Week 10: Permutations

Instructor: Igor Kortchemski (igor.kortchemski@polytechnique.edu)
Tutorial Assistants:
– Apolline Louvet (groups A&B, apolline.louvet@polytechnique.edu)
– Milica Tomasevic (groups C&E, milica.tomasevic@polytechnique.edu)
– Benoît Tran (groups D&F, benoit.tran@polytechnique.edu).

1 Important exercises

The solutions of the exercises which have not been solved in some group will be available on the course webpage.

Exercise 1. Consider the permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 4 & 8 & 7 & 6 & 2 & 1 \end{pmatrix}$

(1) Compute σ^{-1}. (2) Write σ as a product of cycles with disjoint supports.

(3) Write σ^2 in table notation and in cycle notation. (4) Compute σ^{2019}.

Solution of exercise 1.

1. We read the "table" representation of σ upwards:
$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 7 & 1 & 3 & 2 & 6 & 5 & 4 \end{pmatrix}.$$

2. We have $\sigma = (1,3,4,8)(2,5,7)$.

3. We can either use the "table" representation, or the cycle representation. In view of the next question, lets use the cycle notation. Then
$$(1,3,4,8)^2 = (1,3,4,8)(1,3,4,8) = (1,4)(3,8), \qquad (2,5,7)^2 = (2,5,7)(2,5,7) = (2,7,5).$$
Hence
$$\sigma^2 = (1,4)(3,8)(2,7,5)$$
and
$$\sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 7 & 8 & 1 & 2 & 6 & 5 & 3 \end{pmatrix}.$$

4. We use the cycle representation and observe that
$$(1,3,4,8)^3 = (1,8,4,3), \qquad (2,5,7)^3 = \mathrm{Id}.$$
Since $2019 = 3 \mod 4$ and $2019 = 0 \mod 3$, we get that
$$\sigma^{2019} = (1,3,4,8)^{2019}(2,5,7)^{2019} = (1,3,4,8)^3 = (1,8,4,3).$$

□

Definition. Let $\sigma \in S_n$ be a permutation. For $1 \le i, j \le n$, we say that (i, j) is an inversion if $i < j$ and $\sigma(i) > \sigma(j)$. We denote by $I(\sigma)$ the total number of inversions of σ, and we define $\epsilon(\sigma) = (-1)^{I(\sigma)}$ to be the *signature* of σ. If $\epsilon(\sigma) = 1$, we say that σ is an *even* permutation, and if $\epsilon(\sigma) = -1$, we say that σ is an *odd* permutation.

Theorem. If $\pi, \sigma \in S_n$ are two permutations, we have $\epsilon(\pi\sigma) = \epsilon(\pi)\epsilon(\sigma)$.
We say that ϵ is *multiplicative*. You should remember this result. See the course webpage for the (optional) proof, based on the identity $\epsilon(\pi) = \prod_{1 \le i < j \le n} \frac{\pi(j)-\pi(i)}{j-i}$.

Exercise 2. If σ is the permutation of exercise 1, find $I(\sigma)$ and $\epsilon(\sigma)$.

Solution of exercise 2. We have 2 inversions starting with 1 ((1,7), (1,8)), 3 starting with 2 ((2,3), (2,7), (2,8)) and so on: 2 starting with 3, 4 starting with 4, 3 starting with 5, 2 starting with 6 and 1 starting with 7. We therefore have $I(\sigma) = 17$ and $\epsilon(\sigma) = (-1)^{17} = -1$. □

The following exercise gives a way to compute the signature of a permutation by using its cycle decomposition.

Exercise 3. Fix an integer $n \ge 1$.

1. Let $\tau_{i,j}$ be the transposition which exchanges i and j (with $1 \le i < j \le n$). Show that $\varepsilon(\tau_{i,j}) = -1$.
2. If $\sigma = \tau_1\tau_2\cdots\tau_N$ is a product of transpositions, show that $\varepsilon(\sigma) = (-1)^N$ (**you should remember this result**).
3. Let $\tau = (x_1, \dots, x_p)$ be a p-cycle (with $p \ge 2$).
   a) Show that $\tau = (x_1, x_p) \circ (x_1, x_{p-1}) \circ \cdots (x_1, x_3) \circ (x_1, x_2)$.
   b) Show that the signature of a p-cycle is $(-1)^{p-1}$ (**you should remember this result**).
4. Use the previous questions to find the signature of the permutation σ defined in exercise 1.

Solution of exercise 3.

1. Let us find the number of inversions of $\tau_{i,j}$. Every element of $\{i+1, \dots, j-1\}$ contributes to 2 inversions (one with i and one with j), this gives $2(j-i-1)$ inversions, and (i, j) is also an inversion. We therefore have $2(j-1)-1$ inversions, so that $\varepsilon(\tau_{i,j}) = -1$.

2. Simply write
$$\varepsilon(\sigma) = \varepsilon(\tau_1)\varepsilon(\tau_2)\cdots\varepsilon(\tau_N) = (-1)^N.$$

3. (a) First, if $k \notin \{x_1, \dots, x_p\}$, then $\tau(k) = k$ and $(x_1, x_p)(x_1, x_{p-1})\cdots(x_1, x_3)(x_1, x_2)\big(k\big) = k$. Next, for $1 \le i \le p-1$,
$$\tau(x_i) = x_{i+1} \qquad \text{and} \qquad (x_1, x_p)(x_1, x_{p-1})\cdots(x_1, x_3)(x_1, x_2)\big(x_i\big) = x_{i+1}$$
and
$$\tau(x_p) = x_1 \qquad \text{and} \qquad (x_1, x_p)(x_1, x_{p-1})\cdots(x_1, x_3)(x_1, x_2)\big(x_p\big) = x_1.$$
This shows that τ and $(x_1, x_p)(x_1, x_{p-1})\cdots(x_1, x_3)(x_1, x_2)$ are equal.

(b) By question 2,

$$\varepsilon(\tau) = \varepsilon((x_1, x_p)) \cdots \varepsilon((x_1, x_2)) = (-1)^{p-1},$$

since the product has $p-1$ terms.

4. Since we know the cycle decomposition of σ, by using the previous question we have

$$\varepsilon(\sigma) = \varepsilon((1,3,4,8))\varepsilon((2,5,7)) = (-1)^{4-1} \cdot (-1)^{3-1} = -1,$$

which is consistent with the result of exercise 2.

□

Exercise 4. Fix an integer $n \geq 3$.

1. Find two permutations $\sigma, \tau \in \mathfrak{S}_n$ such that $\sigma \circ \tau = \tau \circ \sigma$.
2. Find two permutations $\sigma, \tau \in \mathfrak{S}_n$ such that $\sigma \circ \tau \neq \tau \circ \sigma$.

Solution of exercise 4.

1. Take $\sigma = \tau = \mathrm{Id}$.

2. Take $\sigma = (1,2,3)$ and $\tau = (1,2)$ in the cycle representation. Then

$$\sigma \circ \tau = (1,2,3) \circ (1,2) = (1,3), \qquad \tau \circ \sigma = (1,2) \circ (1,2,3) = (2,3).$$

□

2 Homework exercise

You have to individually hand in the written solution of the next exercise to your TA on December, 9th.

Exercise 5. Consider the permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 1 & 7 & 4 & 6 & 2 \end{pmatrix}$.

(1) Write σ^{2019} as a product of cycles with disjoint support. (2) What is the signature of σ^{2019}? Justify your answers (you can use without proof the results of the previous exercises)

Solution of exercise 5.

(1) We first find the cycle decomposition of σ: $\sigma = (1,3)(2,5,4,7)$. We have $(1,3)^2 = Id$, $(2,5,4,7)^4 = Id$ and $(2,5,4,7)^3 = (2,7,4,5)$. Since $2019 = 1 \mod 2$ and $2019 = 3 \mod 4$, it follows that

$$\sigma^{2019} = (1,3)^{2019}(2,5,4,7)^{2019} = (1,3)(2,5,4,7)^3 = (1,3)(2,7,4,5).$$

(2) We have $\epsilon(\sigma^{2019}) = \epsilon((1,3)(2,7,4,5)) = \epsilon((1,3))\epsilon((2,7,4,5)) = (-1)^{2-1}(-1)^{4-1} = 1.$ □

3 More involved exercises (optional)

The solution of these exercises will be available on the course webpage at the end of week 10.

Exercise 6. 1) List all the elements of $\mathfrak{S}_4$ which are 3-cycles.

2) Fix two integers $2 \leq k \leq n$. How many different k-cycles of $\mathfrak{S}_n$ are there? Justify your answer.

Solution of exercise 6.

1) The 3-cycles of $\mathfrak{S}_4$ are $(1,2,3)$, $(1,3,2)$, $(1,2,4)$, $(1,4,2)$ $(1,3,4)$, $(1,4,3)$, $(2,3,4)$, $(2,4,3)$. There are 8 of them.

2) A k-cycle of $\mathfrak{S}_n$ may be constructed by first a choice of the k elements of its support ($\binom{n}{k}$ choices), and then by an ordering of these k elements ($k!$ choices). However, in this construction, every k-cycle is counted k times. Therefore the total number is

$$(k-1)! \times \binom{n}{k}.$$

Remark. For $n = 4$ and $k = 3$, we get 8 3-cycles in $\mathfrak{S}_4$, which is consistent with the first question. $\square$

Exercise 7. Fix an integer $n \geq 1$ and a permutation $\pi \in \mathfrak{S}_n$. Show that the function $f : \mathfrak{S}_n \to \mathfrak{S}_n$ defined by $f(\sigma) = \sigma \circ \pi$ for every $\sigma \in \mathfrak{S}_n$ is a bijection.

Solution of exercise 7. We first check that f is one-to-one. Let $\sigma, \sigma' \in \mathfrak{S}_n$ be such that $f(\sigma) = f(\sigma')$. Then $\sigma \circ \pi = \sigma' \circ \pi$. By composing by π^{-1} on the right, we get that $\sigma \circ \pi \circ \pi^{-1} = \sigma' \circ \pi \circ \pi^{-1}$. Therefore $\sigma = \sigma'$, so that f is one-to-one.

We next show that f is onto. Let $\tau \in \mathfrak{S}_n$ be a permutation. Then $f(\tau \circ \pi^{-1}) = \tau \circ \pi^{-1} \circ \pi = \tau$. This shows that τ has at least one preimage by f, so that f is onto.

We conclude that f is a bijection. $\square$

Exercise 8. Fix an integer $n \geq 2$, a permutation $\sigma \in \mathfrak{S}_n$ and consider a p-cycle $c = (a_1, a_2, \ldots, a_p)$. Show that $\sigma \circ c \circ \sigma^{-1} = \big(\sigma(a_1), \ldots, \sigma(a_p)\big)$.

Solution of exercise 8. First, it is a simple matter to see that $\sigma \circ c \circ \sigma^{-1}(k)$ and $(\sigma(a_1), \ldots, \sigma(a_p)(k)$ take the same value for $k \in \{\sigma(a_1), \ldots, \sigma(a_p)\}$. If $k \notin \{\sigma(a_1), \ldots, \sigma(a_p)\}$, then $\sigma^{-1}(k) \notin \{a_1, \ldots, a_p\}$, so that $c \circ \sigma^{-1}(k) = \sigma^{-1}(k)$. It follows that

$$\sigma \circ c \circ \sigma^{-1}(k) = \sigma \circ \sigma^{-1}(k) = k = (\sigma(a_1), \ldots, \sigma(a_p)(k).$$

This completes the proof. $\square$

Exercise 9. Let $n \geq 3$ be an integer. For $1 \leq i \neq j \leq n$, denote by $\tau_{i,j}$ the transposition exchanging i and j.

1. Show that for every $2 \leq i < j \leq n$, $\tau_{i,j} = \tau_{1,i} \circ \tau_{1,j} \circ \tau_{1,i}$. Deduce that every permutation of $\mathfrak{S}_n$ can be written as a product of transpositions of the form $\tau_{1,i}$ with $2 \leq i \leq n$.

2. Show that for every $2 \leq i < j \leq n$, $(1,i,j) = \tau_{1,j} \circ \tau_{1,i}$. Deduce that every even permutation can be written as a product of cycles of the form $\tau_{1,i,j}$ with $2 \leq i \neq j \leq n$.

Solution of exercise 9.

1. If $k \notin \{1,i,j\}$, k does not belong to the supports of $\tau_{i,j}$, $\tau_{1,i}$, $\tau_{1,j}$, so that $\tau_{i,j}(k) = \tau_{1,i} \circ \tau_{1,j} \circ \tau_{1,i}(k) = k$. Otherwise,
$$\tau_{i,j}(1) = 1, \quad \tau_{i,j}(i) = j, \quad \tau_{i,j}(j) = i$$
and
$$\tau_{1,i} \circ \tau_{1,j} \circ \tau_{1,i}(1) = 1, \quad \tau_{1,i} \circ \tau_{1,j} \circ \tau_{1,i}(i) = j, \quad \tau_{1,i} \circ \tau_{1,j} \circ \tau_{1,i}(j) = i.$$
We saw in the lecture that every permutation of $\mathfrak{S}_n$ can be decomposed into a product of transpositions. We have just established that every transposition can be written as a product of transpositions of the form $\tau_{1,i}$ with $2 \leq i \leq n$. The desired result follows.

2. If $k \notin \{1,i,j\}$, k does not belong to the supports of $(1,i,j)$, $\tau_{1,j}$ and $\tau_{1,i}$ so that
$$(1,i,j)\big(k\big) = k, \quad \tau_{1,j} \circ \tau_{1,i}(k) = k.$$
Otherwise,
$$(1,i,j)\big(1\big) = i, \quad (1,i,j)\big(i\big) = j, \quad (1,i,j)\big(j\big) = 1$$
and
$$\tau_{1,j} \circ \tau_{1,i}(1) = i, \quad \tau_{1,j} \circ \tau_{1,i}(i) = j, \quad \tau_{1,j} \circ \tau_{1,i}(j) = 1.$$
Let σ be an even permutation. By the first question, σ can be decomposed as a product of transpositions of the form $\tau_{1,i}$ with $2 \leq i \leq n$. Since the signature of a transposition is -1, it follows that such a decomposition is composed of an even number of transpositions. By grouping them 2 by 2, it follows by the previous paragraph that every even permutation can be written as a product of cycles of the form $\tau_{1,i,j}$ with $2 \leq i \neq j \leq n$.

□

Exercise 10. Fix an integer $n \geq 2$ and consider the circular permutation $c = (1,2,\ldots,n-1,n)$. Find all the permutations $\sigma \in \mathfrak{S}_n$ that commute with c (that is $\sigma \circ c = c \circ \sigma$).

Solution of exercise 10. First notice that every permutation σ of the form $\sigma = c^i$ with $i \geq 1$ commutes with c.

Conversely, assume that $\sigma \in \mathfrak{S}_n$ commutes with c. Then $\sigma \circ c \sigma^{-1} = c$. But by exercise 4, $\sigma \circ c \circ \sigma^{-1} = (\sigma(1), \sigma(2), \sigma(3), \ldots, \sigma(n))$. Therefore $c = (\sigma(1), \sigma(2), \sigma(3), \ldots, \sigma(n))$. This implies that there exists an integer $1 \leq i \leq n-1$ such that $\sigma(i) = 1$, $\sigma(i+1) = 2$, $\ldots$, $\sigma(n) = n-i+1$, $\sigma(1) = n-i+2, \ldots \sigma(i-1) = n$. Therefore $\sigma = c^i$.

This completes the proof. □

Exercise 11. Fix integers $1 \leq k \leq n$. If $\sigma \in \mathfrak{S}_n$ is a permutation and $1 \leq k \leq n$, we say that k is a record of σ if for every $1 \leq i \leq k-1$ we have $\sigma(i) < \sigma(k)$. Show that the number of permutations of $\mathfrak{S}_n$ having k cycles in their cycle decomposition is equal to the number of permutations of $\mathfrak{S}_n$ having k records.

Hint. Try to find a bijection!

Solution of exercise 11. Start with a permutation $\sigma \in \mathfrak{S}_n$. Consider its cycle decomposition, written in such a way that each cycle starts with its largest element, and such that the cycles are ordered in increasing order of their first elements (and we write cycles having only one element in this writing). For example, if $\sigma = (1,4)(3,9)(2,7,5) \in \mathfrak{S}_9$, we write $\sigma = (4,1)(6)(7,5,2)(8)(9,3)$. Then let $f(\sigma)$ be the permutation obtained in table notation by erasing the parentheses. With the previous example, this gives

$$f(\sigma) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 1 & 6 & 7 & 5 & 2 & 8 & 9 & 3 \end{pmatrix}.$$

In order to show that f is a bijection, we explicitly construct its inverse function. More precisely, if π is a permutation written in table notation, let $g(\pi)$ be the permutation in cycle notation obtained by inserting an opening parenthesis at the beginning, a closing parenthesis at the end, and a ")(" before every record, except the first. For example, if

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ \boxed{4} & 1 & \boxed{6} & \boxed{7} & 5 & 2 & \boxed{8} & \boxed{9} & 3 \end{pmatrix}$$

with records in boxes, we get $g(\sigma) = (1,4)(3,9)(2,7,5)$.

By construction, it is a simple matter to see that $f(g(\sigma)) = g(f(\sigma)) = \sigma$ for every $\sigma \in \mathfrak{S}_n$. By Exercise 7 of Week 8, this implies that f is a bijection and that g is its inverse bijection.

In addition, by construction σ has k cycles if and only if $f(\sigma)$ has k records. This implies the desired result.

Remark. The number $s(n,k)$ of permutations of $\mathfrak{S}_n$ having k cycles is called the Stirling number of the first kind. □

Exercise 12. Let n be an odd integer and $\sigma \in \mathfrak{S}_n$. Show that 4 divises $\prod_{i=1}^{n}(\sigma(i)^2 - i^2)$.

Solution of exercise 12. Start with writing

$$\prod_{i=1}^{n}(\sigma(i)^2 - i^2) = \prod_{i=1}^{n}(\sigma(i) - i) \cdot \prod_{i=1}^{n}(\sigma(i) - i(\sigma(i) + i).$$

The idea is to show that each one of these two big products contain at least one even term. To this end, observe that $\sum_{i=1}^{n} \sigma(i) = \sum_{i=1}^{n} i$, so that $\sum_{i=1}^{n}(\sigma(i) - i)$ and $\sum_{i=1}^{n}(\sigma(i) + i)$ are both even. But these terms have an odd number of terms (since n is odd). Hence in both of these sums, at least one term is even. This completes the proof. □

Exercise 13. Fix an integer $n \geq 1$ and consider the sub-vector space $\{(x_1, \ldots, x_n) \in \mathbb{R}^n : x_1 + x_2 + \cdots + x_n = 0\}$ of $\mathbb{R}^n$. Denote by $(e_i)_{1 \leq i \leq n}$ the canonical basis. For every $\sigma \in \mathfrak{S}_n$, let $f_\sigma : \mathbb{R}^n \to \mathbb{R}^n$ be the endomorphism such that $f_\sigma(e_i) = e_{\sigma(i)}$ for every $1 \leq i \leq n$. Set $p = \frac{1}{n!} \sum_{\sigma \in \mathfrak{S}_n} f_\sigma$.

1. Show that p is a projector, that is $p \circ p = p$ (*hint:* You may use the result of exercise 7).
2. Find $\operatorname{Im} p$ and $\ker p$.

Solution of exercise 13.

1. First note that p is an endomorphism as a linear combination of endomorphisms. Then write

$$p^2 = \frac{1}{n!^2}\left(\sum_{\sigma\in\mathfrak{S}_n} f_\sigma\right)^2 = \frac{1}{n!^2}\sum_{\sigma,\sigma'\in\mathfrak{S}_n} f_\sigma \circ f_{\sigma'}.$$

   But $f_\sigma \circ f_{\sigma'} = f_{\sigma\circ\sigma'}$ and the map $\sigma \mapsto \sigma\circ\sigma'$ is a bijection from $\mathfrak{S}_n$ to itself. It follows that for fixed $\sigma' \in \mathfrak{S}_n$,

$$\sum_{\sigma\in\mathfrak{S}_n} f_{\sigma\circ\sigma'} = \sum_{\sigma\in\mathfrak{S}_n} f_\sigma.$$

   Therefore

$$p^2 = \frac{1}{n!^2}\sum_{\sigma'\in\mathfrak{S}_n}\left(\sum_{\sigma\in\mathfrak{S}_n} f_{\sigma\circ\sigma'}\right) = \frac{1}{n!^2}\sum_{\sigma'\in\mathfrak{S}_n}\left(\sum_{\sigma\in\mathfrak{S}_n} f_\sigma\right) = \frac{n!}{n!^2}\sum_{\sigma\in\mathfrak{S}_n} f_\sigma = p.$$

   This shows that p is a projector.

2. First note that for fixed $1 \le i,j \le n$, there are $(n-1)!$ permutations σ such that $\sigma(i) = j$. It follows that for $1 \le i \le n$,

$$p(e_i) = \frac{1}{n!}\sum_{\sigma\in\mathfrak{S}_n} f_\sigma(e_i) = \frac{1}{n!}\sum_{\sigma\in\mathfrak{S}_n} e_{\sigma(i)} = \frac{1}{n!}\cdot(n-1)!\sum_{k=1}^n e_k = \frac{1}{n}\sum_{k=1}^n e_k.$$

   Therefore, setting

$$u = \frac{1}{n}\sum_{k=1}^n e_k,$$

   we have

$$\operatorname{Im} p = \operatorname{Vect}(p(e_1),\ldots,p(e_n)) = \operatorname{Vect}(u).$$

   To find $\ker p$, if $x = x_1e_1 + \cdots + x_ne_n \in \mathbb{R}^n$, write

$$p(x) \iff \sum_{k=1}^n x_k p(e_k) = 0 \iff \left(\sum_{k=1}^n x_k\right)u = 0 \iff \sum_{k=1}^n x_k = 0 \iff x \in H,$$

   where $H = \{(x_1,\ldots,x_n) \in \mathbb{R}^n : x_1 + x_2 + \cdots + x_n = 0\}$.

   We conclude that p is the projection on $\operatorname{Vect}(u)$ parallel to H.

□

4 Fun exercise (optional)

The solution of this exercise will be available on the course webpage at the end of week 10.

Exercise 14. The names of 100 mathematicians are placed in 100 wooden boxes, one name to a box, and the boxes are lined up on a table in a room. One by one, the mathematicians are led into the room; each may look in at most 50 boxes, but must leave the room exactly as she found it and is permitted no further communication with the others. The mathematicians have a chance to plot their strategy in advance, and they are going to need it, because unless every single mathematician finds her own name all will subsequently lose their funding. Find a strategy for them which has probability of success (mathematics survive) exceeding 30%.

Remark. If each mathematician examines a random set of 50 boxes, their probability of success is $\frac{1}{2^{100}}$ (each mathematician that opens 50 boxes at random among 100 has a probability $\frac{1}{2}$ to find her name), which is very very small.

Solution of exercise 14. See https://en.wikipedia.org/wiki/100_prisoners_problem. □