Homework 3.

Important notice

- If you have any questions regarding the tasks, please email clemence.chanavat@gmail.com;
- This assignment gives you 10% of the final grade;
- Your solution should be in the PDF format. You may either scan a handwritten solution or type your solution in LaTeX and export it into PDF. Submission made in Word typeset are not accepted;
- For submitting your solution in a LaTeX, you may get up to extra 2% to this assignment, but not more than 30% of the points you reached for content;
- Using online tools and/ot someone's else code to solve the tasks is prohibited. If you are suspected of this, then you will receive 0 for the task;
- Plagiarism is prohibited. If you are suspected of this, then you will receive 0 for the task and will be reported to the Dean's office and Program Manager;
- This assignment is due 17th of December, 23:59.

Introduction

This Homework is around the notion of permutation, a very important concept in group theory. Permutation groups are very concrete. Take a deck of card and shuffle it. You just created a permutation. Take a Rubik's cube and shuffle it. You just created a permutation. Take the word "group" and shuffle its letters into "pguro". You just created another permutation. Formally, a permutation is a bijection (a "shuffling") from a finite set to itself. The set of all permutations form a group (doing no shuffle is the neutral element, and shuffling then shuffling again is the composition, while shuffling back is the inverse).

Definition 1: Let $n \geq 1$ a natural number. We define the finite set

$$S_n := \{1, 2, \dots, n\}.$$

A *permutation* is a bijection $\sigma : S_n \to S_n$. We define

$$\Sigma_n := \{\sigma : S_n \to S_n \mid \sigma \text{ permutation}\}.$$

Let $\sigma \in \Sigma_n$, the *two lines's notation* is a way to represent the permutation σ. It consists of an array with two rows and n columns. In the first row are the elements $1, \dots, n$, in the second are the elements $\sigma(1), \dots, \sigma(n)$, we write:

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}.$$

Example 2:

1. The identity function $\mathrm{id} : S_4 \to S_4$ is a permutation, whose two line's notation is
$$\mathrm{id} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}.$$
2. The function $\sigma : S_2 \to S_2$ that sends 1 to 2 and 2 to 1 is a permutation whose two line's notation is
$$\sigma = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}.$$
3. As permutations are in particular functions, we can compose them, so if $\sigma, \tau \in \Sigma_n$, then $\sigma \circ \tau$ is again a function with $\sigma \circ \tau(i) := \sigma(\tau(i))$, for $\leq i \leq n$. We saw in class that the composition of two bijection is again a bijection, so $\sigma \circ \tau$ is also a permutation.

Mandatory Exercises

To get familiar with permutations, we start with some examples.

Exercise 1:

1. Give all the permutations of Σ_3.
2. Let
$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}, \text{ and } \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}.$$
Give (in two line's notation) $\sigma \circ \tau$ and $\tau \circ \sigma$.
3. Let
$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \text{ and } \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}.$$
Give (in two line's notation) $\sigma \circ \tau$ and $\tau \circ \sigma$.
4. Why
$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 2 & 1 \end{pmatrix}$$
is not a permutation in Σ_4?
5. How many elements has Σ_n? (no justification, just give the answer).

Exercise 2: Let $n \geq 1$ be a natural number. Prove that Σ_n is a group, whose binary law is the function composition, neutral element is the identity function, and inverse of $\sigma \in \Sigma_n$ is σ^{-1}, the the inverse function (a permutation is a bijection, so it has an inverse).

Exercise 3: In Exercise 1, you gave all the permutations of Σ_3. Recopy them now, and:

1. Pair up each permutation with its inverse;
2. Give the order of each permutation (recall, the order of an element x of a group is the smallest $n \geq 1$ such that $x^n = e$).
3. Bonus point, what do I mean by: "make sure that your result to the previous question is consistent with Langrage Theorem"?
4. Oh no, someone took the multiplication table of Σ_3 and renamed the permutations by Greek letters...

$\circ$	ι	α	β	γ	δ	ϕ
ι	ι	α	β	γ	δ	ϕ
α	α	ι	δ	ϕ	β	γ
β	β	ϕ	ι	δ	γ	α
γ	γ	δ	ϕ	ι	α	β
δ	δ	γ	α	β	ϕ	ι
ϕ	ϕ	β	γ	α	ι	δ

   Give the appropriate Greek letter $\{\iota, \alpha, \beta, \gamma, \delta, \phi\}$ to each permutation in your homework, so that the above multiplication table is true. Warning: there are multiple correct answers (but just give one!). As the group in not abelian, the convention for reading the table is $\beta \circ \alpha$ for the pink-colored case.

Exercise 4:

1. Show that Σ_2 is abelian.
2. Show that Σ_3 is not abelian (thus, give two permutations $\sigma, \tau \in \Sigma_3$ such that $\sigma \circ \tau \neq \tau \circ \sigma$).
3. Let $n \geq 3$. Show that Σ_n is not abelian (thus, give two permutations $\sigma, \tau \in \Sigma_n$ such that $\sigma \circ \tau \neq \tau \circ \sigma$).

Bonus Exercises

The rest of this homework is dedicated to proving Cayley's theorem: every finite group is isomorphic to the subgroup of a permutation group.

Definition 3: Let G be a finite group. For $g \in G$, we define a function, called a *left-action*,

$$\begin{aligned} \lambda_g : G &\to G \\ x &\mapsto g \cdot x. \end{aligned}$$

We define the set of left-actions:

$$\Lambda_G := \{\lambda_g \mid g \in G\}.$$

Exercise 5: Let $(G, \cdot, e)$ be a finite group, let $g, g' \in G$.

1. Prove that $\lambda_e = \mathrm{id}_G$ (where id_G is the identity on G).
2. Prove that $\lambda_g \circ \lambda_{g'} = \lambda_{g \cdot g'}$.
3. Prove that $\lambda_g \circ \lambda_{g^{-1}} = \mathrm{id}_G$ and $\lambda_{g^{-1}} \circ \lambda_g = \mathrm{id}_G$ (note: it follows almost directly from the two previous questions).
4. Conclude this exercise by proving that Λ_G, is a group, where the binary law is given by composition, whose identity is λ_e, and the inverse is given by $\lambda_g^{-1} := \lambda_{g^{-1}}$.

Exercise 6: Let $(G, \cdot, e)$ be a finite group. Recall from Exercise 5 that Λ_G is a group.

1. Show that the function

$$\begin{aligned} \eta : G &\to \Lambda_G \\ g &\mapsto \lambda_g \end{aligned}$$

   is a group morphism.

2. Show that η is surjective (this is almost by definition of Λ_G).

3. Show that η is injective (recall that it can be done by proving that $\ker(\eta) = \{e\}$).

We did enough work, and the proof of Cayley's theorem now follows. We give it for the interested reader, but it just amount to organize what we did in the previous Exercises (note: the following is not an exercise, simply an explanation for whoever is interested).

Theorem 4 (Cayley's): Let G be a finite group of size n. Then there exists a subgroup K of Σ_n such that $G \cong K$.

Proof. (**Theorem 4**) The η from Exercise 6 is bijective group morphism, also know as isomorphism, thus we have

$$G \cong \Lambda_G,$$

As G has n elements, we can write it as

$$G = \{g_1, g_2, \ldots, g_n\}.$$

Now, if we take $\lambda \in \Lambda_G$, then $\lambda : G \to G$ is a function that does

$$\sigma = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ \lambda(g_1) & \lambda(g_2) & \ldots & \lambda(g_n) \end{pmatrix}.$$

so if we remove the g's from the above, it is as if λ was a permutation in Σ_n:

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ \lambda(1) & \lambda(2) & \ldots & \lambda(n) \end{pmatrix}.$$

As this picture is also compatible with composition and neutral elements, we can see Λ_G as a group isomorphic to K, a subgroup of Σ_n, and we have $G \cong \Lambda_G \cong K$. The reader interested in the formalities of this argument can make it precise by introducing any bijection $f : G \to S_n$, and define $K := \{f^{-1} \circ \lambda_g \circ f \mid g \in G\} \subseteq S_n$ (bonus point: do the proof of this Theorem precisely). $\square$