# I - Exercice 1

## I.A -

On note $A = \{(i \quad i+1) | i \in \{1, 2, \cdots, n-1\}\}$ l'ensemble de transpositions et $\langle A \rangle$ le sous-groupe engendré par A. On va montré $\langle A \rangle = \mathscr{S}_n$ par double inclusion.

- Par définition, $\langle A \rangle$ est un sous-groupe de $\mathscr{S}_n$, donc $\langle A \rangle \subset \mathscr{S}_n$
- $\forall s \in \mathscr{S}_n$, si $\forall i \in \{1, 2, \cdots, n\}, s(i) = i$, c'est le cas de produit vide. Sinon, par la décomposition, on a $s = \tau_1 \circ \tau_2 \cdots \tau_r$, où $\forall i \in \{1, 2, \cdots, r\}$, $\tau_i$ une transposition, et $r \leq n-1$. On va montrer que pour chaque transposition $(i \quad j)$ tel que $(i, j) \in \{1, 2, \cdots, n\}^2, i < j$, elle s'écrit

$$(i \quad j) = (j-1 \quad j) \circ (j-2 \quad j-1) \cdots \circ (i \quad i+1) \circ (i+1 \quad i+2) \circ \cdots (j-1 \quad j)$$

On note $\gamma$ la partie à droite.

  - Par récurrence, on a

$$\begin{aligned}
\gamma(j) &= (j-1 \quad j) \circ (j-2 \quad j-1) \cdots \circ (i \quad i+1) \circ (i+1 \quad i+2) \circ \cdots (j-2 \quad j-1)[j-1] \\
&= (j-1 \quad j) \circ (j-2 \quad j-1) \cdots \circ (i \quad i+1) \circ (i+1 \quad i+2) \circ \cdots (j-3 \quad j-2)[j-2] \\
&= (j-1 \quad j) \circ (j-2 \quad j-1) \cdots (i+1 \quad i+2) \circ (i \quad i+1)[i+1] \\
&= (j-1 \quad j) \circ (j-2 \quad j-1) \cdots (i+1 \quad i+2)[i] \\
&= (j-1 \quad j) \circ (j-2 \quad j-1) \cdots (i+2 \quad i+3)[i] \\
&= i \\
&= (i \quad j)[j]
\end{aligned}$$

  - De même, on a

$$\begin{aligned}
\gamma(i) &= (j-1 \quad j) \circ (j-2 \quad j-1) \cdots \circ (i \quad i+1) \circ (i+1 \quad i+2) \circ \cdots (j-2 \quad j-1)[i] \\
&= (j-1 \quad j) \circ (j-2 \quad j-1) \cdots \circ (i \quad i+1) \circ (i+1 \quad i+2) \circ \cdots (j-3 \quad j-2)[i] \\
&= (j-1 \quad j) \circ (j-2 \quad j-1) \cdots (i+1 \quad i+2) \circ (i \quad i+1)[i] \\
&= (j-1 \quad j) \circ (j-2 \quad j-1) \cdots (i+1 \quad i+2)[i+1] \\
&= (j-1 \quad j) \circ (j-2 \quad j-1) \cdots (i+2 \quad i+3)[i+2] \\
&= (j-1 \quad j)[j-1] \\
&= j \\
&= (i \quad j)[i]
\end{aligned}$$

  - $\forall m \in \{1, 2, \cdots, n\}^2$ tel que $m > j$ ou $m < i$, m n'est pas influencé par chacune des transpositions : $\gamma(m) = (i \quad j)(m)$
  - $\forall k \in \{1, 2, \cdots, n\}^2$ tel que $i < k < j$, on a

$$\begin{aligned}
\gamma(k) &= (j-1 \quad j) \circ \cdots (k \quad k+1) \cdots \circ (i \quad i+1) \circ \cdots (j-2 \quad j-1)[k] \\
&= (j-1 \quad j) \circ \cdots (k \quad k+1) \cdots \circ (i \quad i+1) \circ \cdots (k \quad k+1) \circ \cdots (j-3 \quad j-2)[k] \\
&= (j-1 \quad j) \circ \cdots (k \quad k+1) \cdots (i \quad i+1) \circ \cdots (k \quad k+1)[k] \\
&= (j-1 \quad j) \circ \cdots (k \quad k+1) \cdots (i \quad i+1) \circ \cdots (k+2 \quad k+3)[k+1] \\
&= (j-1 \quad j) \circ \cdots (k \quad k+1)[k+1] \\
&= k \\
&= (i \quad j)[k]
\end{aligned}$$

En tout cas, on a $(i \quad j) = \gamma$, ce qui montre que chaque transposition peut s'écrit comme une produit des $(i \quad i+1)$. Par la composition, $\forall s \in \mathscr{S}_n$ peut aussi s'écrit comme une produit des $(i \quad i+1)$. On a donc $\mathscr{S}_n \subset \langle A \rangle$

Finalement, $\mathscr{S}_n = \langle A \rangle$, on a donc $\boxed{\mathscr{S}_n \text{ est engendré par } A}$

## I.B -

Par la même méthode, on note $B = \{(1 \quad 2), (1 \quad 2 \cdots \quad n)\}$ et $\langle B \rangle$ le sous-groupe engendré par B. On va montré $\langle B \rangle = \mathscr{S}_n$ par double inclusion.

- Par définition, $\langle B \rangle$ est un sous-groupe de $\mathscr{S}_n$, donc $\langle B \rangle \subset \mathscr{S}_n$
- $\forall s \in \mathscr{S}_n$, on a montré qu'elle s'écrit comme un produit de $(i \quad i+1)$, on va montrer que $(i \quad i+1) \in \langle B \rangle$. On note $c = (1 \quad 2 \cdots n)$ le n-cycle. Puisque $c^n = Id_{\{1,2,\cdots n\}}$, on va etudier $\sigma = c^{i-1} \circ (1 \quad 2) \circ c^{n-i+1}$
  - lorsque $i = 1$, $\sigma = c^0 \circ (1 \quad 2) \circ c^n = (1 \quad 2)$
  - pour $1 < i < n$, on a $1 \leq i-1 \leq n-2$ et $2 \leq n-i+1 \leq n-1$, donc $c^{i-1} \neq Id_{\{1,2,\cdots n\}}$, $c^{n-i+1} \neq Id_{\{1,2,\cdots n\}}$. On a donc
    — $\sigma(i) = c^{i-1} \circ (1 \quad 2) \circ c^{n-i+1}(i) = c^{i-1} \circ (1 \quad 2)(1) = c^{i-1}(2) = i+1$
    — $\sigma(i+1) = c^{i-1} \circ (1 \quad 2) \circ c^{n-i+1}(i) = c^{i-1} \circ (1 \quad 2)(2) = c^{i-1}(1) = i$
    — $\forall k \in \{1, 2, \cdots, n\} \backslash \{i, i+1\}$, $c^{n-i+1}(k) \notin \{1, 2\}$, donc
    $\sigma(k) = c^{i-1} \circ (1 \quad 2) \circ c^{n-i+1}(k) = c^{i-1} \circ c^{n-i+1}(k) = c^n(k) = k$

  En tout cas, on a donc $\sigma = (i \quad i+1)$. Donc $(i \quad i+1)$ s'écrit comme un produit d'éléments de $\langle B \rangle$. Par le résultat précédent, on a $s$ aussi. Alors $\forall s \in \mathscr{S}_n, s \in \langle B \rangle$, donc $\mathscr{S}_n \in \langle B \rangle$.

Finalement, par double inclusion, on a $\mathscr{S}_n = \langle B \rangle$, donc $\boxed{\mathscr{S}_n \text{ est engendré par } B}$

## I.C -

### I.C.1 -

- réflexivité : $\forall \sigma \in \mathscr{S}_n$, $\exists Id_{\{1,2,\cdots,n\}} \in \mathscr{S}_n$, tel que $\sigma = Id_{\{1,2,\cdots,n\}} \circ \sigma \circ Id_{\{1,2,\cdots,n\}}$, donc $\sigma$ est conjuguée à elle-même($Id^{-1}_{\{1,2,\cdots,n\}} = Id_{\{1,2,\cdots,n\}}$).
- symétrie : on sait que $\forall \rho \in \mathscr{S}_n$, $\rho^{-1} \in \mathscr{S}_n^2$ car c'est une bijection, alors $\forall (\sigma, \sigma') \in \mathscr{S}_n^2$, $\sigma \mathcal{R} \sigma' \iff \exists \rho \in \mathscr{S}_n, \sigma = \rho \circ \sigma' \circ \rho^{-1} \iff \exists \rho' = \rho^{-1} \in \mathscr{S}_n, \sigma' = \rho' \circ \sigma \circ \rho'^{-1} \iff \sigma' \mathcal{R} \sigma$
- transitivité : $\forall (a, b, c) \in \mathscr{S}_n^3$, soient $a \mathcal{R} b$, $b \mathcal{R} c$, alors $\exists (\rho, \rho') \in \mathscr{S}_n^2$ tels que $a = \rho \circ b \circ \rho^{-1}$, $b = \rho' \circ c \circ \rho'^{-1}$. Alors $a = \rho \circ \rho' \circ c \circ \rho'^{-1} \circ \rho^{-1}$.
  Car $(\mathscr{S}_n, \circ)$ est un groupe, alors $\rho \circ \rho' \in \mathscr{S}_n$, et $(\rho \circ \rho')^{-1} = \rho'^{-1} \circ \rho^{-1} \in \mathscr{S}_n$.
  En notant $\phi = \rho \circ \rho'$, on a $\phi \in \mathscr{S}_n$, et $a = \phi \circ c \circ \phi^{-1}$. On a donc $a \mathcal{R} c$

Alors par les définitions, on a $\boxed{\mathcal{R} \text{ est une relation d'équivalence}}$

### I.C.2 -

Dans le cours, on a montré que $\forall \sigma \in \mathscr{S}_n$, soit $(a_1 \quad a_2 \cdots a_p) \in \mathscr{S}_n$ un p-cycle, alors $\sigma \circ (a_1 \quad a_2 \cdots a_p) \circ \sigma^{-1}$ est aussi un p-cycle. Soin $k \in \{1, 2, \cdots n\}$, $\alpha = (a_1 \quad a_2 \cdots a_k)$, $\beta = (b_1 \quad b_2 \cdots b_k)$ deux k-cycles.
On pose $\rho \in \mathscr{S}_n$ une bijection qui envoie $b_i$ à $a_i$ $\forall i \in \{1, 2, \cdots k\}$. Donc sa réciproque $\rho^{-1}$ est une bijection qui envoie $a_i$ à $b_i$ $\forall i \in \{1, 2, \cdots k\}$. On a donc

- $\forall i \in \{1, 2, \cdots, k-1\}$, on a $\alpha(a_i) = a_{i+1}$. Et on a $\rho \circ \beta \circ \rho^{-1}(a_i) = \rho \circ \beta(b_i) = \rho(b_{i+1}) = a_{i+1}$
- $\alpha(a_k) = a_1$, et $\rho \circ \beta \circ \rho^{-1}(a_k) = \rho \circ \beta(b_k) = \rho(b_1) = a_1$
- $\forall j \in \{1, 2, \cdots k\} \backslash \{a_1, \cdots, a_k, b_1, \cdots b_k\}$, $\alpha(j) = j$ et $\rho \circ \beta \circ \rho^{-1}(j) = \rho \circ \beta(j^{-1}) = \rho(j^{-1}) = j$, où $j^{-1}$ est l'image de $j$ par $\rho^{-1}$.(car $\rho, \rho^{-1}$) sont des bijections.

En tout cas, on a $\alpha = \rho \circ \beta \circ \rho^{-1}$, donc les deux k-cycles satisfont $\alpha \mathcal{R} \beta$. De plus, il n'y a pas de bijections entre deux cycles de cardinaux différents.
Finalemant, $\boxed{\text{la classe d'équivalence pour } \mathcal{R} \text{ est l'ensemble des k-cycles de } \mathscr{S}_n.}$

## I.D -

Dans le cours, on sait que $\forall s \in \mathscr{S}_n$, s se décompose comme un produits des k-cycles uniquement à l'ordre près de support distincts.

- sens indirect : si $(s, s^{'}) \in \mathscr{S}_n^2$ qui ont la même liste (dans l'ordre croissant) des longueurs de leurs cycles à supports disjoints. Soit $s = a_1 \circ \cdots \circ a_p$, $s^{'} = b_1 \circ \cdots \circ b_p$, avec $a_i$, $b_i$ les cycles de même longueur(on peut ranger les compositions de $s$ et $s^{'}$ car ils sont de support distincts, donc ils commutent).

  Pour chaque couple des cycles $(a_i, b_i)_{i \in \{1,2,\cdots,p\}}$ (de même longueur), car ils sont dans une même class d'équivalence il exist donc $\rho \in \mathscr{S}_n$ telle que $a_i = \rho \circ b_i \circ \rho^{-1}$. où $\rho$ la bijection qui envoie tous les supports de $a_i$ à ceux de $b_i$, $\forall i \in \{1, 2, \cdots, p\}$ (car les $a_i$ sont de supports disjoints, et $a_i$ est $b_i$ sont de même longueurs, la bijection $\rho$ est bien définie)

  On a donc $s = \rho^p \circ (b_1 \circ \cdots b_p) \circ \rho^{p^{-1}}$

  Car on a $\rho \in \mathscr{S}_n$, et donc $\rho^p \in \mathscr{S}_n$, $\rho^{p^{-1}} \in \mathscr{S}_n$ car $(\mathscr{S}_n, \circ)$ est un groupe. On a donc $s = \rho^p \circ s^{'} \circ \rho^{p^{-1}}$, d'où $s \mathcal{R} s^{'}$
- sens direct : Soit $(s, s^{'}) \in \mathscr{S}_n^2$, conjugué, alors $\exists \rho \in \mathscr{S}_n$ telle que $s = \rho \circ s^{'} \circ \rho^{-1}$. Soit $s^{'}$ se décompose somme $s^{'} = \beta_1 \circ \cdots \circ \beta_p$, $\forall i \in \{1, 2, \cdots, p\}$, on pose $\alpha_i = \rho \circ \beta_i \circ \rho^{-1}$, on a $\alpha_i \mathcal{R} \beta_i$, elles sont dans la même classe d'équivalence, donc elles ont la même longueur. De plus, les $\beta_i$ sont de supports disjoints, donc les $\alpha_i$ sont de supports disjoints car $\rho$ et $\rho^{-1}$ sont des bijections

  On a aussi $s = \rho \circ s^{'} \circ \rho^{-1} = \rho \circ \beta_1 \circ \cdots \circ \beta_p \circ \rho^{-1} = (\rho \circ \beta_1 \circ \rho^{-1}) \circ \cdots \circ (\rho \circ \beta_p \circ \rho^{-1}) = \alpha_1 \circ \cdots \circ \alpha_p$
  les $(a_i)_{i \in \{1,2,\cdots,p\}}$ sont bien une décomposition des cycles de $s$, ils sont de support disjoints(car $(b_i)_{i \in \{1,2,\cdots,p\}}$ le sont, et $\rho$ est une bijection)
  donc $s$ et $s^{'}$ ont la même liste (dans l'ordre croissant) des longueurs de leurs cycles à supports disjoints.

Finalement, on a $\forall (s, s^{'}) \in \mathscr{S}_n^2$, elles sont conjuguées si et seulement si
$\boxed{\text{elles ont la même liste (dans l'ordre croissant) des longueurs de leurs cycles à supports disjoints}}$