Générateurs de $\mathfrak{S}_n$

Mohamed NASSIRI

Références :

Cours de mathématiques, tome 1 : Algèbre, Jean-Marie Arnaudiès et Henri Fraysse - p.174
Mathématiques L3 : Algèbre, Aviva Szpirglas - p.266
Algèbre 3 Oraux x-ens Poche, Serge Francinou, Hervé Gianella et Serge Nicolas - p.67

Recasage :

● ● ● ● ● 105 : Groupe des permutations d'un ensemble fini. Applications.
● ● ● ● ● 108 : Exemples de parties génératrices d'un groupe. Applications.

Résumé :

Ce développement se décompose en deux parties : on montre que les transpositions engendrent $\mathfrak{S}_n$ et puis que $n-1$ est le nombre minimal de transposition engendrant $\mathfrak{S}_n$.

Prérequis :

Groupe symétrique

Théorème : Soit $n \geq 2$.
(i) Les transpositions engendrent $\mathfrak{S}_n$.
(ii) L'ensemble $\{(1\ i), 1 \leq i \leq n\}$ engendre $\mathfrak{S}_n$.
(iii) Le nombre minimal de transpositions engendrant $\mathfrak{S}_n$ est $n-1$.

Démonstration.
(i) Par récurrence sur n.
Pour $n = 2$, c'est évident.
Supposons cela vrai au rang $n-1 \geq 2$, et montrons que cela est vrai au rang n.

- Si $\sigma(n) = n$, posons $s = \sigma_{|[\![1,n-1]\!]}$, d'où $s \in \mathfrak{S}_{n-1}$ et donc par hypothèse de récurrence, $s = t_1 t_2 ... t_k$.
Soit $\tau_i \in \mathfrak{S}_n$ tel que $\tau_i(n) = n$ et $\tau_{i|[\![1,n-1]\!]} = t_i$, alors $\tau_i \in \mathfrak{S}_n$ et on a bien $\sigma = \tau_1 \tau_2 ... \tau_k$

- Si $\sigma(n) = \alpha < n$. Soit τ la transposition de $\mathfrak{S}_n$ telle que $\tau(\alpha) = n$, $\tau(n) = \alpha$ et $\tau(j) = j$ pour $j \neq \{n, \alpha\}$. Alors $\tau\sigma(n) = n$. On se retrouve donc dans le cas précédent, et donc $\tau\sigma = \tau_1 \tau_2 ... \tau_k$ et par suite $\sigma = \tau^{-1}\tau_1\tau_2...\tau_k = \tau\tau_1\tau_2...\tau_k$

(ii) $\forall 1 \leq i, j \leq n$, on a $(i\ j) = (1\ i)(1\ j)(1\ i)$, d'où le résultat.

(iii) Ici la beauté de cette démonstration est qu'elle ne fait pas appel à l'algèbre mais à la théorie des graphes (que l'on se rassure, il n'y a rien à savoir de plus que les quelques lignes ci-dessous).

Donnons nous $\tau_1, ..., \tau_k$ transpositions, avec $k \leq n-2$. On va représenter les entiers de 1 à n par des points non alignés dans le plan. Si la transposition $(a\ b)$ apparaît dans la liste $\tau_1, ..., \tau_k$, on joint par un segment les points a et b. On obtient ce que l'on appelle un *graphe*. On aura besoin du

Nécessairement, pour que $\tau_1, ..., \tau_k$ engendrent $\mathfrak{S}_n$, il faut que l'on puisse passer de n'importe quel sommet $i \in [\![1, n]\!]$ à n'importe quel sommet $j \in [\![1, n]\!]$. Un tel graphe est dit *connexe*.

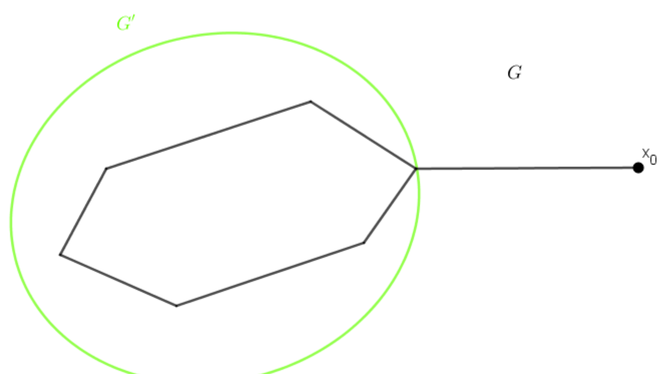
Lemme : Si un graphe G sur un ensemble E de cardinal $n \geq 2$ est connexe, alors il a au moins $n-1$ arêtes.

Démonstration du lemme.
Par récurrence sur n.
Pour $n = 2$, c'est évident.
Supposons cela vrai au rang $n-1$, et montrons que cela est vrai au rang n.

Soit un graphe G à n sommets.
Si x est un sommet, on note $\delta(x)$ le nombre d'arêtes qui arrivent en x. On a donc :

$$\sum_{x \in E} \delta(x) = 2a(G) \qquad (\bigstar)$$

où $a(G) =$ nombre d'arêtes de G.
La connexité de G impose $\delta(x) \geq 1$. Deux cas se présentent donc à nous :
- $\delta(x) \geq 2$, on a donc directement avec $(\bigstar)$ $a(G) \geq n$
- Il existe $x_0 \in E$ tel que $\delta(x_0) = 1$. En retirant x_0 et son arête, on obtient un nouveau graphe G' sur $E' = E \backslash \{x_0\}$



Par hypothèse de récurrence, on a $a(G') \geq |E'| - 1 = n-2$ et donc $a(G) = a(G') + 1 \geq n-2+1 = n-1$. $\square$

Remarques :

- Revenons
- Mises en garde sur le développement :
  Attention à ...