Soit $n \geqslant 2$. On note $[n]$ l'ensemble $\{1, \dots, n\}$ et $\mathfrak{T}_n$ l'ensemble des transpositions de $\mathfrak{S}_n$.

Définition 1. Pour tout sous-ensemble de transpositions $T \subset \mathfrak{T}_n$ on définit le graphe $G_T = ([n], T)$ où (i, j) est une arête de G_T si et seulement si $(i, j) \in T$. On définit sur $[n]$ la relation d'équivalence $i \sim_T j \iff$ il existe un chemin entre i et j dans G_T.

Théorème 2. Soit $T \subset \mathfrak{T}_n$. Alors T engendre $\mathfrak{S}_n$ si et seulement si G_T est connexe.

Démonstration. Supposons que T engendre $\mathfrak{S}_n$. Il est clair que les composantes connexes de G_T sont invariantes sous l'action de T :

$$\forall \tau \in T,\ \forall (i, j) \in [n]^2,\ i \sim_T j \iff \tau(i) \sim_T \tau(j).$$

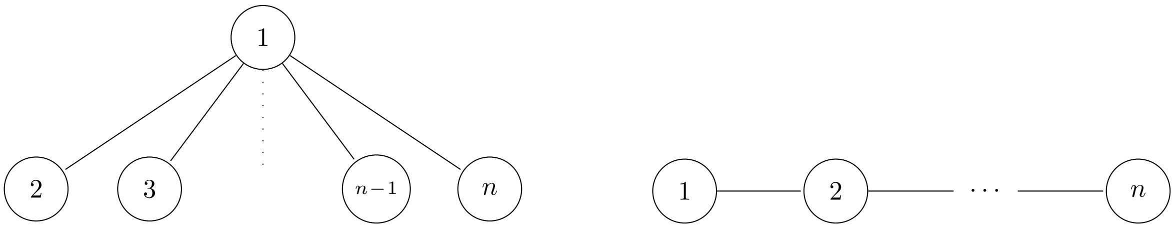
Par conséquent $\langle T \rangle = \mathfrak{S}_n$ fixe chaque composante connexe $C \in [n]/{\sim_T}$. Or la seule partie non vide de $[n]$ stable par tous les éléments de $\mathfrak{S}_n$ est $[n]$ elle-même. D'où $[n]/{\sim_T} = \{[n]\}$: G_T est connexe.

Réciproquement, supposons G_T connexe. Comme $\mathfrak{T}_n$ engendre $\mathfrak{S}_n$, il suffit de montrer que toute transposition est un produit d'éléments de T. Soit donc $\tau = (a, b) \in \mathfrak{T}_n$. Comme G_T est connexe il existe un chemin simple $a = i_0, \dots, i_p = b$ dans G_T : $(i_k, i_{k+1}) \in T$ pour tout $0 \leqslant k < p$. Or

$$(a, b) = (i_0, i_p) = (i_{p-1}, i_p) \cdots (i_2, i_3)(i_1, i_2)(i_0, i_1)(i_1, i_2) \cdots (i_{p-1}, i_p),$$

donc $(a, b) \in \langle T \rangle$. D'où $\langle T \rangle = \mathfrak{S}_n$. ∎

Exemples 3. Les ensembles de transpositions associés aux graphes suivants engendrent $\mathfrak{S}_n$.



(a) $T_1 = \{(1, 2), (1, 3), \dots, (1, n)\}$,

(b) $T_2 = \{(1, 2), (2, 3), \dots, (n-1, n)\}$.

Lemme 4. Pour tout graphe $G = (V, E)$, le nombre $\mathcal{C}(G)$ de composantes connexes de G vérifie

$$\mathcal{C}(G) \geqslant |V| - |E|. \qquad (\star)$$

Preuve. Par récurrence sur le nombre d'arêtes $m := |E|$ des graphes. Si $m = 0$, tout graphe $G = (V, \varnothing)$ a exactement $\mathcal{C}(G) = |V|$ composantes connexes. Supposons $m \geqslant 1$ et le résultat vrai pour $m - 1$ arêtes. Soient $G = (V, E)$ un graphe comprenant $|E| = m$ arêtes, et $e = (x, y) \in E$. Le graphe $G' = (V, E \setminus \{e\})$ a au plus une composante connexe de plus que G (selon que x et y restent ou non dans la même composante connexe), donc d'après l'hypothèse de récurrence $\mathcal{C}(G) \geqslant \mathcal{C}(G') - 1 \geqslant |V| - (|E| - 1) - 1 = |V| - |E|$. ∎

Corollaire 5. Soit $T \subseteq \mathfrak{T}_n$. Si T engendre $\mathfrak{S}_n$, alors $|T| \geqslant n - 1$.

Preuve. D'après le lemme 4 $|T| \geqslant n - \mathcal{C}(G_T)$. Or si T engendre $\mathfrak{S}_n$ alors $\mathcal{C}(G_T) = 1$ d'après le théorème 2 (G_T est connexe), donc $|T| \geqslant n - 1$. ∎

Remarque inutile. Il y a égalité dans $(\star)$ si et seulement si G est une forêt d'arbres.

Références. [RMS]

105 Groupe des permutations d'un ensemble fini. Applications.

108 Exemples de parties génératrices d'un groupe. Applications.

[RMS] Épreuves orales des concours d'entrée aux grandes écoles, exercice 212. *In Revue de la Filière Mathématiques*, numéro 110.

benjamin.dadoun@ens-cachan.fr