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 [DM96]) 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:

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

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

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

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.

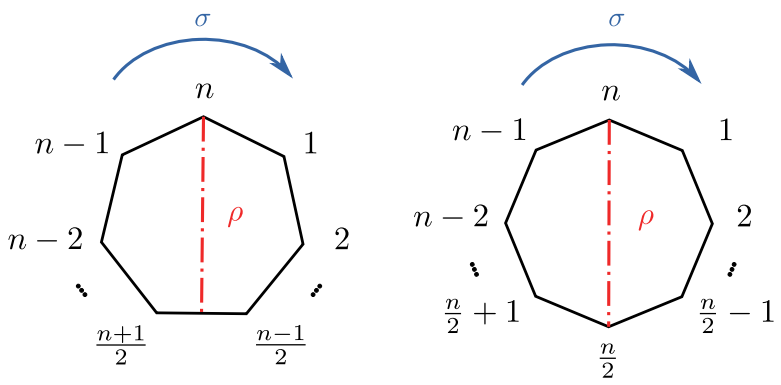


FIGURE 1. The action of D_n

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. □

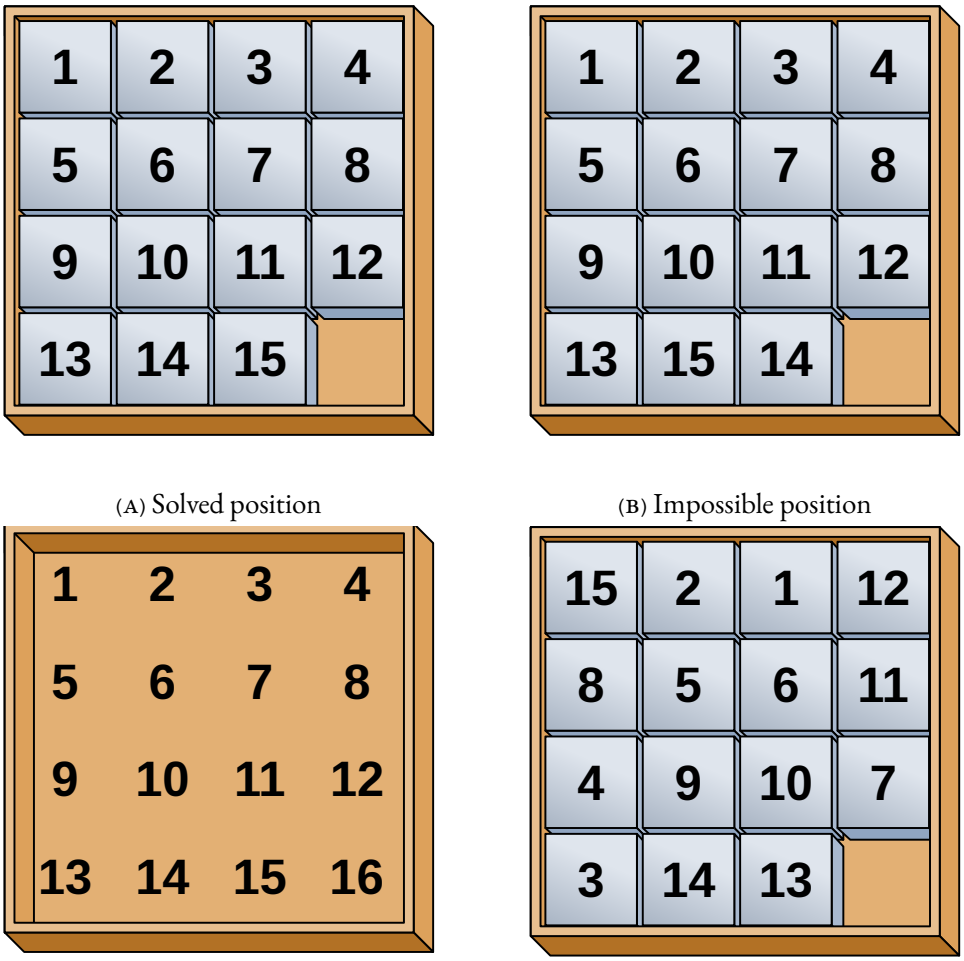
Corollary. *It is impossible to solve the 15-puzzle from the position in Figure 2b.*

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

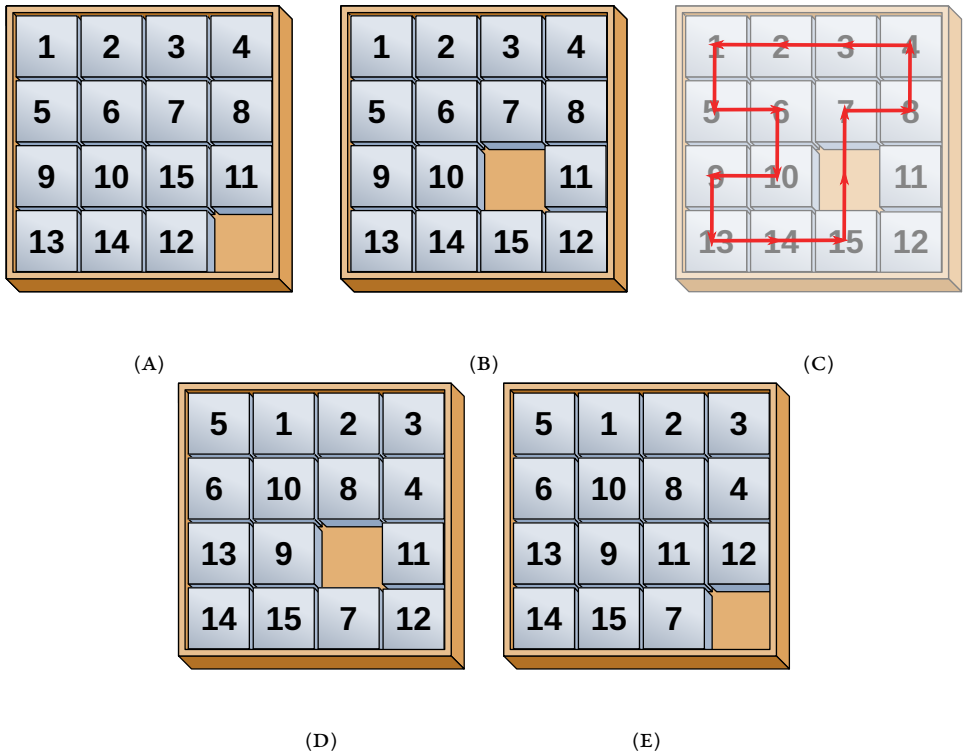


FIGURE 3

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.

[Arm88] 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).

[BW79] Norman L. Biggs and A. T. White. *Permutation Groups and Combinatorial Structures*. Cambridge University Press, Aug. 1979. DOI: 10.1017/cbo9780511600739.

[Cam99] Peter J. Cameron. *Permutation Groups*. Cambridge University Press, Feb. 1999. DOI: 10.1017/cbo9780511623677.

[DM96] 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.

2. Group actions

In the previous section we reviewed basic properties of permutation groups. In this section we will focus on a slightly more general notion, which is that of *group actions*. Informally speaking, group actions are a tool that allows us to treat any group as a permutation group. Formally speaking:

Definition 2.1. Given a group G with neutral element 1 and a set X a *(left) group action* of G on X is a function $\varphi\colon G \times X \to X$ that satisfies

(a) $\varphi\colon (1, x) \mapsto x$ for every $x \in X$
(b) $\varphi\left(gh, x\right) = \varphi\left(g, \varphi(h, x)\right)$ for every $g, h \in G$ and $x \in X$.

We usually omit φ and think of a group action as a way to "evaluate" a group element onto an element of X. In fact, if φ is a left group action, then we usually denote by gx the element $\varphi(g, x) \in X$. With this notation, the element $\varphi\left(gh, x\right)$ should be denoted by $(gh)x$ (we first multiply the elements in the group and then evaluate), whereas the element $\varphi\left(g, \varphi(h, x)\right)$ should be written as $g(hx)$ (we first evaluate h on x and then evaluate g on the resulting element). Thanks to Item (b) of Definition 2.1, we can write ghx without the need of parentheses. If G acts on a set X we say that X is a G-set.

Words of caution: Some authors use *right* group actions, which can be defined in a similar way (see Exercise 2.1). The main difference is the order in which we evaluate the elements, if we take $g, h \in G$ and we and evaluate it (on the left)

in an element x we first evaluate h and then we evaluate g. While if we evaluate the same group element on a right action we first consider the action of g on x and then the action of h on the resulting element. This two operations does not need to be the same. The choice of one side or another is related to the fact that we evaluate permutations on the left. As before, this choice has usually little theoretical consequences, but one needs to be careful (see Exercise 2.1).

We list several examples of group actions below.

Example 2.2. Naturally, if X is any set then the symmetric group S_X acts on the set X in the obvious way:

$$\varphi(\sigma, x) = \sigma(x).$$

Example 2.3. Both the dihedral group and the cyclic group acts on the set $[n]$ by restricting of S_n to the D_n and C_n, respectively. However, both group also act on the set of edges of a n-cycle (equivalently, a regular n-gon) when they are interpreted as symmetries.

Example 2.4. In fact, the previous examples show a obvious but important way to find actions. If G is a permutation group of S_n then G acts naturally on the set $[n]$.

If G is a permutation group, we say that G is of *degree n* if it acts on $[n]$. Some authors also require that there is no $k \in \{1, \dots, n\}$ such that $\sigma(k) = k$ for ever $\sigma \in G$, so that S_3 when interpreted as the subgroup of permutations in S_4 that fix 4 is a group of degree 3 but not of degree 4. We shall make that assumption whenever we refer to a group of degree n.

Example 2.4 suggest a way to find group actions. In fact, it is not hard to see that every group action is essentially given as in this example.

Proposition 2.5. *Let G be a group acting on a set X with the action $\varphi\colon G \times X \to X$. The mapping $\rho_\varphi\colon G \to S_X$ given by $\rho_\varphi(g)\colon x \mapsto gx$ defines a group homomorphism. Conversely, every group homomorphism $\rho\colon G \to S_X$ induces an action of G on X by $gx = \rho(g)(x)$.*

Proof. See Exercise 2.2. □

Example 2.6. Another natural way of finding examples of group actions is by consider the *symmetry group* of geometric figures. That is, the set of symmetries of the space that preserve a given figure. For example, the symmetry group of the cube acts on the set $\{1, 2, 3, 4, 5, 6, 7, 8\}$ of vertices, the set $\{a, b, c, d, e, f, g, h, i, j, k, l\}$ of edges and the set $\{A, B, C, D, E, F\}$ of faces (just to mention some). The 3-fold rotation R on the line that connects the vertices 1 and 7 induce the following permutations the sets of vertices, edges and faces:

$$\begin{aligned} (2\ 5\ 4)(3\ 6\ 8) &\quad \text{on vertices,} \\ (a\ d\ e)(i\ b\ h)(f\ c\ l)(j\ g\ k) &\quad \text{on edges,} \\ (A\ B\ C)(D\ E\ F) &\quad \text{on faces.} \end{aligned}$$

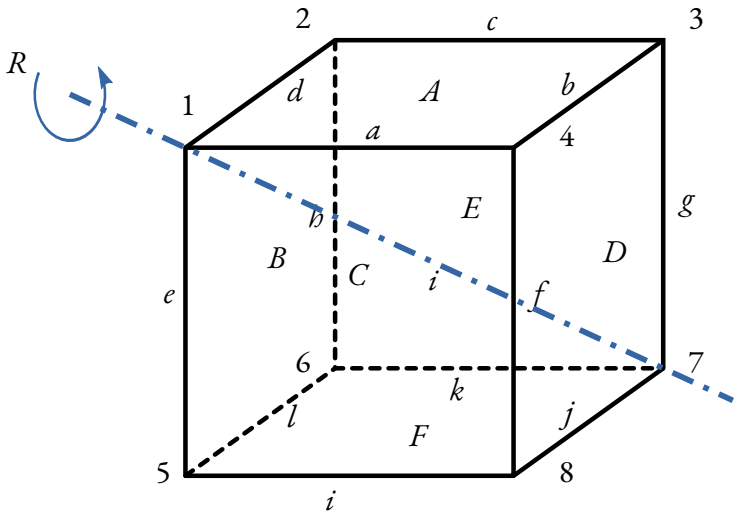


FIGURE 4. A rotation of the cube

Example 2.7. Every group G acts on itself by left multiplication. That is, the action is given by $(g, x) \mapsto gx$ for every $g, x \in G$. If G is finite, say $|G| = n$ the representation $\mu_l \colon G \to S_n$ defined by $\mu_l(g) = \gamma_g$ where $\gamma_g : G \to G$ is given by $\gamma_g(x) = gx$. Yet again, observe that the side for which we multiply is relevant so that μ_l is actually a group-homorphism, i.e.

$$\gamma_{hg} = \mu_l(hg) = \mu_l(h)\mu_l(g) = \gamma_h\gamma_g.$$

The left-most permutation of G in the equation above maps x to $(hg)x$ while the right-most maps x to $\gamma_h(gx) = h(gx)$.

Observe that μ_l is injective. In fact if $\mu_l(g) = \varepsilon$, then $gx = \gamma_g(x) = x$ for every x, which implies that $g = 1$.

The G acts on a set X, the *kernel* of the action is the kernel of the induced representation of G in S_X We say that an action is *faithful* whenever the its kernel is the trivial subgroup. Equivalently, when the associated representation is injective.

The group homomorphism μ_l in Example 2.7 is often called the (left) Cayley representation of G. This homomorphism proves the following theorem.

Theorem 2.8 (Cayley, 1854)**.** *Every finite group with n elements is isomorphic to a subgroup of S_n.*

Even though Theorem 2.8 is more than one hundred years old, it has current relevance. Permutation groups are concrete objects compared to an abstract group. In particular, permutation groups can be understood by a programming language. Unfortunately, the theorem as it is has little practical applications. If a group G is relatively large, the symmetric group on $|G|$ symbols is extremely

complicated. However, the truth is that every faithful action induces an injective homomorphism, so in order to find a representation of an abstract group as a permutation group we only need to find a faithful action. For example, the group G of symmetries of the cube has 48 elements, Theorem 2.8 says that G is isomorphic to a subgroup of S_{48}, which has size 48!. Yet, the action of G on the set of vertices is faithful so G has a representation in S_8. Moreover, the action on the set of faces is also faithful, which implies that G has a representation of degree 6. It is an active research area to find small (minimal) permutation representations of relevant families of finite groups.

Unfortunately, most actions are not faithful. Let us show a example of it.

Example 2.9. Let G be a group and H a subgroup of G. The set X of left cosets of H is a G-set. The action is given by

$$g(xH) = gxH.$$

This action is generally not faithful. If K is a normal subgroup of H then $x^{-1}kx \in K \subseteq H$ for every $k \in K$, which implies that

$$kxH = xH \text{ for every } k \in K$$

Definition 2.10. If $H \leqslant G$ are groups, then the *normal core* (or simply, the *core*) of H in G is the largest normal subgroup of G contained in H, that is

$$\mathrm{Core}_G(H) = \bigcap_{g \in G} g^{-1}Hg$$

Example 2.11. If G is a group, then G is itself a G-set where the action is given by (left) conjugation, that is, the action of a given element g on x is given by

$$g : x \mapsto gxg^{-1}.$$

The kernel of this action is the *centre* $Z(G)$.

Example 2.12. Similarly, G acts on the set $X = \{H : H \text{is subgroup of } G\}$ by $g : H \mapsto gHg^{-1}$.

The intuitive idea of a group G acting on a set X is that every element of G move the elements of X. It makes sense to consider the following important concepts.

Definition 2.13. Assume that G acts on a set X. Given $x \in X$, the *orbit* of x is the set

$$Gx = \{gx : g \in G\}.$$

The *stabiliser* of x is the subgroup (see Exercise 2.5)

$$\mathrm{Stab}_G(x) = \{g \in G : gx = x\}.$$

For a given $g \in G$ the set of *fixed points* is the set

$$\mathrm{Fix}(g) = \{x \in X : gx = x\}.$$

The set of *fixed points* of G is the set

$$\mathrm{Fix}(G) = \{x \in X : gx = x \text{ for all } g \in G\} = \bigcap_{g \in G} \mathrm{Fix}(g)$$

It is important to remark that some authors denote these sets differently. A common notation for the orbit of x is $O(x)$ and the stabiliser is sometimes denoted G_x (see [Rot96], for example). The set of fixed points of an element g and of the group G are sometimes denoted X_g and X_G, respectively.

Observe that the relation $\sim$ in X given by $x \sim y$ if and only if $Gx = Gy$ is an equivalence relation (Exercise 2.4). Therefore this relation defines a partition of X in equivalence classes given by the orbits. The latter implies the following straightforward result.

Proposition 2.14. *The set of orbits induces a partition of X. If $R \subseteq X$ is a set of representatives containing exactly one element for each non-trivial orbit, then*

$$X = \mathrm{Fix}(G) \cup \left(\bigcup_{x \in R} Gx \right)$$

In particular, if X is finite, then

$$|X| = |\mathrm{Fix}(G)| + \left(\sum_{x \in R} |Gx| \right).$$

Let X and Y be two G sets with actions φ_X and φ_Y, respetively. We say that X and Y are *equivalent* (as G-sets) if there exists a bijection $\eta : X \to Y$ such that the following diagram commutes:

$$\begin{array}{ccc} G \times X & \xrightarrow{(\varepsilon, \eta)} & G \times Y \\ \downarrow{\scriptstyle \varphi_X} & & \downarrow{\scriptstyle \varphi_Y} \\ X & \xrightarrow{\eta} & Y \end{array}$$

That is, if

$$\eta\left(\varphi_X(g, x)\right) = \varphi_Y(g, \eta(x))$$

Observe that if X is a G-set and $Z \subseteq X$ is such that $gz \in Z$ for ever $g \in G$, then Z is a G-set. In particular, the orbit of every element of a G-set X is a G-set itself.

Now we present a straightforward but very useful result, sometimes even called the *fundamental theorem of group actions*.

Theorem 2.15 (Orbit-Stabiliser Theorem)**.** *Let G be a group acting on a set X and let $x \in G$. The orbit Gx of x and the set of left cosets of* $\mathrm{Stab}_G(x)$ *are equivalent as G-sets. In particular,*

$$|Gx| = [G : \mathrm{Stab}_G(x)].$$

If G is finite, then

$$|Gx| = \frac{|G|}{|\mathrm{Stab}_G(x)|}$$

Proof. Let S denote the subgroup $\mathrm{Stab}_G(x)$. Consider the mapping $\phi : G/S \to Gx$ given by $\phi(gS) = gx$. First notice that ϕ is well-defined. Indeed if $gS = hS$ then $h^{-1}g \in S$, that is $h^{-1}gx = x$, which implies that $gx = hx$.

Similarly, if g and h are elements in G such that $gx = hx$, then $gS = hS$. In other words, ϕ is injective. Clearly ϕ is surjective. The bijection ϕ defines an equivalence of G-sets. □

We finish this section with some important definitions.

Definition 2.16. Let G be a group acting on a set X. We say that the action is *transitive* if there is only one orbit. That is, if for every two elements $x, y \in X$ there exists a group element g such that $gx = y$.

We say that the action is *free* or *semiregular* if the stabiliser of every element is the trivial group. Finally, we say that an action is *regular* if it is both transitive and semiregular.

Exercises.

2.1 A *right action* of a group G on a set X is mapping $\psi : X \times G \to X$ such that
- $\psi : (x, 1) \mapsto x$ for every $x \in X$
- $\psi\left(x, gh\right) = \psi\left(\psi(x, g), h\right)$.

We usually denote $\psi(x, g)$ by xg.
(a) Prove that if $\varphi : G \times X \to X$ is a left action, then the mapping $\psi : X \times G \to X$ defined by $\psi(x, g) = \varphi(g^{-1}, x)$ defines a right action.
(b) Conversely, if $\psi : X \times G \to X$ is a right action, the mapping $\varphi : G \times X \to X$ given by $\varphi(g, x) = \psi(x, g^{-1})$ defines a left action.
(c) Give an example of a left action φ such that the mapping $\psi : X \times G \to X$ given by $\psi(x, g) = \varphi(g, x)$ is not a right action.

2.2 Proof that every action of a group G on a set X induces a group homomorphism $G \to S_X$ and conversely, that every such homomorphism induces an action of G on X.

2.3 Let G and H be groups. A *group antimorphism* is a function $\phi : G \to H$ that satisfies that

$$\phi(g_1 g_2) = \phi(g_2)\phi(g_1),$$

for every $g_1, g_2 \in G$.
(a) Prove that if $\phi_1 : G \to H$ and $\phi_2 : H \to K$ are group antimorphisms, then $\phi_2 \circ \phi_1 : G \to K$ is a group homomorphism.
(b) Show that $(\,)^{-1} : G \to G$ given by $g \mapsto g^{-1}$ is a group antimorphism.

(c) Conclude that right actions of G to X are incorrespondence with group antimorphisms $G \to S_X$.

2.4 If G is a set acting on a set X, then the relation on X defined by $x \sim y$ if and only if $Gx = Gy$ defines an equivalence relation on X.

2.5 Prove that the stabiliser of a point is a subgroup of G

2.6 Let X and Y two G-sets. Prove that $X \times Y$ is a G set with the action $g(x, y) = (gx, gy)$. Prove that the stabiliser of (x, y) is $\mathrm{Stab}_G(x) \cap \mathrm{Stab}_G(y)$. Show an example where X and Y are transitive but $X \times Y$ is not.

2.7 Show that if $x, y \in X$ belong to the same orbit, then $\mathrm{Stab}_G(x)$ and $\mathrm{Stab}_G(y)$ are conjugate.

2.8 Let X be a transitive G-set. Let S denote the subgroup $\mathrm{Stab}_G(x)$ of a point x. Prove that the core of S on G is precisely the kernel of the action. Prove that this is not necessairly true if X is not transitive.

2.9 If G is a group, a *core-free* subgroup of G is a subgroup H such that $\mathrm{Core}_G(H)$ is trivial. Show that every transitive faithful action of G is equivalent to the left-coset action of a core-free subgroup of G.

2.10 Let H and K subgroup of G, then G is a union of disjoint *double cosets*

$$HgK = \{hgk \in G : h \in H, k \in K\}.$$

If G is finite, then the size of a double coset HgK is $|K| \times \left[H : (gKg^{-1} \cap H)\right]$.

2.11 Let G be a group acting transitively on a set X. Let H be a subgroup of G and let S denote the subgroup $\mathrm{Stab}_G(x)$. Prove that the following statements are equivalent

(a) $G = SH$,
(b) $G = HS$,
(c) H is transitive.

In particular, the only transitive subgroup of G containing S is G itself.

2.12 If G contains a subgroup H of index n, then it contains a normal subgroup $K \leqslant H$ such that $[G : K]$ is finite and divides $n!$.

2.13 if G is a finite group or order m, and p is the smallest prime which divides m, then any group of index p is normal in G.

2.14 Let $n \geqslant 5$, then the only proper subgroup of index less than n in the symmetric group S_n is the alternating group A_n of index 2.

2.15 Prove that there is no simple group of order 56.

2.16 Prove that ther is no simple noncyclic group of order $2^m p^n$ where $m \in \{1, 2, 3\}$ and p an is odd prime.

2.17 For $n \geqslant 2$, $n - 2$ transposition cannnot generate a transitive group of degree n (Compare with Exercise 1.8)

2.18 Let G be a group acting faithfully on a set X. Assume that G has finitely many orbits $X_1, \ldots, X_k$. Notice that G acts transitively on each subset X_i ($i \in \{1, \ldots k\}$). Prove that G is isomorphic to a subgroup of $S_{X_1} \times \cdots \times S_{X_k}$.

2.19 Let G be a group of order p^k with p prime and $k \in \mathbb{N}$. Assume that G acts faithfully on a set X with $|X| = n$ where $n \leqslant p^2$. Prove that $G \cong \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$.

2.20 Let G be an abelian group. Prove that if G acts transitively on a set X, then then the action is regular.

2.21 Find the order of the symmetry group of the cube and the order of the symmetry group of a regular icosahedron.

2.22 If G is a finite non-trivial p-group (that is, a group such that $|G| = p^k$ for some $k \in \mathbb{N}$), then $Z(G)$ is not trivial. **Hint**: consider the action in Example 2.11.

2.23 Let p be a prime such that $p \equiv 1 \pmod 4$. Consider the set

$$X = \left\{(x, y, z) \in \mathbb{N}^3 : x + 4yz = p\right\}.$$

Consider the mapping

$$\phi : (x, y, z) \mapsto \begin{cases} (x + 2z, z, y - x - z) & \text{if } x < y - z \\ (2y - x, y, x - y + z) & \text{if } y - z < x < 2y \\ (x - 2y, x - y + z, y) & \text{if } x > 2y \end{cases}$$

(a) Prove that ϕ is a permutation of order 2 on X with exactly one fixed point.

(b) Prove that the permutation $\psi : (x, y, z) \mapsto (x, z, y)$ must also have at least one fixed point.

(c) Prove a famous theorem in number theory: An odd prime p is a sum of two squares if and only if $p \equiv 1 \pmod 4$.

References.

[Arm88] 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).

[BW79] Norman L. Biggs and A. T. White. *Permutation Groups and Combinatorial Structures*. Cambridge University Press, Aug. 1979. DOI: 10.1017/cbo9780511600739.

[Cam99] Peter J. Cameron. *Permutation Groups*. Cambridge University Press, Feb. 1999. DOI: 10.1017/cbo9780511623677.

[DM96] 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.

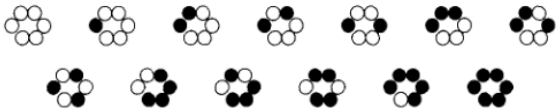


FIGURE 5. 2-colour necklaces of length 6.

[Rot96] Joseph J. Rotman. *A first course in abstract algebra*. Prentice Hall, Inc., Upper Saddle River, NJ, 1996, pp. xiv+265. ISBN: 0-13-311374-4.

3. Pólya theory

Now we turn our attention to a family of counting problems. These are all part of what today is known as Pólya theory of counting but they arise from very basic execercises.

Example 3.1. Assume that we have a broomstick and several cloth pieces of 5 different colours. How many different flags can be constructed using the broomstick as flagpole and two pieces of *different* colour.

Solution. We have 5 possibilities for the colour that goes next to the flagpole and 4 possibilities for the other colour, therefore we have $5 \times 4 = 20$ different flags. □

Example 3.2. If we have the same pieces of cloth as in the previous example, how many flags (with no flagpole) can be built using two pieces of cloth of *different* colour?

Solution. □

Example 3.3. We have the same piece of cloth and the broomstick, how many flags with flagpole can we build if the two colours do not need to be different.

Solution. □

Example 3.4. The same question as above but without the flagpole.

Example 3.5. We want to sit n knights in a round table. Two configurations are the same if one can rotate the table to obtain one from the other. In how many ways can the knights be sit?

Solution. □

Example 3.6. What is the number of essentially different necklaces wich can be made with with n beads of two different colours?

This is not an easy question, for $n = 6$ the number is 13. See Figure 5.

Question 3.7. What is the number of non-isomorphic graphs on n vertices?. For $n = 4$ there are 11.

Question 3.8. What is the number of essentially different ways to paint the faces (or edges, or vertices) of the cube with n colors?

We begin with with the following theorem, which was originally published by Burnside (1897) but was originally prove by Frobenius (1987).

Theorem 3.9 (Burnside's Lemma)**.** *Let G be a group acting on a set X, the number $n(G, X)$ of orbits of G on X is given by*

$$m(G, X) = \frac{1}{|G|} \sum_{g \in G} \mathrm{Fix}(g)$$

Proof. Count the pairs $(g, x) \in G \times X$ such that $gx = x$. A given element $g \in G$ appears in $|\mathrm{Fix}(g)|$ of those pairs. On the other hand, given $x \in X$, there are $|\mathrm{Stab}_G(x)|$ pairs with x as second coordinate. It follows that

$$\sum_{g \in G} |\mathrm{Fix}(g)| = \sum_{x \in X} |\mathrm{Stab}_G(x)| .$$

Now assume that $Y = \{y_1, \ldots, y_m\} \subseteq X$ is a set of elements, one for each orbit (so that $m(G, X) = m$).

$$\begin{aligned}
m(G, X) &= \sum_{y \in Y} 1 \\
&= \sum_{x \in Gy_1|} \frac{1}{|Gy_1|} + \cdots + \sum_{x \in Gy_m} \frac{1}{|Gy_m|} \\
&= \sum_{x \in Gy_1} \frac{1}{|Gx|} + \cdots + \sum_{x \in Gy_m} \frac{1}{|Gx|} \\
&= \sum_{x \in X} \frac{1}{|Gx|} \\
&= \sum_{x \in X} \frac{|\,\mathrm{Stab}_G(x)|}{|G|} \\
&= \frac{1}{|G|} \sum_{x \in X} |\,\mathrm{Stab}_G(x)| \\
&= \frac{1}{|G|} \sum_{g \in X} |\,\mathrm{Fix}(g)|.
\end{aligned}$$

□

Let us apply Burnside's Lemma to solve Example 3.5. Clearly, the cyclic group C_n acts mapping one arrangement of the table to another. Two arrangements are essentially different if and only if they are not in the same orbit. This means that we want to count orbits under the action of C_n of all the possible ways of

sitting the knights. The amount of possible arrangements is $n!$. The permutation $id \in C_n$ fixes every arrangement while every non-trivial element has no fixed arrangements. By Burnside lemma the number of orbits is

$$\frac{1}{n}|\operatorname{Fix}(id)| = \frac{n!}{n}.$$

Let us now formalise this notion of conting colouring configurations of objects. Let $K = \{1, \dots, k\}$ be a set, which we call the set of *colours*. Assume that X is a set. A *colouring* of X is a function $c : X \to K$, that is, a function that assigns the colour $c(x)$ to each element $x \in X$. The set of *colourings* of X (with colour-set K) is the set

$$K^X = \{c : X \to K\}.$$

Observe that if $|X| = n$, then $|K^X| = k^n$, as expected.

Let G be a a permutation group of X, then the group G acts on K^X by

$$\sigma c = c(\sigma^{-1}),$$

that is, for every $x \in X$, the colouring σc is given by

$$(\sigma c)(x) = c(\sigma^{-1}(x)).$$

The inverse is necessary to guarantee that the previous mapping is actually a left action.

Now we use Burnside Lemma to compute the number of orbits of colourings of a set X with respect a permutation group G of X.

Proposition 3.10. *Let X be a set with n elements and G a permutation group of S_X. Let K be a set of colours with $|K| = k$. Let m denote the number of orbits of G on K^X, the set of colourings of X. Then*

$$m = \frac{1}{|G|} \sum_{\ell} c_\ell(G) k^\ell,$$

where $c_\ell(G)$ denotes the number of elements of G that have ℓ cicles.

Proof. Let $\sigma \in G$. Assume that c is colouring fixed by σ, that is, for every $x \in X$

$$c(\sigma^{-1}x) = \sigma(c)(x) = c(x).$$

If follows that if any two elements of X in the same cycle of σ must have the same colour. Clearly, if σ has ℓ cycles, there are k^ℓ colourings of X satisfying that any two elements in the same cycle have the same colour. Any such colouring is fixed by σ. The result follows from Burnside's Lemma. □

We can now solve Example 3.6. We need to compute the number $c_\ell(D_6)$ for the dihedral group D_6. The elements of D_6 are listed below:

(1)(2)(3)(4)(5)(6)	(1 2 3 4 5 6)	(1 3 5)(2 4 6)
(1 4)(2 5)(3 6)	(1 5 3)(2 6 4)	(1 6 5 4 3 2)
(1)(4)(2 6)(3 5)	(2)(5)(1 3)(4 6)	(3)(6)(2 4)(1 5)
(1 2)(3 6)(4 5)	(2 3)(1 4)(5 6)	(3 4)(2 5)(1 6)

It follows that $c_1(D_6) = 2$, $c_2(D_6) = 2$, $c_3(D_6) = 4$, $c_4(D_6) = 3$, $c_5(D_6) = 0$ and $c_6(D_6) = 1$.

The 6 permutations in the first two rows above are precisely the elements of the cycle group C_6. We can compute the numbers $c_1(C_6) = c_2(C_6) = 2, c_3(C_6) = 1$ and $c_6(C_6) = 1$.

We can now compute the number of necklaces of legth 6 with two colors with respect to rotations (using C_6) or with respect to rotation and flips (using D_6).

$$m(D_6) = \frac{1}{12}\left(2 \times 2 + 2 \times 2^2 + 4 \times 2^3 + 3 \times 2^4 + 1 \times 2^6\right) = \frac{156}{12} = 13$$
$$m(C_6) = \frac{1}{6}\left(2 \times 2 + 2 \times 2^2 + 1 \times 2^3 + 1 \times 2^6\right) = \frac{84}{6} = 14$$

The fact that we get one extra orbit with the cyclic group is that all but one of the orbits with respect to the dihedral group have mirror reflection (see Figure 5). The rightmost necklace in the first row does not admit mirror reflection, hence its orbit with respecct to the dihedral group has to be split into two different orbits of the cyclic group.

Proposition 3.10 allows us to count colored objects that are essentially different with respect to the symmetires of the group G. That number depends only on the cycle structure of the elements on G, more precisely on the numbers $c_\ell(G)$. In the following paragraph we will introduce the *cycle index* of a permutation group G, which generalise in some sense the numbers $c_\ell(G)$.

Let G be a permutation group of a set X, with $|X| = n$ and let $\sigma \in G$, the *cycle monomial* of σ is defined as

$$M_\sigma(t_1, \ldots, t_n) = \prod_{i=1}^{k} t_{\ell_i}$$

if σ has k cycles and the i-th cycle is of length t_{ℓ_i}. In other words, the exponent of t_i, $i \in \{1, \ldots, n\}$ in $M_\sigma(t_1, \ldots, t_n)$ is k whenever σ has k cycle of lenth i.

The *cycle index of* G is the polynomial

$$Z_G(t_1, \ldots, t_n) = \frac{1}{|G|} \sum_{\sigma \in G} M_\sigma(t_1, \ldots, t_n).$$

Observe that the cycle index actually generalises the numbers $c_\ell(G)$ discussed before. In fact, the sum of the coefficients of the terms of degree ℓ in $Z_G(t_1,\dots,t_n)$ is precisely the number the $\frac{c_\ell(G)}{|G|}$.

From the previous discussion the following proposition is obvious.

Proposition 3.11. *Let X be a set with n elements and G a permutation group of S_X. Let K be a set of colours with $|K| = k$. Let m denote the number of orbits of G on K^X, the set of colourings of X. Then*

$$m = Z_G(k,\dots,k).$$

We will compute some cycle index as excercises (see Exercises 3.1 to 3.4). We shall use them just to show how they work.

According to Exercise 3.2, the cycle index of the cyclic group is

$$Z_{C_n}(t_1,\dots t_n) = \frac{1}{n}\sum_{d|n}\phi(d)t_d^{n/d}.$$

For $n = 6$ we have

$$Z_{C_6}(t_1,\dots,t_6) = \frac{1}{6}\left(t_1^6 + t_2^3 + 2t_3^2 + 2t_6\right)$$

Similaryly for the dihedral group D_6,

$$Z_{D_6}(t_1,\dots,t_6) = \frac{1}{12}\left(t_1^6 + t_2^3 + 2t_3^2 + 2t_6 + 3t_1^2t_2^2 + 3t_2^3\right)$$

Then we can use Proposition 3.11 to solve the 2-colour necklace problem:

$$Z_{C_6}(2,\dots,2) = \frac{1}{6}\left(2^6 + 2^3 + 2\cdot 2^2 + 2\cdot 2\right) = \frac{84}{6} = 14$$

$$Z_{D_6}(2,\dots,2) = \frac{1}{12}\left(2^6 + 2^3 + 2\cdot 2^2 + 2\cdot 2 + 3\cdot 2^2\cdot 2^2 + 3\cdot 2^3\right) = \frac{156}{12} = 13$$

Proposition 3.11 allows us to compute the number of orbits of coloured objects whith no restrictions, but say that we are interested in finding 2-coloured necklaces of length 6 such that only 2 white bead are used.

From now on we will modify slightly our notation, and we shall denote $K = \{y_1,\dots,y_k\}$ the set of colours.

Definition 3.12. Let X be a set with n elements and let $G \leqslant S_n$ a permutation group acting on X. Let $K = \{y_1,\dots,y_k\}$ a set of colours. Let $\bar{v} = (n_1,\dots,n_k)$ a vector of k integers such that $n_i \geqslant 0$ for every i and $n_1 + \cdots n_k = n$. Let a_v denote the number of non-equivalent colourings (with respect to G) such that the colour y_i is used n_i times. The *pattern inventory* of G is the polynomial

$$P_G(y_1,\dots,y_k) = \sum_{\bar{v}} a_{\bar{v}} y_1^{n_1}\dots y_k^{n_k}.$$

Clearly, if we know an explicit expression for P_G then we how many colourings of a given type we have. Our task now is to find a way to compute P_G. Before doing that let us compute a very simple to show how the pattern inventory works.

Example 3.13. Let X be a set with n elements. How many colourings with 2 colours exists if we do not mind symmetry?.

Proof. Solution Let say tha the colour-set is $K = \{x, y\}$ For this problem the vectors $\overline{v}$ are of length 2 and since both entries must sum n they are of the form $(i, n-i)$. Obiously, the number of colourings using the colour x i times, when no symmetry is considered is determined by which of the elements of X are coloured with the given colour. In other words

$$a_{(i,n-i)} = \binom{n}{i},$$

hence the pattern inventoy is just

$$P_{\{id\}}(x, y) = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-1}$$

□

The expression on the right side of prevoious equations should be familiar for the reader. A well-known theorem claims that $P_{id}(x, y) = (x + y)^n$, and this is not a coincidence; let us explore this example further.

If we express the product $(x + y)^n$ as

$$\underbrace{(x + y)(x + y) \cdots (x + y)}_{n \text{ times}}$$

one can see that every term of the product, before reducing similar terms, is given by chosing either x or y on each of the monomials. This explains the fact tha the coefficient of $x^i y^{n-i}$ is precisely $\binom{n}{i}$, the number of ways of chossing i times the letter x. We shall see that this coincides with the ways of chossing one colour for each cyclie of the (unique) element on the group $\{id\}$. More precisely,

Theorem 3.14 (Polya counting formula)**.** *Let X be a set of n elements and $G \leqslant S_n$ a group acting on X. Let $K = \{y_1, \cdots, y_k\}$ be a colour-set. Denote bye $P_G(y_1, \ldots, y_k)$ the pattern inventory and by $Z_G(t_1, \ldots, t_n)$ the cycle index of G, then*

$$P_G(y_1, \ldots, y_k) = Z_G\left(\sum_{j=1}^{k} y_j, \sum_{j=1}^{k} y_j^2, \ldots, \sum_{j=1}^{k} y_j^n\right).$$

Proof. Let $\overline{v} = (n_1, \ldots, n_k)$ be a vector such that $n_i \geqslant 0$ for every i and $n_1 + \cdots + n_k = n$. Let $C_{\overline{v}} \subseteq K^X$ the set of colourings of X such that there are exactly n_i

elements of colour y_i. For $\sigma \in G$, let $C_{\bar{v},\sigma} \subseteq C_{\bar{v}}$ the set of colourings in $C_{\bar{v}}$ that are preserved by σ.

For $\bar{v}$ as above, let $\bar{y}^{\bar{v}}$ denote the term $y_1^{n_1} \cdots y_k^{n_k}$. If $c \in C_{\bar{v},\sigma}$ then every two elements on a cycle have the same colour, because the colouring must be preserved by σ. Moreover, the lengths of the cycles coloured with a given colour y_i must add n_i. Obivously every colouring satisfying those two conditions is in $C_{\bar{v},\sigma}$.

Consider the monomial $M_\sigma\left(\sum_{j=1}^k y_j, \sum_{j=1}^k y_j^2, \ldots, \sum_{j=1}^k y_j^n\right)$. This monomial is just

$$M_\sigma\left(\sum_{j=1}^k y_j, \sum_{j=1}^k y_j^2, \ldots, \sum_{j=1}^k y_j^n\right) = \prod_\ell \left(y_1^\ell + \cdots + y_k^\ell\right)$$

where ℓ runs over the lengths of the cycles of σ. Observe that the the term $\bar{y}^{\bar{v}}$ appears in $\prod_\ell \left(y_1^\ell + \cdots + y_k^\ell\right)$ as many times as the ways of choosing one letter (of $\{y_1, \ldots, y_k\}$) per cycle of σ such that the sum of the lengths of the cycles where we choose y_i is n_i.

When comparing the two previous analysis it is easy to see that the coefficient of $\bar{y}^{\bar{v}}$ in $M_\sigma\left(\sum_{j=1}^k y_j, \sum_{j=1}^k y_j^2, \ldots, \sum_{j=1}^k y_j^n\right)$ is precisely $|C_{\bar{v},\sigma}|$. When we sum over all possible $\bar{v}$ we have

$$M_\sigma\left(\sum_{j=1}^k y_j, \sum_{j=1}^k y_j^2, \ldots, \sum_{j=1}^k y_j^n\right) = \sum_{\bar{v}} |C_{\bar{v},\sigma}|\, \bar{y}^{\bar{v}}.$$

Now we sum over all possible elements $\sigma \in G$ and divide by $|G|$ and we have:

$$\begin{aligned}
Z_G\left(\sum_{j=1}^k y_j, \sum_{j=1}^k y_j^2, \ldots, \sum_{j=1}^k y_j^n\right) &= \frac{1}{|G|} \sum_{\sigma \in G} M_\sigma\left(\sum_{j=1}^k y_j, \sum_{j=1}^k y_j^2, \ldots, \sum_{j=1}^k y_j^n\right) \\
&= \frac{1}{|G|} \sum_{\sigma \in G} \sum_{\bar{v}} |C_{\bar{v},\sigma}|\, \bar{y}^{\bar{v}} \\
&= \sum_{\bar{v}} \left(\frac{1}{|G|} \sum_{\sigma \in G} |C_{\bar{v},\sigma}|\right) \bar{y}^{\bar{v}} \\
&= \sum_{\bar{v}} a_{\bar{v}} \bar{y}^{\bar{v}} \\
&= P_G(y_1, \ldots, y_k)
\end{aligned}$$

where the second to last equality follows from Burnside Lemma. □

As an example let us compute the pattern inventory of possible colouring of necklaces of length 4 using colours red (r) first with respect to the dihedral group

and then with respecto to the cyclic group.

$$Z_{D_4}(t_1, t_2, t_3, t_4) = \frac{1}{8}\left(t_1^4 + 3t_2^2 + 2t_4 + 2t_1^2 t_2\right)$$
$$Z_{C_4}(t_1, t_2, t_3, t_4) = \frac{1}{4}\left(t_1^4 + t_2^2 + 2t_4\right)$$

Using Polya counting formula we can see that

$$\begin{aligned} P_{D_4}(r,g,b) &= Z_{D_4}(r+g+b, r^2+g^2+b^2, r^3+g^3+b^3, r^4+g^4+b^4) \\ &= \frac{1}{8}\left((r+g+b)^4 + 3(r^2+g^2+b^2)^2 + 2(r^4+g^4+b^4) + \right. \\ &\qquad \left. 2(r+g+b)^2(r^2+g^2+b^2)\right) \\ &= r^4 + r^3g + 2r^2g^2 + rg^3 + g^4 + r^3b + 2r^2gb + 2rg^2b + g^3b + \\ &\qquad + 2r^2b^2 + 2rgb^2 + 2g^2b^2 + rb^3 + gb^3 + b^4 \end{aligned}$$

and

$$\begin{aligned} P_{C_4}(r,g,b) &= Z_{C_4}(r+g+b, r^2+g^2+b^2, r^3+g^3+b^3, r^4+g^4+b^4) \\ &= \frac{1}{4}\left((r+g+b)^4 + (r^2+g^2+b^2)^2 + 2(r^4+g^4+b^4)\right) \\ &= r^4 + r^3g + 2r^2g^2 + rg^3 + g^4 + r^3b + 3r^2gb + 3rg^2b + g^3b + \\ &\qquad + 2r^2b^2 + 3rgb^2 + 2g^2b^2 + rb^3 + gb^3 + b^4 \end{aligned}$$

Observe that there are two non-equivalent colouring with two red beads, one green and one blue under D_4 wheareas there are three of them under C_4. This is essentially because the necklaces (r, r, g, b) and (r, r, b, g) are different with respecto to the cyclic group but equivalent with resepct to the dihedral group.

Consider now the following example:

Example 3.15. Suppose a jewelry company plans to market a new line of unisex bracelets. The bracelets are sold in pairs, for a couple to share. Each bracelet consists of n beads, some gold and some silver, and the two bracelets in a pair are opposites, in the sense that one can be obtained from the other by changing each silver bead to a gold one and each gold to a silver. For example, if one bracelet has two adjacent gold beads and $n - 2$ silver beads, then its mate has two adjacent silver beads and $n - 2$ gold beads.

Using the cycle index of D_4 computed before we can see that there are 6 non equivalent bracelets with two colours. Moreover, using Polya counting formula we can easily see that the pattern inventory is

$$P_{D_4}(g, s) = s^4 + s^3g + 2s^2g^2 + sg^3 + g^4$$

Meaning that bracelets can be represented as (s, s, s, s), (s, s, s, g), (s, g, s, g) (s, s, g, g), (s, g, g, g) and (g, g, g, g). However, when we consider the change of colours we

only have three different pairs, namelly

$$\{(s,s,s,s),(g,g,g,g)\}$$
$$\{(s,g,s,g),(g,s,g,s)\}$$
$$\{(s,s,g,g),(g,g,s,s)\}$$
$$\{(g,g,g,s),(s,s,s,g)\}$$

Notice that the pair of the bracelet (s,g,s,g) is (g,s,g,s), which is equivalent to the former under the action of D_4. In other words, that pair of bracelets consists of two identical bracelets.

We can take a step back and count unfasten bracelets (that is, linear $\{g,s\}$-sequences) and then consider two of them equivalet if we can obtain one from the other by either the action of a dihedral group or by a swich of colours. We can see that we obtain precisely the same equivalence classes as before:

$\{(s,s,s,s),(g,g,g,g)\}$
$\{(s,g,s,g),(g,s,g,s)\}$
$\{(s,s,g,g),(g,g,s,s),(s,g,g,s),(g,s,s,g)\}$
$\{(g,g,g,s),(g,g,s,g),(g,s,g,g),(s,g,g,g),(s,s,s,g),(s,s,g,s),(s,g,s,s),(g,s,s,s)\}$

Observe that in these consists of the orbits of linear $\{g,s\}$-sequences under the action of two groups. On the one hand we have the group D_4 acting as symmetries of the necklaces and on the other hand we have a cyclic group C_2 swapping the colours. Let us formalise these ideas for the general case.

Let X be a set with n elements and $G \leqslant S_n$ a permutation group acting on X. Let K be a set with k *colours* and $H \leqslant S_k$ a permutation group acting on K. If $\sigma \in G$, $\tau \in H$ and $c \in K^X$ the mapping $(\sigma,\tau)c \mapsto \bar{c}$ where $\bar{c}$ is the colouring defined by

$$\bar{c}(x) = \tau\left(c(\sigma^{-1}x)\right)$$

defines a left action of $G \times H$ on K^X (see Exercise 3.14).

The following result tells us how to count the number of orbits for this action.

Proposition 3.16. *Let X be a set with $|X| = n$ and $G \leqslant S_n$ a permutation group acting on X. Let K be a set of colours with $|K| = k$ and $H \leqslant S_k$ a permutation group acting on K. The number of orbits N of K^X under the action on $G \times H$ defined above is:*

$$N = \frac{1}{|H|}\sum_{\tau\in H} Z_G(m_1(\tau),\ldots,m_n(\tau))$$

where $m_i(\tau) = \sum_{j|i} j \cdot z_j(\tau)$ and $z_j(\tau)$ denotes the number of cycles of length j in τ.

Proof. Let $\sigma \in G$ and $\tau \in H$. Denote by $\phi(\sigma, \tau)$ the number of colourings preserved by (σ, τ). By Burnside lemma

$$N = \frac{1}{|G \times H|} \sum_{(\sigma,\tau)\in G\times H} \phi(\sigma, \tau) = \frac{1}{|H|} \sum_{\tau\in H} \left(\frac{1}{|G|} \sum_{\sigma\in G} \phi(\sigma, \tau) \right)$$

It remains to show that

$$\frac{1}{|G|} \sum_{\sigma\in G} \phi(\sigma, \tau) = Z_G(m_1(\tau), \ldots, m_n(\tau)).$$

Let $\gamma_1, \ldots, \gamma_d$ be the cycle of σ and let us denote $V_i = supp(\gamma_i) \subseteq X$ the *support* of γ_i, that is $V_i = X \setminus \mathrm{Fix}(\gamma_i)$. Clearly a colouring c is preserved by (σ, τ) if and only if each of its restriction $c_i : V_i \to K$ is preserved by (γ_i, τ). Let $\phi_i(\sigma, \tau)$ be the number of colourings of V_i preserved by (γ_i, τ). From the previous observation we have that $\phi(\sigma, \tau) = \prod_{i=1}^{d} \phi_i(\gamma_i, \tau)$. Observe that if $c_i : V_i \to X$ is a colouring fixed by (γ_i, τ) then

$$c_i(x) = (\gamma_i, \tau)c_i(x) = \tau(c_i(\gamma_i^{-1}x)) = \tau(c_i(\sigma^{-1}x)) \text{ for all } x \in V_i,$$

or equivalently

$$c_i(\sigma y) = \tau(c_i(y)) = \text{ for all } y \in V_i$$

Assume that γ_i has length ℓ_i (that is $|V_i| = \ell_i$), pick $x_0 \in V_i$ and let $k := c_i(x_0)$. Observe that the colour of every other element in V_i depends only on k and τ. In fact, if $y = \sigma^r(x_0)$ then $c_i(y) = c_i(\sigma^r x_0) = \tau^r(c_i(x_0)) = \tau^r(k)$. In particular, since this is true for $r = \ell_i$, we have that the cycle of τ containing k must divide ℓ_i.

Conversely, if we pick any element $k \in K$ such that the cycle of τ containing k has length a divisor of ℓ_i, then the mapping $c_i : V_i \to X$ defined by $c_i(\gamma_i^r x_0) = \tau^r(k)$ is a well-defined colouring that is preserved by (γ_i, τ).

In other words the number $\phi_i(\sigma, \tau)$ is equal to the number of ways of picking a colour k lying on a cycle of τ of length a divisor of ℓ_i. Obviously this number is

$$\phi_i(\sigma, \tau) = \sum_{j|\ell_i} j z_j(\tau) = m_{\ell_i}(\tau)$$

Finally, observe that

$$\phi(\sigma, \tau) = \prod_{i}^{d} \phi_i(\sigma, \tau) = \prod_{i}^{d} m_{\ell_i}(\tau) = M_\sigma(m_1(\tau), \ldots, m_n(\tau)).$$

The result follows from taking the sum over the elements of G and dividing by $|G|$ □

We finish the section of the notes by remarking that the previous result solves the problem of finding the number of non-equivalent colourings under the action of the group G on the set of elements and the group H on the set of colours.

The notion of a *patter inventory* can be also extended to this context and an analogous result to Theorem 3.14 was proved by De Brujin in 1964. We leave this result out of these notes but is the reader is interested a proof can be found on [Bru67]

Exercises.

3.1 Find the cycle index of the group of rotations of the cube.

3.2 Prove that the cycle index if the cyclic group is

$$Z_{C_n}(t_1, \dots t_n) = \frac{1}{n} \sum_{d|n} \phi(d) t_d^{n/d}.$$

3.3 Prove that the cycle index of the dihedral group $D_n$is

$$Z_{D_n}(t_1, \dots, t_n) = \begin{cases} \frac{1}{2n} \left(\sum_{d|n} \phi(d) t_d^{n/d} + n t_1 t_2^{\frac{n-1}{2}} \right) & \text{for } n \text{ odd,} \\ \frac{1}{2n} \left(\sum_{d|n} \phi(d) t_d^{n/d} + \frac{n}{2} t_1^2 t_2^{\frac{n}{2}-1} + \frac{n}{2} t_2^{\frac{n}{2}} \right) & \text{for } n \text{ even} \end{cases}$$

3.4 We say that a partition P of $[n]$ is of type $(k_1, k_2, \dots k_n)$ if P has k_1 subsets of size 1, k_2 of size 2, etc.

(a) Find the number of partitions of $[n]$ of a given type $(k_1, \dots k_n)$.

(b) Use the previous item to prove that

$$Z_{S_n}(t_1, \dots, t_n) = \sum_{(k_1, \dots k_n)} \frac{1}{1^{k_1} 2^{k_2} \cdots n^{k_n} k_1! k_2! \cdots k_n!} t_1^{k_1} \cdots t_n^{k_n}.$$

(c) Compute explicitly the cycle index of S_n for $n \leqslant 5$.

3.5 Find the number of essentially different colourings of the vertices of K_5 (the complete graph with 5 vertices) with at most 5 colours.

3.6 Let X_1 and X_2 be two disjoint sets of size n_1 and n_2, respectivelly. Let G_i a permutation group of the set X_i ($i \in \{1, 2\}$). Consider the group $G = G_1 \times G_2$.

(a) Prove that G acts faithfully on $X = X_1 \cup X_2$.

(b) Prove that

$$Z_G(t_1, \dots, t_{n_1}, s_1, \dots, s_{n_1}) = Z_{G_1}(t_1, \dots, t_{n_1}) \cdot Z_{G_2}(s_1, \dots, s_{n_2})$$

(c) Compute the cycle index of the largest subgroup of S_5 that preserves the partition $\{\{1, 2, 3\}, \{4, 5\}\}$.

3.7 The commander of a space cruiser wishes to post four sentry ships arrayed around the cruiser at the vertices of a tetrahedron for defensive purposes, since an attack can come from any direction.

(a) How many ways are there to deploy the ships if there are two different kinds of sentry ships available, and we discount all symmetries of the tetrahedral formation?

(b) How many ways are there if there are three different kinds of sentry ships available?

3.8 Consider the natural action of the dihedral group D_4 on the tiles of an unpainted 4×4 chekerboard. Let G denote the induced permutation group of the 16 tiles.

(a) Find the cycle index of G.
(b) In how many ways can we paint the board if we use colours black and white.
(c) In how many ways can we paint the checkerboard if 8 tiles must be black and 8 must be white?
(d) What if we paint exactly 4 tiles black and there must be exactly one black tile on each row and each column?

3.9 Consider the symmetric group S_4 acting on the 6 edges of a complete graph K_4. Let G denote the induced permutation group, that is $G \leqslant S_6$.

(a) Compute the cycle index of G.
(b) Use this to compute the number of non-isomorphic graphs on 4 vertices.

3.10 How many 0, 1-sequences of lenght 12 exists if two sequences are considered to be the same if one can be obtained from the other by a cyclic shift. How many are there if each consists of exactly 6 ones and 6 zeros.

3.11 What is the pattern inventory for coloring n objects using the m colours $y_1, \ldots, y_m$ if the group of symmetries is S_n?

3.12 Two identical cubes are glued to two oposite faces of a third cube to form a 3×1 prism. The prism has 14 squares exposed (4 of the cube in the middle 5 of each of the other two cubes).

(a) Find the permutation group G on the 14 squares induced by all the possible ways of rotating the prism.
(b) Compute the cycle index of G.
(c) In how many ways can the squares be painted using at most three colours: black, white and blue.
(d) Whay if exactly two of the squares must be blue?

3.13 What is the number of essentially different ways to paint the faces of a cube such that one face is red, two are blue, and the remaining three are green?

3.14 Let X be a set with n elements and $G \leqslant S_n$ a permutation group acting on X. Let K be a set with k *colours* and $H \leqslant S_k$ a permutation group acting on K. Prove that if $\sigma \in G$, $\tau \in H$ and $c \in K^X$ the mapping $(\sigma, \tau)c \mapsto \bar{c}$ where $\bar{c}$ is the colouring defined by

$$\bar{c}(x) = \tau\left(c(\sigma^{-1}x)\right)$$

defines a left action of $G \times H$ on K^X.

3.15 The hydrocarbon naphthalene has ten carbon atoms arranged in a double hexagon as in Figure 6, and eight hydrogen atoms attached at each of the positions labeled 1 through 8.

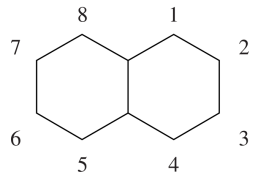


FIGURE 6. Naphthalene

(a) Naphthol is obtained by replacing one of the hydrogen atoms of naphthalene with a hydroxyl group (*OH*). How many isomers of naphtholare there?
(b) Tetramethylnaphthalene is obtained by replacing four of the hydrogen atoms of naphthalene with methyl groups (CH_3). How many isomers of tetramethylnaphthalene are there?
(c) How many isomers may be constructed by replacing three of the hydrogen molecules of naphthalene with hydroxyl groups, and another three with methyl groups?
(d) How many isomers may be constructed by replacing two of the hydrogen molecules of naphthalene with hydroxyl groups, two with methyl groups, and two with carboxyl groups (*COOH*)?

3.16 Determine the number of ways to color the faces of a cube using the three colors red, blue, and green, if two colorings are considered to be equivalent if one can be obtained from the other by rotating the cube in some way in three-dimensional space, and possibly exchanging green and red.

References.

[Bru10] Richard Brualdi. *Introductory combinatorics*. Upper Saddle River, N.J: Pearson/Prentice Hall, 2010. ISBN: 0136020402.

[Bru67] N. G. de Bruijn. "Color patterns that are invariant under a given permutation of the colors". en. In: *Journal of Combinatorial Theory* 2.4 (June 1967), pp. 418–421. ISSN: 0021-9800. DOI: 10.1016/S0021-9800(67)80052-8. URL: https://www.sciencedirect.com/science/article/pii/S0021980067800528 (visited on 04/10/2022).

[HHM10] John Harris, Jeffry L. Hirst, and Michael Mossinghoff. *Combinatorics and Graph Theory*. SPRINGER NATURE, Dec. 2010. 400 pp. ISBN: 1441927239. URL: https://www.ebook.de/de/product/13975405/john_harris_jeffry_l_hirst_michael_mossinghoff_combinatorics_and_graph_theory.html.

[J H09] R. M. Wilson J. H. Van Lint. *A Course in Combinatorics*. Cambridge University Press, Mar. 2009. 620 pp. ISBN: 0521006015. URL: https://www.ebook.de/de/product/3258175/j_h_van_lint_r_m_wilson_a_course_in_combinatorics.html.

[Mer03] Russell Merris. *Combinatorics*. John Wiley & Sons, Inc., Aug. 2003. DOI: 10.1002/0471449687.