Les permutations

Séance Parimaths
Marc Abboud

14 avril 2018

Résumé

Ceci est la feuille de la séance de Parimaths du groupe débutant du 14 avril 2018. La séance portait sur les permutations. J'ai essayé de mettre une correction ou en tout cas une idée de correction pour les exercices que je n'ai pas eu le temps de faire pendant la séance. J'ai apporté quelques modifications par rapport au texte que j'avais donné pendant la séance, en particulier la preuve du théorème 2.2 était complètement fausse dans le papier de la séance et j'ai mis la preuve correcte dans ce papier.

1 Définitions et premiers résultats

Définition 1.1. Soient E, F des ensembles et $f : E \to F$ une fonction. On dit que f est *bijective* si pour tout $y \in F$, il existe un unique $x \in E$ tel que $f(x) = y$.

Remarque. Il faut voir qu'une bijection est une fonction que l'on peut "inverser" dans le sens où l'on peut définir $f^{-1} : F \to E$ tel que $f \circ f^{-1} = \mathrm{id}_F$ et $f^{-1} \circ f = \mathrm{id}_E$.

Exercice 1. Être bijectif est une propriété stable par composition. C'est à dire soient E, F, G des ensembles et $f : E \to F, g : F \to G$ des fonctions. Si f et g sont bijectives, alors $g \circ f$ l'est aussi.

Définition 1.2. Une bijection d'un ensemble dans lui-même est appelé une *permutation*. Si X est un ensemble, on note $\mathrm{Bij}(X)$ l'ensemble des permutations de X.

Exercice 2. Montrer que si on prend deux ensembles finis X et Y de même cardinal alors $\mathrm{Bij}(X)$ et $\mathrm{Bij}(Y)$ sont en bijections. [Indication : Numéroter les éléments de X et montrer que $\mathrm{Bij}(X)$ est en bijection avec $\mathrm{Bij}(\{1, .., n\})$].

Exemple. Il faut interpréter cet exercice comme le fait que $\mathrm{Bij}(\{1, 2, 3\}) = \mathrm{Bij}(\{a, b, c\})$.

Exercice 3. Donner le cardinal de $\mathrm{Bij}(\{1, ..., n\})$.

Définition 1.3. On appelle *groupe symétrique* l'ensemble des bijections de $\{1, ..., n\}$. on le note $\mathcal{S}_n$ (ou $\mathfrak{S}_n$ pour les plus courageux).

Exercice 4. Montrer que pour tout ensemble X, $\mathrm{Bij}(X)$ est un groupe pour la loi de composition de neutre id. Montrer que la bijection de l'exercice 2 est un (iso)morphisme de groupe.

Ainsi, dans la suite, lorsqu'on aura deux permutations α et β, on notera indifféremment $\alpha \circ \beta$ ou $\alpha\beta$ pour la composée de α et β. ATTENTION, le produit dans le groupe symétrique n'est pas commutatif pour $n \geq 3$! C'est à dire que de manière générale, $\alpha\beta \neq \beta\alpha$.

Il y a plusieurs façons de représenter une permutation. Une des façons classique est de l'écrire sous forme de tableau à deux lignes, la première étant $(1 \cdots n)$ et la deuxième l'image de la première ligne par σ. Plus précisément, soit $x_i \in [|1, n|]$ l'entier tel que $\sigma(i) = x_i$, on représente alors σ par le tableau :

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ x_1 & x_2 & \cdots & x_n \end{pmatrix} = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

Exercice 5. Décrire $\mathcal{S}_n$ pour $n = 1, 2, 3$.

Exercice 6. On définit $\varphi : \mathcal{S}_{n-1} \to \mathcal{S}_n$ l'application définie par

$$\varphi(\sigma) = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n-1) & n \end{pmatrix}$$

Montrer que φ est une bijection entre $\mathcal{S}_{n-1}$ et $\{\sigma \in \mathcal{S}_n \mid \sigma(n) = n\}$.

Montrer de plus que σ est un morphisme de groupe, c'est à dire $\varphi(\mathrm{id}_{\mathcal{S}_{n-1}}) = \mathrm{id}_{\mathcal{S}_n}$ et $\forall \tau, \sigma \in \mathcal{S}_{n-1}, \varphi(\sigma\tau) = \varphi(\sigma)\varphi(\tau)$.

Définition 1.4. Soit E un ensemble et $f : E \to E$ une fonction. On dit que $x \in E$ est un *point fixe* de f si $f(x) = x$.

2 Les cycles

Nous allons nous intéresser maintenant à une classe particulière de permutations : les cycles.

Définition 2.1. Soit n un entier naturel et $p \in [|2, n|]$. Un *p-cycle* est une permutation σ telle qu'il existe des entiers $x_1, ..., x_p$ tous distincts tel que $\forall 1 \leq i \leq p-1, \sigma(x_i) = x_{i+1}$, $\sigma(x_p) = x_1$ et pour tout $j \notin \{x_1, ..., x_p\}, \sigma(j) = j$.

L'ensemble $\{x_1, ..., x_p\}$ est appelé *le support* de σ.

On notera $\sigma = (x_1\ x_2\ \cdots\ x_p)$.

Remarque. Si $\gamma \in \mathcal{S}_n$ est un cycle, alors les éléments qui ne sont pas dans le support de σ sont exactement les points fixes de γ.

Remarque. Si on travaille dans $\mathcal{S}_3$, il faut comprendre que $(1\ 2\ 3) = (2\ 3\ 1)$.

Définition 2.2. Un 2-cycle est appelé *une transposition.*

Remarque. En particulier, une transposition τ vérifie $\tau^2 = \mathrm{id}$.

Exercice 7. Donner le nombre de p-cycles dans $\mathcal{S}_n$.

Exercice 8. Décrire l'inverse d'un cycle. Montrer que si γ est un p-cycle, alors $\gamma^p = \mathrm{id}$.

Exercice 9. Soit σ une permutation et $x_1, ..., x_p$ des entiers. Montrer que $\sigma(x_1\ x_2\ \cdots\ x_p)\sigma^{-1} = (\sigma(x_1)\ \sigma(x_2)\ \cdots\ \sigma(x_p))$.

Exercice 10. Montrer que deux cycles γ et α à support disjoints commutent, c'est à dire $\gamma \circ \alpha = \alpha \circ \gamma$.

Théorème 2.1. *Les transpositions engendrent $\mathcal{S}_n$. C'est à dire que toute permutation $\sigma \in \mathcal{S}_n$, il existe des transpositions $\tau_1, ..., \tau_s$ telles que $\sigma = \tau_1 \cdots \tau_s$.*

Exercice 11 (Preuve du théorème)**.** On procède par récurrence sur n.

1. Montrer le résultat pour $n = 1, n = 2, n = 3$.
2. On suppose le résultat vrai pour $\mathcal{S}_{n-1}$. Soit $\sigma \in \mathcal{S}_n$, en utilisant l'exercice 6, montrer que le résultat est vrai si $\sigma(n) = n$.
3. On prend $\sigma \in \mathcal{S}_n$ quelconque. Montrer qu'il existe une transposition $\tau \in \mathcal{S}_n$ tel que $\sigma' := \tau\sigma$ est telle que $\sigma'(n) = n$ et conclure.

Exercice 12 (Dur)**.** En déduire de ce théorème et du fait que deux transpositions sont conjuguées qu'il n'existe que deux morphismes de groupe $\mathcal{S}_n \to \mathbf{C}^*$. C'est le morphisme trivial et la signature.

Montrer que la signature d'un p-cycle est $(-1)^{p-1}$.

Remarque. L'ensemble des permutations de $\mathcal{S}_n$ de signature 1 est noté $\mathcal{A}_n$, on l'appelle le *groupe alterné*. Il a des propriétés très intéressantes qui nécessiteraient un cours complet sur les groupes pour pouvoir en parler.

Montrer en s'inspirant de la preuve de l'exercice 11 que pour $n \geq 3$, les 3-cycles engendrent $\mathcal{A}_n$.

Correction. Soit $\varphi : \mathcal{S}_n \to \mathbf{C}^*$ un morphisme de groupe. Il suffit de trouver la valeur de φ pour les transpositions, car si $\sigma = \tau_1 \cdots \tau_s$, alors $\varphi(\sigma) = \varphi(\tau_1) \cdots \varphi(\tau_s)$.

De plus, deux transpositions sont conjuguées entre elles. En effet, soient $(a\ b)$ et $(c\ d)$ deux transpositions. On pose $\sigma := (a\ c)(b\ d)$ et alors $\sigma(a\ b)\sigma^{-1} = (c\ d)$ par l'exercice 9. Donc $\varphi((a\ b)) = \varphi(\sigma)\varphi((c\ d))\varphi(\sigma)^{-1} = \varphi(c\ d)$. Donc toutes les transpositions ont même image par φ. Or, une transposition τ vérifie $\tau^2 = \mathrm{id}$ donc $\varphi(\tau)^2 = 1$. C'est à dire $\varphi(\tau) = 1$ ou $\varphi(\tau) = -1$. Dans le premier cas, on obtient le morphisme trivial qui envoie toutes les permutations sur 1 et dans le second cas, on obtient la signature.

Calculons la signature d'un p-cycle. on le fait par récurrence sur p, si $p = 2$ la formule est vraie par définition de la signature. Supposons la formule vraie pour les $(p-1)$- cycles.

Tout d'abord par l'exercice 9, on voit que tous les p-cycles ont la même signature. Il suffit donc de calculer la signature d'un p-cycle par exemple, le cycle $\gamma = (1\ \cdots\ p)$. On a $(1\ p)\gamma = (1\ \cdots\ p-1)$ qui est un $(p-1)$-cycle. Donc, par hypothèse de récurrence, en notant $s(\gamma)$ la signature de γ, il vient

$$(-1)s(\gamma) = (-1)^{p-2} \Rightarrow s(\gamma) = (-1)^{p-1}$$

La formule est donc vraie par récurrence.

Pour la deuxième question, on montre que le résultat est vrai pour $n = 3$ de manière triviale, puis on procède par récurrence.

Supposons le résultat vrai pour $\mathcal{A}_{n-1}$ avec $n - 1 \geq 3$, soit $\sigma \in \mathcal{A}_n$. Si $\sigma(n) = n$, on utilise l'exercice 6 pour conclure par récurrence. Si $\sigma(n) = k$ avec k différent de n, on prend i différent de n et k (ce qui est possible car $n \geq 4$). Alors $\sigma' := (i\ k\ n)\sigma$ est une permutation de signature

1 qui fixe n, il existe donc avec les notations de l'exercice 6 une permutation $\mu \in \mathbf{A}_{n-1}$ telle que $\varphi(\mu) = \sigma'$. Par hypothèse de récurrence, il existe des 3-cycles $\gamma_1, \cdots, \gamma_t \in S_{n-1}$ tels que $\mu = \gamma_1 \cdots \gamma_t$ et alors $\sigma' = \varphi(\mu) = \varphi(\gamma_1) \cdots \varphi(\gamma_t)$ qui est un produit de 3-cycles. Finalement, en multipliant par $(i\ k\ n)^2$ des deux côtés, on obtient

$$\sigma = (i\ k\ n)^2 \varphi(\gamma_1) \cdots \varphi(\gamma_t)$$

Et le résultat est vrai par récurrence.

Exercice 13 (Encore plus dur)**.** 1. Montrer que $(1\ 2), ..., (1\ n)$ engendrent $\mathcal{S}_n$.

2. On cherche à montrer que le nombre minimal de transpositions nécessaire pour engendrer $\mathcal{S}_n$ est $n-1$. Pour se faire, on prend une partie $\mathcal{T} = \{\tau_1, ..., \tau_s\}$ génératrice de $\mathcal{S}_n$ composée uniquement de transpositions.

   On définit Γ le graphe dont les sommets sont $V(\Gamma) = \{1, ..., n\}$ et on met une arête entre a et b si $(a\ b) \in \mathcal{T}$. Montrer que si $\mathcal{T}$ est génératrice, alors nécessairement le graphe est connexe. C'est à dire qu'entre deux points du graphe il y a toujours un chemin qui les relie.

3. On cherche à montrer qu'un graphe connexe à n sommets a au moins $n-1$ arêtes. Soit $x \in V(\Gamma)$, on note $\delta(x)$ la valence de x, c'est à dire le nombre d'arêtes qui partent de x. Montrer que
$$\sum_{x \in V(\Gamma)} \delta(x) = 2a(\Gamma)$$
   avec $a(\Gamma)$ le nombre d'arêtes de Γ.

4. Conclure par récurrence, selon qu'il existe $x_0 \in V(\Gamma)$ tel que $\delta(x_0) = 1$ ou bien $\forall x \in V(\Gamma), \delta(x) \geq 2$.

5. Conclure.

Théorème 2.2. *Toute permutation $\sigma \in \mathcal{S}_n$ se décompose en produit de cycles à support disjoints. C'est à dire qu'il existe $\gamma_1, ..., \gamma_s$ des cycles (de longueurs potentiellement différentes) tels que $\sigma = \gamma_1 \cdots \gamma_s$. En particulier, ces cycles commutent et cette décomposition est unique.*

Démonstration. Soit $\sigma \in \mathcal{S}_n$, on utilise le fait suivant : soit $x \in [|1, n|]$, alors l'ensemble $\left\{\sigma^i(x) \;\middle|\; i \in \mathbf{N}\right\}$ est fini.

Exercice 14. Soit $N = \text{Card}\left\{\sigma^i(x) \;\middle|\; i \in \mathbf{N}\right\}$, montrer que $\sigma^N(x) = x$. [Indication : Montrer que l'application $n \in \mathbf{N} \mapsto \sigma^n(x)$ n'est pas injective]. Montrer que lorsqu'on restreint σ à $\{\sigma^n(x) \mid n \geq 0\}$ on obtient le N-cycle $(x\ \sigma(x)\ \cdots\ \sigma^{N-1}(x))$.

On procède alors à l'algorithme suivant :

— Si $\sigma = \text{id}$, il n'y a rien à faire. Sinon, soit i_0 le plus petit entier tel que $\sigma(i_0) \neq i_0$ (en particulier, $\sigma(i_0) > i_0$), on note $N_0 = \text{Card}\left\{\sigma^j(i_0) \;\middle|\; j \geq 0\right\}$ et on définit le cycle $\gamma_0 := (i_0\ \sigma(i_0)\ \sigma^2(i_0)\ \cdots\ \sigma^{N_0-1}(i_0))$.

— On définit ensuite $i_1 = \min[|i_0, n|] \setminus (\text{supp}\,\gamma_0 \cup \{\text{points fixes de } \sigma\})$ si cet ensemble est non vide, sinon on arrête. On a $i_1 > i_0$ et note $\gamma_1 = (i_1\ \sigma(i_1)\ \cdots\ \sigma^{N_1-1}(i_1))$ avec $N_1 := \text{Card}\,\{\sigma^n(i_1) \mid n \geq 0\}$..

— Supposons avoir construit une suite strictement croissante $i_0 < i_1 < .... < i_t$ et des cycles $\gamma_0, ..., \gamma_t$. On pose $i_{t+1} = \min[|i_t, n|] \setminus (\operatorname{supp}\gamma_0 \cup \cdots \cup \operatorname{supp}\gamma_t \cup \{ \text{ points fixes de } \sigma\})$ si cet ensemble est non vide et on pose $\gamma_{t+1} = (i_{t+1}\ \sigma(i_{t+1})\ \cdots\ \sigma^{N_{t+1}-1}(i_{t+1}))$, on arrête sinon.

1. Montrer que l'algorithme termine.
2. Montrer que les cycles $\gamma_0, \ldots, \gamma_s$ construits sont à supports disjoints.
3. Montrer que $\sigma = \gamma_0 \cdots \gamma_s$ et que cette décomposition est unique.

□

Correction. Pour la première partie, on définit $L := \min\left\{k > 0 \;\middle|\; \sigma^k(x) = x\right\}$ et on va montrer que $L = N$. Tout d'abord L existe, car l'application $n \in \mathbf{N} \to [|1, n|]$ ne peut pas être injective car $\mathbf{N}$ est infini. Donc il existe $k < l$ tel que $\sigma^l(x) = \sigma^k(x)$ et alors $\sigma^{l-k}(x) = x$ et $l - k > 0$. Donc l'ensemble $\left\{k > 0 \;\middle|\; \sigma^k(x) = x\right\}$ est non vide et on peut prendre L son minimum.

Enfin, on montre que si $0 \geq k < l \geq L-1$, alors $\sigma^l(x) \neq \sigma^k(x)$, sinon on aurait $\sigma^{l-k}(x) = x$ avec $0 < l - k < L$ et c'est absurde par minimalité de L. Donc on a $L \leq N$. De plus, soit $m \geq 0$, on écrit la division euclidienne de m par L : $m = qL + r$ avec $0 \geq r \geq L - 1$. Et on obtient

$$\sigma^m(x) = \sigma^{qL+r}(x) = \sigma^r(\sigma^{qL}(x)) = \sigma^r(x)$$

Finalement, $\left\{\sigma^k(x) \;\middle|\; k \geq 0\right\} = \{\sigma^r(x) \mid 0 \leq r \leq L - 1\}$. Donc $N = L$, et on a bien que σ restreint à $\left\{\sigma^k(x) \;\middle|\; k \geq 0\right\}$ est le cycle $(x\ \sigma(x)\ \cdots\ \sigma^{L-1}(x))$, car $\sigma^L(x) = x$.

Pour les questions suivantes :

1. On crée une suite strictement croissante d'entiers naturels qui sont inférieurs à n, cette suite ne peut donc pas être infinie et l'algorithme termine.
2. Supposons qu'il existe $k < j$ tel que γ_j et γ_k ne soit pas à supports disjoints. Soit $x \in \operatorname{supp}\gamma_j \cap \operatorname{supp}\gamma_k$. Par construction, il existe d_j et d_k tels que $i_k = \sigma^{d_k}(x)$et $i_j = \sigma^{d_k}(x)$, mais alors on peut trouver un entier N tel que $\sigma^n(i_k) = i_j$, cela voudrait dire que $i_j \in \operatorname{supp}\gamma_k$ et c'est absurde par la définition de i_j.
   Les supports construits sont donc bien à supports disjoints.
3. Soit $x \in \mathcal{S}_n$, si x est fixe pour σ, x n'appartient au support de aucun des γ_i, et donc $\gamma_1 \cdots \gamma_s(x) = x$. Sinon, soit γ_k l'unique cycle dont le support contient x.Par construction, il existe l tel que $x = \sigma^l(i_k)$ et alors $\sigma(x) = \sigma^{l+1}(i_k) = \gamma_k(x)$. Maintenant, comme les cycles construits sont à supports disjoints on a que $\gamma_1 \cdots \gamma_s(x) = \gamma_k(x) = \sigma(x)$. On a bien, $\sigma = \gamma_1 \cdots \gamma_s$.

Exercice 15. Appliquer cet algorithme à la permutation suivante :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 7 & 5 & 3 & 1 & 2 & 8 & 6 \end{pmatrix}$$

3 Structure du groupe symétrique

Définition 3.1. On dit que $\sigma \in \mathcal{S}_n$ est conjuguée à $\tau \in \mathcal{S}_n$ s'il existe une permutation $\gamma \in \mathcal{S}_n$ telle que

$$\sigma = \gamma\tau\gamma^{-1}$$

Définition 3.2. Soit n un entier. Une *partition* de n est la donnée d'entiers $0 < x_0 \geq x_1 \leq x_2 \leq \cdots \leq x_p$ tels que $x_0 + x_1 + \cdots + x_p = n$.

On note $p(n)$ le nombre de partition de l'entier n.

Exercice 16.
1. Montrer qu'une permutation est conjuguée à elle-même.
2. Montrer que σ est conjuguée à τ si et seulement si τ est conjuguée à σ.
3. Montrer que si σ est conjuguée à τ et que τ est conjuguée à μ, alors σ est conjuguée à μ.
4. Pour $\sigma \in \mathcal{S}_n$, on note $C_\sigma = \{\tau \in \mathcal{S}_n \mid \sigma \text{ est conjuguée à } \tau\}$. Montrer que si $C_\sigma \cap C_\tau \neq \emptyset$, alors σ est conjuguée à τ et en fait $C_\sigma = C_\tau$. On dit que C_σ est une *classe de conjugaison.*
5. (Dur) Montrer que $\text{Card}\,\{C_\sigma \mid \sigma \in \mathcal{S}_n\} = p(n)$. [Indication : décomposer σ en cycle à support disjoints et utiliser l'exercice 9 pour étudier la classe de conjugaison de σ].

Correction.

4. Soit $\mu \in C_\sigma \cap C_\tau$, alors σ est conjuguée à μ et μ est conjuguée à τ par 3., on a que σ est conjuguée à τ, donc $C_\sigma = C_\tau$.

5. Soit $\sigma \in \mathcal{S}_n$, on décompose σ en cycles à supports dijoints : $\sigma = \gamma_1 \cdots \gamma_s$ et alors pour tout $\tau \in \mathcal{S}_n$, on a

$$\tau\sigma\tau^{-1} = (\tau\gamma_1\tau^{-1})(\tau\gamma_2\tau^{-1}) \cdots (\tau\gamma_s\tau^{-1})$$

Donc on voit que lorsqu'on conjugue σ par une autre permutation, le nombre de p-cycles qui apparaissent dans sa décomposition à supports disjoints reste le même pour tout $2 \geq p \geq n$. Il faut montrer que la réciproque est vraie, c'est à dire que deux permutations qui ont le même nombre de p-cycles dans leur décomposition en cycle à supports disjoints pour tout $2 \geq p \geq n$ sont conjuguées. (Pour le voir, faîtes des cas particuliers. Commencez par des cycles, puis faîtes le pour un produit de deux cycles, puis pour un produit de trois cycles et essayez de généraliser).

Une fois que l'on a fait ça, on écrit $\sigma = \gamma_1 \cdots \gamma_s$ en produit de cycles à support disjoints et on suppose que les γ_i sont rangés en ordre croissant de taille de support (c'est à dire $\#\,\text{supp}(\gamma_i) \leq \#\,\text{supp}(\gamma_{i+1})$). On pose $x_0(\sigma) = \#\,\{\text{points fixes de } \sigma\}$ et pour tout $1 \geq i \geq s, x_i(\sigma) = \#\,\text{supp}(\gamma_i)$. On vérifie que $(x_0(\sigma), ..., x_s(\sigma)$ est une partition de n. Cette partition ne dépend que de la classe de conjugaison de σ (si on avait pris τ conjuguée à σ, on aurait eu la même partition) et à toute partition de n, on peut associer une permutation qui nous redonne cette partition.

Ce procédé est donc bijectif et on a le résultat.

Théorème 3.1 (Théorème de Cayley)**.** *Soit G un groupe fini de cardinal n, montrer qu'il existe un morphisme de groupe injectif $G \hookrightarrow \mathcal{S}_n$.*

Démonstration. Soit $g \in G$, on voit que g permute les éléments de G par translation. Plus précisément, on définit $\varphi_g : G \to G$ définie par $\forall x \in G, \varphi_g(x) = gx$.

Exercice 17.
1. Montrer que φ_g est une bijection.
2. Montrer que $g \in G \mapsto \varphi_g \in \text{Bij}(G)$ est un morphisme de groupe injectif. C'est à dire montrer que l'application est injective, que $\varphi_{e_G} = \text{id}$ et que $\forall g, h \in G, \varphi_{gh} = \varphi_g \circ \varphi_h$.
3. En déduire le résultat.

□

Correction. 1. On a $\varphi_g \circ \varphi_{g^{-1}} = \varphi_{g^{-1}} \circ \varphi_g = \mathrm{id}$ donc φ_g est bien une bijection.

2. On a $\varphi_g(e_G) = g$ donc $g \neq g' \Rightarrow \varphi_g \neq \varphi_{g'}$ et $g \mapsto \varphi_g$ est bien une application injective. Le fait que c'est un morphisme de groupe est clairement vrai.
3. $\mathrm{Bij}(G)$ est isomorphe à S_n car G est de cardinal n, donc on a le résultat.

Théorème 3.2. *Soit $n \geq 3$, le centre de $\mathcal{S}_n$ est trivial. C'est à dire que l'ensemble*

$$\{\sigma \in \mathcal{S}_n \mid \forall \tau \in \mathcal{S}_n, \sigma\tau = \tau\sigma\}$$

est réduit à $\{\mathrm{id}\}$.

Exercice 18 (preuve du théorème)**.** Soit $\tau \in \mathcal{S}_n$ une permutation qui commute avec toutes les autres permutations.

1. Soit $i \in [|1, n|]$. Montrer qu'il existe une permutation $\sigma \in \mathcal{S}_n$ telle que i est l'unique point fixe de σ.
2. En utilisant le fait que τ et σ commute, montrer que $\tau(i) = i$.
3. Conclure.

Correction. 1. Il suffit de prendre la permutation $\sigma = (1\ 2\ \cdots i-1\ i+1\ \cdots\ n)$. Le seul point fixe de σ est i.

2. On a $\sigma\tau = \tau\sigma$, en particulier, $\sigma(\tau(i)) = \tau(\sigma(i))$, mais $\sigma(i) = i$, donc on obtient

$$\sigma(\tau(i)) = \tau(i)$$

Donc $\tau(i)$ est un point fixe de σ, et le seul point fixe de σ est i, ainsi $\tau(i) = i$.

3. On peut faire ce procédé pour n'importe quel i, donc pour tout i, $\tau(i) = i$. Finalement, $\tau = \mathrm{id}$.