Étude de $\langle (i\ j), (1\ \ldots\ n)\rangle$

Ivan Lejeune

8 novembre 2024

Introduction

Dans ce document, nous allons étudier le sous-groupe de $\mathfrak{S}_n$ engendré par

$$\sigma = \langle (i\ j), (1\ \ldots\ n)\rangle$$

pour $1 \leq i < j \leq n$. On travaillera aussi "modulo n" où les indices iront de 1 à n et où $n + 1 = 1$.

Quelques résultats préliminaires

> **Lemme.** Soit $\sigma \in \mathfrak{S}_n$ et $i_1\ \ldots\ i_k$ une permutation de $1, \ldots, k$. Alors
>
> $$\sigma(i_1\ \ldots\ i_k)\sigma^{-1} = (\sigma(i_1)\ \ldots\ \sigma(i_k)).$$

> **Lemme.** Soit $\sigma \in \mathfrak{S}_n$ et $i\ j$ une transposition. Alors
>
> $$\langle \sigma, (i\ j)\rangle = \langle \sigma, (1\ k)\rangle$$
>
> où $k = j - i + 1$.

> **Lemme.** Soit $\sigma = (1\ \ldots\ n)$. Alors
>
> $$\sigma(1\ k)\sigma^{-1} = (2\ k+1)$$
>
> pour $k \in \mathbb{N}$.

Le choix de i et j

Le cas $j = i + 1$

Comme on l'a déjà vu en TD, si $i = 1, j = 2$, alors

$$\langle (1\ 2), (1\ \ldots\ n)\rangle = \mathfrak{S}_n.$$

Si on ne fixe pas i et on prend $j = i + 1$, on peut alors se ramener à ce cas en utilisant le lemme 2. Ainsi, un des premiers résultats que l'on peut obtenir est le suivant.

> **Théorème.** Soit $\sigma = \langle (i\ i+1), (1\ \ldots\ n)\rangle$ pour $1 \leq i < n$. Alors
>
> $$\sigma = \mathfrak{S}_n.$$

Démonstration. On a

$$\begin{aligned}\sigma &= \langle (i\ i+1), (1\ \ldots\ n)\rangle \\ &= \langle (1\ 2), (1\ \ldots\ n)\rangle \\ &= \mathfrak{S}_n.\end{aligned}$$

□

Le cas $j \neq i+1$

C'est ici que les choses se compliquent. On va essayer de trouver des conditions sur i et j pour que

$$\langle (i\ j), (1\ \dots\ n) \rangle = \mathfrak{S}_n.$$

La première chose qu'on peut faire est de se ramener à un cas plus simple en utilisant le lemme 2. On étudie alors

$$\sigma = \langle (1\ k), (1\ \dots\ n) \rangle$$

▷ Le premier point important à aborder est que pour engendrer l'ensemble des transpositions adjacentes (qui engendrent $\mathfrak{S}_n$), il suffit d'en engendrer une seule. En effet, on a

$$(i+1\ i+2) = (1\ \dots\ n)(i\ i+1)(1\ \dots\ n)^{-1}, \quad 1 \leq i < n.$$

De plus, on a un "décalage de l'écart entre les indices" qu'on peut effectuer. En effet, à partir de $(i\ j)$ et $(j\ k)$, on peut obtenir $(i\ k)$ en utilisant

$$(i\ j)(j\ k)(i\ j) = (i\ k).$$

Essayons maintenant de voir comment on peut obtenir une telle transposition à partir de $(1\ k)$.

Lemme. Soit $\sigma = \langle (1\ k+1), (1\ \dots\ n) \rangle$. Alors

$$k \wedge n = 1 \implies \sigma = \mathfrak{S}_n.$$

Démonstration. On peut énumérer certains éléments de σ :

$$\begin{aligned}
(1\ k+1) &\to (2\ k+2) \\
(2\ k+2) &\to (3\ k+3) \\
&\vdots \\
&\to (k+1\ 2k+1) \\
&\vdots \\
&\to (2k+1\ 3k+1) \\
&\vdots
\end{aligned}$$

On voit alors qu'à partir de $(1\ k+1)$, on peut obtenir

$$\{(1\ \lambda k+1) \mid \lambda \in \mathbb{N}\}.$$

D'autre part, si $k \wedge n = 1$, alors il existe $a, b \in \mathbb{Z}$ tels que

$$ak + bn = 1.$$

En particulier, pour $\lambda = a$, on a

$$\begin{aligned}
(1\ \lambda k+1) &= (1\ ak+1) \\
&= (1\ 1-bn+1) \\
&= (1\ 2).
\end{aligned}$$

On a donc $(1\ 2) \in \sigma$ et on peut obtenir toutes les transpositions adjacentes. □

On a donc une condition suffisante pour que $\langle (i\ j), (1\ \dots\ n) \rangle = \mathfrak{S}_n$.
On peut facilement vérifier que si $k \wedge n \neq 1$, alors on ne peut pas obtenir de transposition adjacente à partir de seulement $(1\ k+1)$ et $(1\ \dots\ n)$.
Cependant, il est difficile de prouver que c'est une condition nécessaire.

Conclusion

On a vu que si $j = i+1$, alors $\langle (i\ j), (1\ \dots\ n) \rangle = \mathfrak{S}_n$.
Si $j \neq i+1$, on a vu qu'il est possible d'obtenir $\mathfrak{S}_n$ si $k \wedge n = 1$.
Cependant, on n'a pas réussi à déterminer ce qu'il se passe si $k \wedge n \neq 1$.
Ainsi, on peut dire que

Théorème. Soit $\sigma = \langle (i\ j), (1\ \dots\ n) \rangle$ pour $1 \leq i < j \leq n$. Alors

$$\sigma = \mathfrak{S}_n$$

si $j = i + 1$ ou $(j - i + 1) \wedge n = 1$.

Remarque

Dans certains cas, on peut vérifier ce qui se passe pour $k \wedge n \neq 1$ mais cela est difficile pour des valeurs de n élevées.

Exemple

On peut vérifier que pour $n = 4$ et $k = 2$, on a

$$\begin{aligned}\langle (1\ 3), (1\ \dots\ 4) \rangle = \{&(1\ 3), (2\ 4),\\ &(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3),\\ &(1\ 2\ 3\ 4), (1\ 4\ 3\ 2)\} \neq \mathfrak{S}_4.\end{aligned}$$

Cela ne prouve pas que si $k \wedge n \neq 1$, alors $\langle (1\ k+1), (1\ \dots\ n) \rangle \neq \mathfrak{S}_n$ mais le montre pour $n = 4$.