# DM 28 : un corrigé

## Partie I : Définition

**1°)** Il s'agit d'une question de cours.
Si $f, g \in S(E)$, alors $f \circ g$ est encore une bijection de $E$ dans $E$, donc la composition est une loi interne sur $S(E)$.
Soit $f, g, h \in S(E)$ et $x \in E$.
Alors $[f \circ (g \circ h)](x) = f((g \circ h)(x)) = f(g(h(x))) = (f \circ g)(h(x)) = [(f \circ g) \circ h](x)$, donc $f \circ (g \circ h) = (f \circ g) \circ h$ : la loi de composition est associative.
Pour tout $f \in S(E)$, $f \circ Id_E = Id_E \circ f = f$, donc $Id_E$ est un élément neutre.
Pour tout $f \in S(E)$, $f$ est bijective, donc on dispose de sa bijection réciproque notée $f^{-1}$. Alors $f \circ f^{-1} = f^{-1} \circ f = Id_E$, donc tout élément de $S(E)$ possède un symétrique.
En conclusion, $(S(E), \circ)$ est bien un groupe.

**2°)** Soit $x, y, z \in E$.
Par convention, $f^0 = Id_E$ (car $Id_E$ est l'élément neutre de $S(E)$), donc $x = f^0(x)$, ce qui prouve que $x \ R_f \ x$. Ainsi, $R_f$ est réflexive.
Supposons que $x \ R_f \ y$. Il existe $k \in \mathbb{Z}$ tel que $y = f^k(x)$.
Alors $f^{-k}(y) = (f^k)^{-1} \circ f^k(x) = x$, donc $y \ R_f \ x$, ce qui prouve que $R_f$ est symétrique.
Supposons que $x \ R_f \ y$ et $y \ R_f \ z$. Il existe $k, h \in \mathbb{Z}$ tels que $y = f^k(x)$ et $z = f^h(y)$.
Alors $z = f^h \circ f^k(x) = f^{h+k}(x)$, donc $x \ R_f \ z$. $R_f$ est donc transitive.
En conclusion, on a montré que $R_f$ est une relation d'équivalence sur $E$.

**3°)** Avec des notations usuelles, $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 2 & 7 & 5 & 1 & 3 & 8 & 6 \end{pmatrix}$. Sa décomposition en produit de cycles à supports disjoints est donc $f = (1\ 4\ 5) \circ (3\ 7\ 8\ 6)$.
2 est un point fixe de $f$, donc l'orbite de 2 est $\overline{2} = \{2\}$.
Les itérés successifs de 1 sont $1, 4, 5, 1 \ldots$, donc $\overline{1} = \{1, 4, 5\}$.
De même, $\overline{3} = \{3, 7, 8, 6\}$.
Ces trois ensembles constituent déjà une partition de $\mathbb{N}_8$, donc on dispose de toutes les orbites de $f$.

**4°)** Soit $c \in E/R_f$. Il existe $x \in E$ tel que $c = \overline{x} = \{f^k(x) \ / \ k \in \mathbb{Z}\}$.
Ainsi $c = \bigcup_{k \in \mathbb{Z}} \{f^k(x)\}$ est une réunion dénombrable d'ensembles finis, donc d'après le cours, c'est un ensemble au plus dénombrable.

Supposons que $E/R_f$ est au plus dénombrable. Alors $E = \bigcup_{c\in E/R_f} c$ est une union au plus dénombrable d'ensembles au plus dénombrables, donc $E$ est aussi au plus dénombrable, ce qui est faux. Ainsi, $E/R_f$ est infini non dénombrable.

**5°)** Soit $n \in \mathbb{N}^*$. Notons $R(n)$ l'assertion suivante : pour toute famille $(F_1, \dots, F_n)$ de $n$ ensembles finis, $|\bigcup_{k=1}^{n} F_k| = \sum_{A\in\mathcal{P}(\mathbb{N}_n)\setminus\{\emptyset\}} (-1)^{|A|+1} |\bigcap_{i\in A} F_i|$.
Lorsque $n = 1$, $\mathcal{P}(\mathbb{N}_1) \setminus \{\emptyset\} = \{1\}$, donc $R(1)$ se résume à $|F_1| = |F_1|$.
Lorsque $n = 2$, $R(2)$ est une formule du cours : $|F_1 \cup F_2| = |F_1| + |F_2| - |F_1 \cap F_2|$.
Supposons $R(n)$ (et $n \geq 2$) et montrons $R(n+1)$. Soit $(F_1, \dots, F_{n+1})$ une famille de $n+1$ ensembles finis. $|\bigcup_{k=1}^{n+1} F_k| = |F_{n+1} \cup \bigcup_{k=1}^{n} F_k|$ donc d'après $R(2)$,
$|\bigcup_{k=1}^{n+1} F_k| = |\bigcup_{k=1}^{n} F_k| + |F_{n+1}| - |F_{n+1} \cap \bigcup_{k=1}^{n} F_k| = |\bigcup_{k=1}^{n} F_k| + |F_{n+1}| - |\bigcup_{k=1}^{n}(F_{n+1} \cap F_k)|$,
donc d'après $R(n)$ appliqué deux fois,

$$\begin{aligned}
|\bigcup_{k=1}^{n+1} F_k| &= \sum_{A\in\mathcal{P}(\mathbb{N}_n)\setminus\{\emptyset\}} (-1)^{|A|+1} |\bigcap_{i\in A} F_i| + |F_{n+1}| - \sum_{A\in\mathcal{P}(\mathbb{N}_n)\setminus\{\emptyset\}} (-1)^{|A|+1} |\bigcap_{i\in A}(F_i \cap F_{n+1})| \\
&= \sum_{\substack{A\in\mathcal{P}(\mathbb{N}_{n+1})\setminus\{\emptyset\} \\ n+1\notin A}} (-1)^{|A|+1} |\bigcap_{i\in A} F_i| + \sum_{\substack{A\in\mathcal{P}(\mathbb{N}_{n+1})\setminus\{\emptyset\} \\ n+1\in A}} (-1)^{|A|+1} |\bigcap_{i\in A} F_i| \\
&= \sum_{A\in\mathcal{P}(\mathbb{N}_{n+1})\setminus\{\emptyset\}} (-1)^{|A|+1} |\bigcap_{i\in A} F_i|,
\end{aligned}$$

ce qui prouve $R(n+1)$.

**6°)** Soit $\sigma \in S_n$. Si $\sigma$ possède une orbite de cardinal inférieur à 1, il existe $x \in \mathbb{N}_n$ tel que $\{\sigma^k(x) \ / \ k \in \mathbb{Z}\} = \overline{x} = \{x\}$. Alors $\sigma(x) = x$, donc $\sigma$ possède un point fixe. Réciproquement, si $\sigma$ possède un point fixe $x \in \mathbb{N}_n$, alors $\overline{x} = \{x\}$. Ainsi, on cherche à dénombrer l'ensemble des permutations de $S_n$ sans point fixe, c'est-à-dire l'ensemble noté $D$ des dérangements de $\mathbb{N}_n$.

Si l'on note $F_k = \{\sigma \in \mathcal{S}_n / \sigma(k) = k\}$, pour tout $k \in \mathbb{N}_n$, alors $D = S_n \setminus \bigcup_{k=1}^{n} F_k$.

D'après la formule du crible, $|\bigcup_{k=1}^{n} F_k| = \sum_{A\in\mathcal{P}(\mathbb{N}_n)\setminus\{\emptyset\}} (-1)^{|A|+1} |\bigcap_{i\in A} F_i|$.
Soit $A \in \mathcal{P}(\mathbb{N}_n) \setminus \{\emptyset\}$. Pour construire un élément quelconque de $\bigcap_{i\in A} F_i = \{\sigma \in S_n \ / \ \forall i \in A, \ \sigma(i) = i\}$, il suffit de choisir la bijection $\sigma|_{\mathbb{N}_n\setminus A}^{\mathbb{N}_n\setminus A}$, donc $|\bigcap_{i\in A} F_i| = (n - |A|)!$. Alors la formule du crible devient :
$|\bigcup_{k=1}^{n} F_k| = \sum_{A\in\mathcal{P}(\mathbb{N}_n)\setminus\{\emptyset\}} (-1)^{|A|+1}(n - |A|)!$, puis par sommation par paquets :

$$|\bigcup_{k=1}^{n} F_k| = \sum_{k=1}^{n} \sum_{\substack{A\subset\mathbb{N}_n \\ |A|=k}} (-1)^{k+1}(n-k)! = \sum_{k=1}^{n} \binom{n}{k} (-1)^{k+1}(n-k)!.$$

On en déduit que $d_n = |D| = n! + \sum_{k=1}^{n} \frac{n!}{k!}(-1)^k = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}$.

Ainsi, $\frac{d_n}{n!} = \sum_{k=0}^{n} \frac{(-1)^k}{k!} \underset{n\to+\infty}{\longrightarrow} \frac{1}{e}$, d'après le cours.

## Partie II : Décomposition en produit de transpositions

**7°)** Soit $c$ un cycle de longueur $\ell \in \{2, \dots, n\}$. Il existe $x_1, \dots, x_\ell \in \mathbb{N}_n$, deux à deux distincts tels que $c = (x_1\ x_2\ \cdots\ x_\ell)$. Alors l'orbite de $x_1$ est égal au support de $c$, c'est-à-dire à $S = \{x_1, \dots, x_\ell\}$ et pour tout $x \in \mathbb{N}_n \setminus S$, $c(x) = x$, donc l'orbite de $x$ est $\{x\}$. Il y a donc $n - \ell$ orbites réduites à un singleton et une unique orbite de cardinal supérieur à 2, égale à $S$. Ainsi, $O(c) = n - \ell + 1$.

**8°)** Soit $\sigma \in S_n$. D'après le cours, il existe des cycles $c_1, \dots, c_d$, où $d \in \mathbb{N}$, tels que $\sigma = c_1 \circ c_2 \cdots \circ c_d$, les cycles $c_1, \dots, c_d$ étant de plus à supports disjoints.
Soit $x \in \mathbb{N}_n$. Si $x$ n'appartient à aucun support de ces cycles, alors $\sigma(x) = x$ et l'orbite de $x$ est réduite au singleton $\{x\}$.
Sinon, il existe $i \in \mathbb{N}_d$ tel que $x$ est dans le support de $c_i$. On sait alors que $\sigma$ et $c_i$ coïncident sur le support de $c_i$, donc $\{\sigma^k(x)\ /\ k \in \mathbb{Z}\} = \{c_i^k(x)\ /\ k \in \mathbb{Z}\}$, ce qui est égal au support de $c_i$. Ainsi, les orbites de $\sigma$ sont exactement les supports des cycles $c_i$ et les singletons $\{x\}$, où $x$ décrit $\mathbb{N}_n$ privé de la réunion des supports des cycles.
En notant $\ell_1, \dots, \ell_d$ les longueurs respectives des cycles $c_1, \dots, c_d$, on en déduit que $O(\sigma) = d + (n - \ell_1 - \cdots - \ell_d)$.
Soit $i \in \mathbb{N}_d$. Notons $c_i = (x_1\ x_2\ \cdots\ x_{\ell_i})$. On sait alors que
$c_i = (x_1\ x_2) \circ (x_2\ x_3) \circ \cdots \circ (x_{\ell_i - 1}\ x_{\ell_i})$, ce que l'on peut vérifier en calculant les images par ces deux permutations de $x_1, x_2, \dots, x_{\ell_i}$ et de $x \in \mathbb{N}_n \setminus \{x_1, x_2, \dots, x_{\ell_i}\}$.
Ainsi, on parvient à décomposer $c_i$ en un produit de $\ell_i - 1$ transpositions.
Ceci permet de décomposer $\sigma = c_1 \circ \cdots \circ c_d$ en un produit de $T = \sum_{i=1}^{d} (\ell_i - 1)$ transpositions. Or $T = n - (n - T) = n - (n + d - \sum_{i=1}^{d} \ell_i) = n - O(\sigma)$.

**9°)**
**a)** pour tout $h \in \mathbb{N}_k$, on peut écrire $c = (x_h\ x_{h+1}\ \cdots x_k\ x_1\ \cdots\ x_{h-1})$, donc on peut supposer que $a = x_1$.
De même, on peut supposer que $b = y_1$.
**b)** On calcule que

$$\begin{aligned} c \circ d \circ (a\ b) &= (x_1\ x_2\ \cdots\ x_k) \circ (y_1\ y_2\ \cdots\ y_h) \circ (x_1\ y_1) \\ &= (x_1\ y_2\ \cdots\ y_h\ y_1\ x_2\ \cdots\ x_k), \end{aligned}$$

en vérifiant la dernière égalité en prenant les images par ces deux permutations de $x_1, \dots, x_k$, puis de $y_1, \dots, y_h$ et de $x \in \mathbb{N}_n \setminus [\{x_1, \dots, x_k\} \cup \{y_1, \dots, y_h\}]$.
**c)** D'après la question 7, $O(c \circ d \circ (a\ b)) = n - (h+k) + 1$. De plus, d'après le début de la question 8, $O(c \circ d) = n - (h+k) + 2$. Ainsi, $O(c \circ d \circ (a\ b)) = O(c \circ d) - 1$.

**10°)** Notons encore $c = (x_1\ x_2\ \cdots\ x_\ell)$.
Comme en question 9.a, on peut supposer que $a = x_1$.
De plus, il existe $h \in \{2, \dots, \ell\}$ tel que $b = x_h$.
$\diamond$ Premier cas : on suppose que $c = (a\ b)$. Alors $c \circ (a\ b) = Id_{\mathbb{N}_n}$.
Pour les autres cas, on se place donc sous l'hypothèse que $\ell \geq 3$.
$\diamond$ Second cas : on suppose que $h = \ell$. Alors on calcule que
$c \circ (a\ b) = (x_1\ x_2\ \cdots\ x_\ell) \circ (x_1\ x_\ell) = (x_2\ x_3\ \cdots\ x_\ell)$ : on vérifie la dernière égalité en prenant les images par ces deux permutations de $x_1, \dots, x_\ell$ et de $x \in \mathbb{N}_n \setminus \{x_1, \dots, x_\ell\}$.
$\diamond$ Troisième cas : on suppose que $h = 2$. Alors on calcule que
$c \circ (a\ b) = (x_1\ x_2\ \cdots\ x_\ell) \circ (x_1\ x_2) = (x_1\ x_3\ x_4\ \cdots\ x_\ell)$
$\diamond$ Quatrième cas : on suppose que $3 \leq h \leq \ell - 1$. Alors on calcule que
$c \circ (a\ b) = (x_1\ x_2\ \cdots\ x_\ell) \circ (x_1\ x_h) = (x_1\ x_{h+1}\ x_{h+2}\ \cdots\ x_\ell) \circ (x_2\ x_3\ \cdots\ x_h)$.
Ainsi, dans tous les cas, lorsqu'on remplace $c$ par $c \circ (a\ b)$, l'orbite correspondant au support de $c$ est scindée en 2 orbites exactement (éventuellement réduites à un singleton), les autres orbites (des singletons) n'étant pas modifiées.
Ainsi, $O(c \circ (a\ b)) = O(c) + 1$.

**11°)** Soit $\sigma \in S_n$ et $\tau = (a\ b)$ une transposition.
Il existe des cycles à supports disjoints $c_1, \dots, c_d$ tels que $\sigma = c_1 \circ \cdots \circ c_d$.
$\diamond$ Premier cas : On suppose que $a$ et $b$ ne sont dans aucun des supports des cycles $c_i$. Alors $\sigma \circ (a\ b)$ se décompose en produit de cycles à supports disjoints sous la forme $\sigma \circ (a\ b) = c_1 \circ \cdots \circ c_d \circ (a\ b)$. Ainsi, en passant de $\sigma$ à $\sigma \circ (a\ b)$, les deux orbites $\{a\}$ et $\{b\}$ de $\sigma$ sont regroupées en une seule orbite égale à $\{a, b\}$. Les autres orbites ne sont pas modifiées, donc $O(\sigma \circ (a\ b)) = O(\sigma) - 1$.
$\diamond$ Second cas : On suppose qu'il existe $i \in \mathbb{N}_d$ tel que $a$ et $b$ appartiennent au support de $c_i$. D'après le cours, des cycles à supports disjoints commutent entre eux, donc $\sigma \circ (a\ b) = (c_i \circ (a\ b)) \circ \prod_{\substack{j=1 \\ j \neq i}}^{d} c_j$. Alors, d'après la question 10, en passant de $\sigma$ à $\sigma \circ (a\ b)$, l'orbite de $c_i$ est scindée en 2 orbites, les autres orbites n'étant pas modifiées. Ainsi, $O(\sigma \circ (a\ b)) = O(\sigma) + 1$.
$\diamond$ Troisième cas : il existe $i, j \in \mathbb{N}_d$ avec $i \neq j$ tels que $a$ est dans le support de $c_i$ et $b$ dans le support de $c_j$. Alors on peut écrire $\sigma \circ (a\ b) = (c_i \circ c_j \circ (a\ b)) \circ \prod_{\substack{k=1 \\ k \notin \{i,j\}}}^{d} c_k$, donc d'après la question 9.b, en passant de $\sigma$ à $\sigma \circ (a\ b)$, les deux orbites correspondant aux supports de $c_i$ et $c_j$ sont regroupées en une seule orbite, les autres orbites n'étant pas modifées. Ainsi, $O(\sigma \circ (a\ b)) = O(\sigma) - 1$.

$\diamond$ Dernier cas : il reste le cas où par exemple $a$ appartient au support de l'un des cycles, que l'on notera $c_i$, alors que $b$ n'appartient à aucun des supports des cycles. Alors $\sigma(a\ b) = \Big(\prod_{\substack{k=1\\k\neq i}}^{d} c_k\Big) \circ c_i \circ (a\ b)$. On peut supposer que $c_i = (x_1\ x_2\ \cdots\ x_\ell)$ où $a = x_1$. Alors on calcule que $c_i \circ (a\ b) = (b\ x_2\ \cdots\ x_\ell\ x_1)$, et on en déduit que $O(\sigma \circ (a\ b)) = O(\sigma) - 1$.
Dans tous les cas, on a bien montré que $O(\sigma \circ \tau) = O(\sigma) + \varepsilon$, où $\varepsilon \in \{-1, 1\}$.

**12°)** Supposons que $\sigma = \prod_{i=1}^{k} \tau_i$, où $k \in \mathbb{N}$ et où les $\tau_i$ sont des transpositions. Alors $\sigma \circ \tau_k \circ \tau_{k-1} \circ \cdots \circ \tau_1 = Id_{\mathbb{N}_n}$, or d'après la question 11, pour tout $\sigma \in S_n$ et pour toute transposition $\tau$, modulo 2, $O(\sigma \circ \tau) \equiv O(\sigma) + 1$. Ainsi, toujours modulo 2, on en déduit par récurrence sur $k$ que $n = O(Id_{\mathbb{N}_n}) \equiv O(\sigma \circ \tau_k \circ \tau_{k-1} \circ \cdots \circ \tau_1) \equiv O(\sigma) + k$. Ainsi, $k \equiv n - O(\sigma)$, ce qu'il fallait démontrer.
Ceci justifie la définition de la signature de $\sigma$, en tant que parité du nombre de transpositions intervenant dans une décomposition de $\sigma$ en produit de transpositions. On voit de plus que la signature de $\sigma$ est égale à $(-1)^{n-O(\sigma)}$.

**13°)** Supposons à nouveau que $\sigma = \prod_{i=1}^{k} \tau_i$, où $k \in \mathbb{N}$ et où les $\tau_i$ sont des transpositions. Alors $\sigma \circ \tau_k \circ \tau_{k-1} \circ \cdots \circ \tau_1 = Id_{\mathbb{N}_n}$, or d'après la question 11, pour tout $\sigma \in S_n$ et pour toute transposition $\tau$, $O(\sigma \circ \tau) \leq O(\sigma) + 1$. On en déduit par récurrence sur $k$ que $n = O(Id_{\mathbb{N}_n}) \equiv O(\sigma \circ \tau_k \circ \tau_{k-1} \circ \cdots \circ \tau_1) \leq O(\sigma) + k$. Ainsi, $k \geq n - O(\sigma)$, ce qu'il fallait démontrer.
On a donc prouvé que toute permutation de $S_n$ se décompose en un produit de transpositions et que le nombre minimal de transpositions intervenant dans un tel produit est exactement $n - O(\sigma)$.

## Partie III : Décomposition en produit d'involutions

**14°)** $\diamond$ Soit $x \in O$. On a $x\ R_f\ f(x)$, par définition de $R_f$, donc $f(x) \in \overline{x} = O$. Ainsi, l'application $f|_O^O$ est bien définie. C'est une injection en tant que restriction d'une application injective. De plus, si $y \in O$, alors $y\ R_f\ f^{-1}(y)$, donc $f^{-1}(y) \in O$ et $f(f^{-1}(y)) = y$. Ainsi, $y = f|_O^O(x)$ en posant $x = f^{-1}(y)$, ce qui prouve que $f|_O^O$ est surjective. Ceci démontre que $f|_O^O$ est une bijection.
$\diamond$ On suppose que $P_{f|_O^O}$ est vraie pour toute orbite $O$ de $f$, c'est-à-dire que, pour toute orbite $O$ de $f$, il existe deux involutions de $O$ dans $O$, notées $g_O$ et $h_O$ telles que $f|_O^O = g_O \circ h_O$.
$R_f$ est une relation d'équivalence, donc les orbites de $f$ constituent une partition de $E$. Si $x \in E$, il existe donc une unique orbite $O$ de $f$ telle que $x \in O$. On pose alors $g(x) = g_O(x)$ et $h(x) = h_O(x)$. On définit ainsi deux applications $g$ et $h$ de $E$ dans $E$.

Soit $x \in E$. Notons encore $O$ l'unique orbite qui contient $x$. Alors $g(x) \in O$, donc $g(g(x)) = g_O(g(x)) = g_O(g_O(x)) = x$, car $g_O$ est une involution.
De même, $(g \circ h)(x) = g_O(h_O(x)) = f|_O^O(x) = f(x)$.
Ceci démontre que $g \circ g = Id_E$ et que $g \circ h = f$. On démontre de même que $h \circ h = Id_E$, ce qui conclut.

**15°)** Il existe $x \in E$ tel que $O = \overline{x} = \{f^n(x) \ / \ n \in \mathbb{Z}\}$.
$\diamond$ Notons $\varphi$ l'application de $\mathbb{Z}$ dans $O$ définie par $\varphi(n) = f^n(x)$ pour tout $n \in \mathbb{Z}$.
$\varphi$ est surjective car $O = \{f^n(x) \ / \ n \in \mathbb{Z}\}$.
Soit $n, m \in \mathbb{Z}$ tels que $m < n$. Supposons que $\varphi(n) = \varphi(m)$. Alors $f^{n-m}(x) = x$ et $n - m \geq 1$. Posons $q = n - m$.
Soit $h \in \mathbb{Z}$. Par division euclidienne, $h = qd + r$, où $d \in \mathbb{Z}$ et $0 \leq r < q$. Ainsi, $f^h(x) = f^r((f^q)^d(x)) = f^r(x)$, donc $O \subset \{f^r(x) \ / \ 0 \leq r < q\}$ ce qui est faux car $O$ est supposée infinie. Ainsi, $\varphi(n) \neq \varphi(m)$, donc $\varphi$ est injective.
On a prouvé que $\varphi$ est une bijection de $\mathbb{Z}$ dans $O$.
Soit $n \in \mathbb{Z}$. Alors $\varphi^{-1} \circ f|_O^O \circ \varphi(n) = \varphi^{-1}(f(f^n(x))) = \varphi^{-1}(f^{n+1}(x)) = n + 1$, donc $\varphi^{-1} \circ f|_O^O \circ \varphi = S$, où $S$ désigne l'application de $\mathbb{Z}$ dans $\mathbb{Z}$ qui à $n$ associe $n + 1$.
$\diamond$ Posons $\begin{array}{rccc} g : & \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ & i & \longmapsto & 1 - i \end{array}$ et $\begin{array}{rccc} h : & \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ & i & \longmapsto & -i \end{array}$.
Pour tout $i \in \mathbb{Z}$, on vérifie que $(g \circ g)(i) = 1 - (1 - i) = i$ et $(h \circ h)(i) = i$, donc $g$ et $h$ sont des involutions de $\mathbb{Z}$. De plus, pour tout $i \in \mathbb{Z}$, $(g \circ h)(i) = 1 - (-i) = i + 1 = S(i)$, donc $S = g \circ h$.
On en déduit que $f|_O^O = \varphi \circ S \circ \varphi^{-1} = (\varphi g \varphi^{-1})(\varphi h \varphi^{-1})$, ce qui conclut car il est simple de vérifier que $\varphi g \varphi^{-1}$ et $\varphi h \varphi^{-1}$ sont deux involutions de $O$ dans $O$.

**16°)** D'après la question 14, il reste à montrer $P_{f|_O^O}$ lorsque $O$ est une orbite finie. Notons $n$ son cardinal.
$\diamond$ Il existe $x \in E$ tel que $O = \overline{x} = \{f^k(x) \ / \ k \in \mathbb{Z}\}$.
Posons $A = \{k \in \mathbb{N}^* \ / \ f^k(x) = x\}$.
$O$ est finie, donc l'application $k \longmapsto f^k(x)$, de $\mathbb{Z}$ dans $O$, n'est pas injective. Ainsi, il existe $h, k \in \mathbb{Z}$ avec $h < k$ tel que $f^h(x) = f^k(x)$. En composant par $f^{-h}$, on en déduit que $f^{k-h}(x) = x$ et $k - h \in \mathbb{N}^*$, donc $A$ est une partie non vide de $\mathbb{N}^*$. Ainsi, elle possède un minimum, que l'on notera $m$.
Soit $k \in \mathbb{Z}$. Par division euclidienne, on a $k = qm + r$, où $q \in \mathbb{Z}$ et $0 \leq r < m$. Alors $f^k(x) = f^r((f^m)^q(x)) = f^r(x)$, donc $O \subset \{f^r(x) \ / \ 0 \leq r < m\}$. L'inclusion réciproque est évidente.
Soit $h, k \in \{0, \ldots, m-1\}$ tel que $h \leq k$ et $f^h(x) = f^k(x)$. Alors $f^{k-h}(x) = x$. Si $h \neq k$, alors $k - h \in A$, donc $k - h \geq \min(A) = m$, ce qui est faux. Ainsi $h = k$.
Par contraposition, on a montré que pour tout $h, k \in \{0, \ldots, m-1\}$,
$h \neq k \Longrightarrow f^h(x) \neq f^k(x)$, donc $O$ est de cardinal $m$.
On en déduit que $m = n$ et que les éléments deux à deux distincts de $O$ sont exactement $x, f(x), \ldots, f^{n-1}(x)$.
$\diamond$ Notons $\varphi$ l'application de $\mathbb{Z}/n\mathbb{Z}$ dans $O$ définie par $\varphi(\overline{k}) = f^k(x)$ pour tout $k \in \mathbb{Z}$.

Commençons par montrer que $\varphi$ est correctement définie : soit $h, k \in \mathbb{Z}$ tel que $\overline{h} = \overline{k}$. Alors il existe $q \in \mathbb{Z}$ tel que $h = qn + k$, donc $f^h(x) = f^k((f^n)^q(x)) = f^k(x)$. Ainsi la quantité $f^k(x)$ ne dépend que de $\overline{k}$, ce qu'il fallait démontrer.
$\varphi$ est surjective car $O = \{f^k(x) \ / \ k \in \mathbb{Z}\}$.
Soit $h, k \in \mathbb{Z}$ tels que $\varphi(k) = \varphi(h)$. Alors $f^{k-h}(x) = x$.
Par division euclidienne, on a $k - h = qn + r$ où $0 \leq r < n$. Alors $x = f^{k-h}(x) = f^r(x)$, donc si $r \neq 0$, $r \in A$, puis $r \geq \min(A) = n$, ce qui est faux. Ainsi, $r = 0$ puis $\overline{k} = \overline{h}$. Ceci prouve que $\varphi$ est injective.
On a prouvé que $\varphi$ est une bijection de $\mathbb{Z}/n\mathbb{Z}$ dans $O$.
Soit $k \in \mathbb{Z}$. Alors $\varphi^{-1} \circ f|_O^O \circ \varphi(\overline{k}) = \varphi^{-1}(f(f^k(x))) = \varphi^{-1}(f^{k+1}(x)) = \overline{k} + \overline{1}$, donc $\varphi^{-1} \circ f|_O^O \circ \varphi = S$, où $S$ désigne l'application de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$ qui à $\overline{k}$ associe $\overline{k} + \overline{1}$.
$\diamond$ Posons $\begin{array}{rccc} g : & \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ & \overline{k} & \longmapsto & \overline{1} - \overline{k} \end{array}$ et $\begin{array}{rccc} h : & \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ & \overline{k} & \longmapsto & -\overline{k} \end{array}$.
Pour tout $k \in \mathbb{Z}$, on vérifie que $(g \circ g)(\overline{k}) = \overline{1} - (\overline{1} - \overline{k}) = \overline{k}$ et $(h \circ h)(\overline{k}) = \overline{k}$, donc $g$ et $h$ sont des involutions de $\mathbb{Z}/n\mathbb{Z}$.
De plus, pour tout $k \in \mathbb{Z}$, $(g \circ h)(\overline{k}) = \overline{1} - (-\overline{k}) = \overline{k} + \overline{1} = S(\overline{k})$, donc $S = g \circ h$.
On en déduit que $f|_O^O = \varphi \circ S \circ \varphi^{-1} = (\varphi g \varphi^{-1})(\varphi h \varphi^{-1})$, ce qui conclut car il est simple de vérifier que $\varphi g \varphi^{-1}$ et $\varphi h \varphi^{-1}$ sont deux involutions de $O$ dans $O$.