set of solvable position as those that blank space is in the bottom-right corner and can be reached from the position S. Moreover, if P_1 and P_2 are solvable positions then so it is the position P_1P_2, which is defined as the position given by applying a sequence of

[1]Pictures and historical notes were taken from Wikipedia

movements that take S to P_2 to the position P_1. Observe that this is only possible because P_1 has the blank space at the bottom-right corner. By definition, we can take S to P_1P_2 and since P_2 also has the blank space at the bottom-right corner, then P_1P_2 has the blank space at the bottom-right cornet. It follows that if P_1 and P_2 are solvable position, then so it is P_1P_2.

If you want to play, you can do it here[2].

The 15-puzzle is often associated with the puzzle inventor and problem composer Sam Loyd (1841-1911), who claimed his entire life that he had invented the puzzle. Loyd should be credited with the original challenge: to take the puzzle from the position in Figure 2b to the solved position. It is believe that Loyd offered a prize of $1,000 USD to that who could solve the problem. In 1879 Johnson and Story proved that this was in fact impossible. We will prove a slightly more general result.

First, observe that we can associate a permutation σ to any position of the puzzle. We can label the spaces of the grid at the bottom of the box, as in Figure 2c.

A given position of the puzzle can be associated with the permutation $\sigma \in S_{16}$ defined by

$$\sigma(x) = y \Leftrightarrow \text{ the tile } x \text{ is over the space } y.$$

Here the blank space is thought as a tile with number 16.

For example the position in Figure 2d is given by the permutation

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 3 & 2 & 13 & 9 & 6 & 7 & 12 & 5 & 10 & 11 & 8 & 4 & 15 & 14 & 1 & 16 \end{bmatrix}$$

Of course, we can also write

$$\sigma = (1\,3\,13\,15)(4\,9\,10\,11\,8\,5\,6\,7\,12)(14)(16).$$

A valid move in the puzzle consists in swapping the blank space with an adjacent tile. Assume that P_1 is the position associated to the permutation σ and let P_2 the position resulting from P_1 after applying a valid movement. An natural question is: can we obtain the permutation τ associated to P_2 in terms of σ. The answer is yes, we claim that

$$\tau = \sigma(16\ y),$$

where y is the tile that we swap with the blank space.

To see, this observe that any tile that is not 16 or the one on the space y in P_1 remains in the same place. In other words, if $x \notin \{16, y\}$, then

$$\tau(x) = \sigma(x) = \sigma(16\ y)(x).$$

In P_2, the blank space is where the tile y used to be in P_1, that is $\tau(16) = \sigma(y)$. Meanwhile, in P_2 the tile y is in the space where 16 used to be in P_1, that is $\tau(y) = \sigma(16)$. This proves that τ and $\sigma(16\ y)$ are exactly the same permutation.

[2]Applet obtained from ©Jamie Mulholand's website (SFU Math)

In our example, let us slide the tile with 7 to de blank space. Our claim is that we obtain the permutation $\tau = \sigma(16\,7)$. In fact, this is obvious if we look at the matrix representation of $(16\,7)$, which is

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 1 & 2 & 3 & 4 & 5 & 6 & 16 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 7 \end{bmatrix},$$

and the matrix representation of σ:

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 3 & 2 & 13 & 9 & 6 & 7 & 12 & 5 & 10 & 11 & 8 & 4 & 15 & 14 & 1 & 16 \end{bmatrix}$$
$$= \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 16 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 7 \\ 3 & 2 & 13 & 9 & 6 & 7 & 16 & 5 & 10 & 11 & 8 & 4 & 15 & 14 & 1 & 12 \end{bmatrix}.$$

It follows that

$$\sigma(16\,7) = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 3 & 2 & 13 & 9 & 6 & 7 & 16 & 5 & 10 & 11 & 8 & 4 & 15 & 14 & 1 & 12 \end{bmatrix}.$$

Claim. *If σ is a permutation associated to a solvable position of the 15-puzzle, then*

(a) σ fixes 16.
(b) $\sigma \in A_{16}$, that is, σ is an even permutation.

Proof. The first condition is obvious, since it is equivalent to the fact that the blank tile is on the space 16, which was part of the definition of a solvable position. To see that the second condition must hold, just consider a checkboard colouring of the bottom of the box. Observe that every movement changes the color below the blank space. Since the blank space starts and ends over the space labelled with 16, we need an even number of movements. By our analysis above, this is equivalent to the associated permutation being a product of an even number of transpositions. □

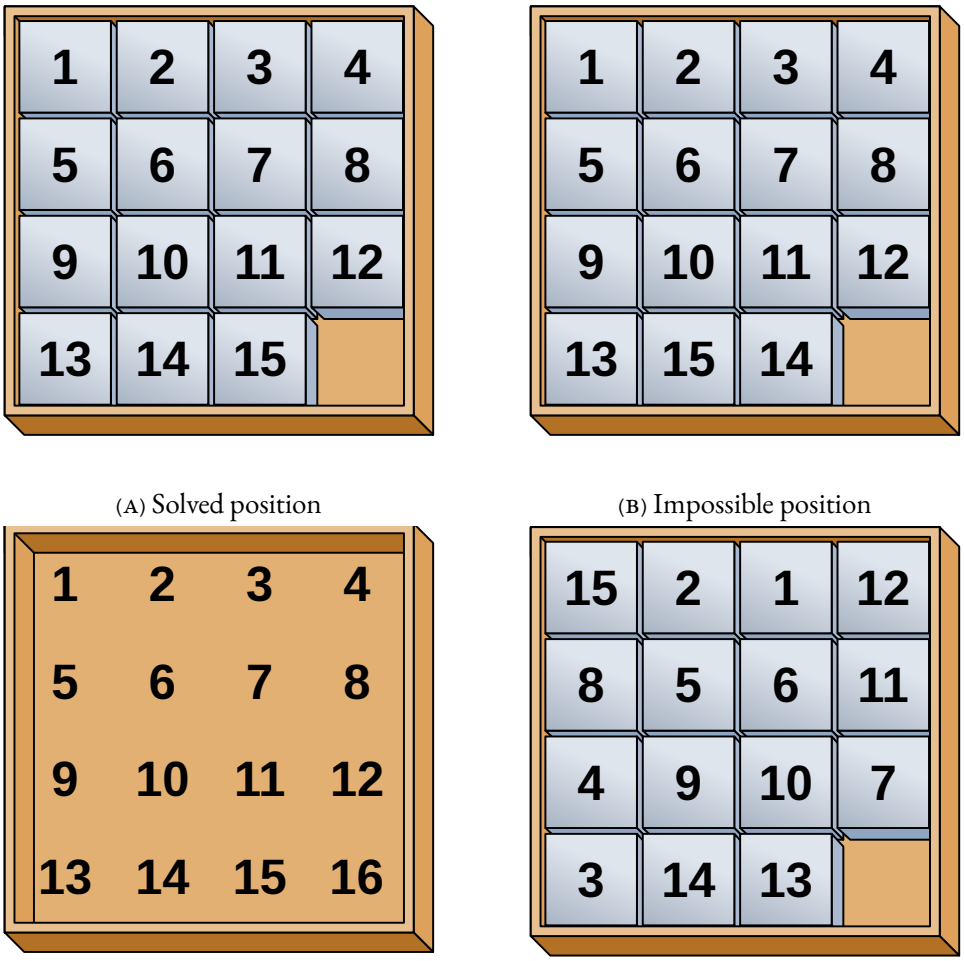
Corollary. *It is impossible to solve the 15-puzzle from the position in Figure 2b.*

We will prove that the conditions in our previous claim are not only necessary but also sufficient. More precisely:

Proposition 1.10. *If $\sigma \in A_{16}$ is a permutation such that $\sigma(16) = 16$, then the associated position of the 15-puzzle is solvable. In particular, there are exactly $\frac{15!}{2}$ solvable positions of the this puzzle.*

Before proving this proposition observe that

Remark 1.11. The set of permutation associated with solvable positions of the 15-puzzle is a subgroup of the symmetric group S_{15}.



(A) Solved position

(B) Impossible position

(C) Empty box of 15 puzzle

(D) An arbitrary position.

FIGURE 2. The 15-puzzle

Proof. The trivial permutation is associated to the solved position.

Let σ and τ be the permutation associated to the (solvable positions P_σ and P_τ, respectively. Let $P = P_\sigma P_\tau$, that is, the position obtained after applying to P_σ the same sequence of movements that takes the solved position to P_τ. We claim that the permutation associated with P is precisely $\tau\sigma$. To see this just observe that a given tile x is on the space $\sigma(x)$ in P_σ. If we ignore the numbers on the tiles and apply a sequence of movements that takes the solved position to P_τ to any position (whenever this is possible) the tile on the space y will end up in on $\tau(y)$. In particular, for P_σ that means that the tile x is at $\tau(\sigma(x)) = \tau\sigma(x)$ in the position P.

A very similar argument can be used to prove that if σ is associated with P_σ then the sequence of movements that takes P_σ to S takes S to $P_{\sigma^{-1}}$, the position associated with σ^{-1}.

Finally observe that all the permutation associated to solvable positions fix the tile 16, hence the associated subgroup is not only a subgroup of S_{16}, but a subgroup of S_{15}. □

Proof (of Proposition 1.10). We will show that the group G associated to the set of solvable position is in fact the alternating group A_{15}. First, observe that by moving the blank tile to the following spaces

$$16 \longrightarrow 12 \longrightarrow 11 \longrightarrow 15 \longrightarrow 16$$

We end up with the position associated to the 3-cycle $\gamma = (11\ 12\ 15)$ (see Figure 3a). This proves that $\gamma \in G$. From the solved position move the tiles 12 and 11 (in that order) so that the resulting position is as shown in Figure 3b. Consider the drawn by the arrows in Figure 3c. For every $x \in [15] \setminus \{11, 12\}$ we can move the blank space along that cycle as many time as needed so that x ends on the space 15 and the blank tile on the space 11. For example, if $x = 7$, after moving the blank tile along the cycle once, we obtain the position in Figure 3d. Then we can move the tiles 11 and 12 to its original position.

Notice the final position is a solvable one: it was constructed by a sequence of valid movements and the blank tile is at the bottom-right corner. It follows that the induced permutation $\mu_x \in G$. Observe that μ_x satisfies that

$$\begin{aligned} \mu_x(x) &= 15 \\ \mu_x(11) &= 11 \\ \mu_x(12) &= 12. \end{aligned}$$

The latter imply that $\mu^{-1}\gamma\mu = (11\,12\,x)$. It follows that $(11\,12\,x) \in G$ and since we have proved that $G \leqslant A_{15}$, Exercise 1.14 implies that G is indeed A_{15} □

Exercises.

1.1 Show that if X and Y are (not necessarily finite) sets with $|X| = |Y|$, then $S_X \cong S_Y$.

1.2 Let X be a set.
- (a) If $|X| = n$, how many elements does the set S_X have?
- (b) Let X be a countably infinite set, that is, $|X| = |\mathbb{N}|$. Prove that $|S_X| \gneq |\mathbb{N}|$ (that is, strictly greater than $|\mathbb{N}|$). Can you determine $|S_X|$?

1.3 Prove that a k-cycle $\sigma = (x_1 \cdots x_k)$ and an ℓ-cycle $\tau = (y_1 \cdots y_\ell)$, both elements of S_n, are equal if and only if $k = \ell$ and for some $h \in \mathbb{Z}$, $x_{i+h} = y_i$ or every $1 \leqslant i \leqslant r$ (the indices are taken modulo r).

1.4 Prove that every permutation σ can be written as a product of disjoint cycles. **Hint:** two symbols $x, y \in X$ lie in the same cycle of σ if some

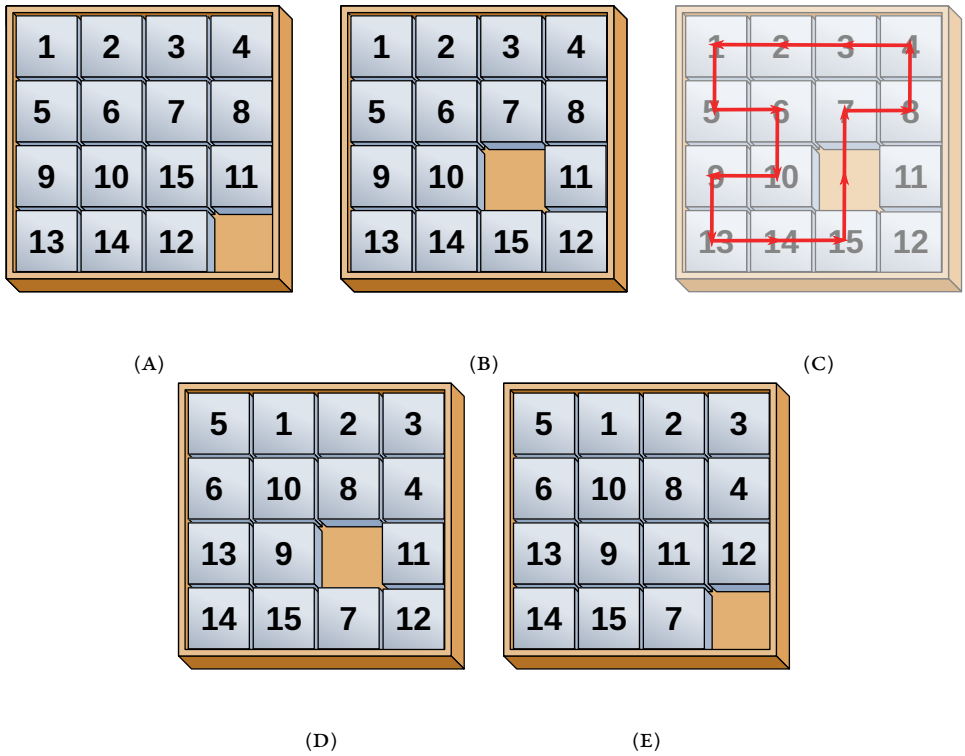


FIGURE 3

power of σ maps x to y. Prove that this condition defines an equivalence relation and hence a partition of X.

1.5 Prove that disjoint cycles commute.

1.6 Let $n \in \mathbb{N}$.

(a) Prove that if $\sigma = (x_1 \cdots x_k)$ is a k-cycle and $\mu \in S_n$ then $\mu\sigma\mu^{-1} = \big(\mu(x_1) \cdots \mu(x_k)\big)$.

(b) Show that for every $k \leqslant n$ every two k-cycles are conjugate.

(c) Conclude that two permutations in S_n are conjugate if and only if they have the same cycle-type.

1.7 Let X be a infinite set. An *infinite cycle* in S_X is a permutation γ such that there exists a family $Z = \{x_i : i \in \mathbb{Z}\}$ of elements of X with $\gamma(x_i) = x_{i+1}$ for every $i \in \mathbb{Z}$ and $\gamma(y) = y$ for every $y \in X \setminus Z$. Find two infinite cycles in $S_{\mathbb{Z}}$ that are not conjugate.

1.8 Let $n \in \mathbb{N}$. Show that the set of involutions $I = \{(1\,k) : 2 \leqslant k \leqslant n\}$ is a minimal generating set of S_n. That is, show that

$$S_n = \langle (1\,k) : 2 \leqslant k \leqslant n \rangle,$$

and that no proper subset of I generates S_n.

1.9 Let $n \in \mathbb{N}$. Show that The involution $(1\ n)$ and the n-cycle $(1\ 2\ \cdots\ n)$ generate S_n.

1.10 Let $n \in \mathbb{N}$, find necessary and sufficient conditions for $i, j \in [n]$ so that

$$\langle (i\ j), (1\ 2 \cdots\ n) \rangle = S_n$$

1.11 Show that the group $S_{\mathbb{N}}$ cannot be generated by a finite number of permutations.

1.12 Prove that the set A_n is a subgroup of S_n.

1.13 Prove that an r-cycle in S_n is even if and only if r is odd. Conclude that a permutation σ is even if and only if the number of even entries in its cycle-type is even.

1.14 Let $n \geqslant 3$ and let A_n denote the alternating group.

- Show that
$$A_n = \left\langle (x\ y\ z) : x, y, z \in [n] \right\rangle.$$
- Show that
$$A_n = \langle (1\ 2\ z) : z \in [n] \rangle.$$
- Show that if x and y are fixed elements in $[n]$ then
$$A_n = \left\langle (x\ y\ z) : z \in [n] \right\rangle.$$

1.15 Prove that if Γ is a permutation group, then either Γ consists of only even permutations or half of the permutations in Γ are even. Conclude that A_n is normal in S_n and that every permutation group that contains an odd permutation has a normal subgroup of index 2.

1.16 Show that if n is prime, then any two cyclic of order n in S_n are conjugate. Find two cyclic groups of order 6 in S_6 that are not conjugate.

1.17 Let $n \in \mathbb{N}$ and $D_n = \langle \rho, \sigma \rangle$ the dihedral group defined in Equation (1.2).

(a) Show that these permutations satisfy the following relations:

$$\rho^2 = \varepsilon$$
$$\sigma^n = \varepsilon$$
$$\rho\sigma\rho = \sigma^{-1}$$

(b) Define $\tau = \sigma\rho$. Show that the relations above are quivalent to

$$\tau^2 = \rho^2 = (\tau\rho)^n = \varepsilon$$

We will prove later that any group generated by two involutions is isomorphic to a dihedral group.

1.18 Prove that $|D_n| = 2n$. **Hint:** work the cases where n is even and n is odd separately.

1.19 Find the conjugacy clases of the symmetric group S_5 and of the alternating group A_5. Hence, show that A_5 is the only normal subgroup of S_5 (apart from 1 and S_5, and that A_5 is simple.)

1.20 If $H \leqslant G$ are groups, the *normaliser of H in G* is the largest subgroup of G in which H is normal. Find the nomaliser in S_n of the cyclic group $C_n = \langle (1\,2 \ldots\ n) \rangle$.

References.

[1] Mark A. Armstrong. *Groups and Symmetry*. en. Undergraduate Texts in Mathematics. New York: Springer-Verlag, 1988. ISBN: 9780387966755. DOI: 10.1007/978-1-4757-4034-9. URL: https://www.springer.com/gp/book/9780387966755 (visited on 08/16/2021).

[2] Norman L. Biggs and A. T. White. *Permutation Groups and Combinatorial Structures*. Cambridge University Press, Aug. 1979. DOI: 10.1017/cbo9780511600739.

[3] Peter J. Cameron. *Permutation Groups*. Cambridge University Press, Feb. 1999. DOI: 10.1017/cbo9780511623677.

[4] John D. Dixon and Brian Mortimer. *Permutation groups*. Vol. 163. Graduate Texts in Mathematics. Springer-Verlag, New York, 1996, pp. xii+346. ISBN: 0-387-94599-7. DOI: 10.1007/978-1-4612-0731-3. URL: http://dx.doi.org/10.1007/978-1-4612-0731-3.