

# DM 14. Corrigé

## 1 Actions de groupes

### 1.1 Exemples

1°) a) Dans cette question, on pose donc  $h \times x = hx$  pour tout  $h \in H$  et  $x \in G$ .

Pour tout  $x \in G$ ,  $1_H \times x = 1_G x = x$

et pour tout  $g, h \in H$  et  $x \in G$ ,  $g \times (h \times x) = g(hx) = (gh)x = (gh) \times x$ ,

donc il s'agit bien d'une action du groupe  $H$  sur l'ensemble  $G$ .

b) Dans cette question, on pose  $h \times g = hgh^{-1}$  pour tout  $h \in H$  et  $g \in G$ .

On vérifie que pour tout  $g \in G$ ,  $1_H \times g = g$  et que, pour tout  $h, h' \in H$  et  $g \in G$ ,

$h \times (h' \times g) = h \times (h'gh'^{-1}) = hh'gh'^{-1}h^{-1} = (hh') \times g$ , donc il s'agit bien également d'une action du groupe  $H$  sur l'ensemble  $G$ .

2°) Supposons que l'on dispose d'une action du groupe  $G$  sur un ensemble  $E$ , que l'on

note  $G \times E \longrightarrow E$   
 $(g, x) \longmapsto g \times x$ .

Pour tout  $g \in G$  et  $X \in \mathcal{P}(E)$ , posons  $g \times X = \{g \times x / x \in X\}$ .

Ainsi, pour tout  $X \in \mathcal{P}(E)$ ,  $1_G \times X = X$ .

Soit  $g, h \in G$  et  $X \in \mathcal{P}(E)$ .  $g \times (h \times X) = g \times \{h \times x / x \in X\} = \{g \times (h \times x) / x \in X\}$ ,

donc  $g \times (h \times X) = (gh) \times X$ . On a donc bien ainsi défini une opération du groupe  $G$  sur l'ensemble des parties de  $E$ .

3°) Pour tout  $x \in E$ ,  $1_{\mathcal{S}(E)} \times x = Id_E(x) = x$ .

Soit  $\sigma, \sigma' \in \mathcal{S}(E)$  et  $x \in E$ .  $\sigma \times (\sigma' \times x) = \sigma \times (\sigma'(x)) = \sigma(\sigma'(x)) = (\sigma \circ \sigma')(x) = (\sigma \sigma') \times x$ .

Il s'agit donc bien d'une action du groupe  $\mathcal{S}(E)$  sur l'ensemble  $E$ .

### 1.2 Théorème de Cayley

4°) Soit  $g \in G$ . Pour tout  $x \in E$ ,

$\gamma_g \circ \gamma_{g^{-1}}(x) = \gamma_g(g^{-1} \times x) = g \times (g^{-1} \times x) = (gg^{-1}) \times x = x$ , donc  $\gamma_g \circ \gamma_{g^{-1}} = Id_E$ . De même on vérifie que  $\gamma_{g^{-1}} \circ \gamma_g = Id_E$ .

Ainsi,  $\gamma_g$  est une bijection dont l'application réciproque est  $\gamma_{g^{-1}}$ .

---

5°) Soit  $g, h \in G$ . Pour tout  $x \in E$ ,  $\gamma_h \circ \gamma_g(x) = h(gx) = (hg)x = \gamma_{hg}(x)$ . Ainsi,  $\gamma_h \circ \gamma_g = \gamma_{hg}$ , ce qui prouve que l'application  $\gamma: G \rightarrow \mathcal{S}(E)$  est un morphisme de groupes.

6°) Soit  $G$  un groupe fini de cardinal  $n \in \mathbb{N}^*$ .

Faisons opérer  $G$  sur lui-même par translation à gauche (cf question 1.a).

La question précédente fournit alors un morphisme  $\gamma$  de  $G$  dans  $\mathcal{S}(G)$ .

Montrons qu'il est injectif.

Soit  $g \in G$  tel que  $\gamma_g = Id_G$ . Ainsi, pour tout  $h \in G$ ,  $h = Id_G(h) = \gamma_g(h) = gh$ . En particulier, pour  $h = 1_G$ , on obtient que  $g = 1_G$ . Donc  $\text{Ker}(\gamma) = \{1_G\}$  et  $\gamma$  est un morphisme injectif.

Ainsi  $G$  est isomorphe à  $\gamma(G)$  qui est un sous-groupe de  $\mathcal{S}(G)$ .

$G$  est de cardinal  $n$ , donc il existe une bijection  $b$  de  $G$  dans  $\{1, \dots, n\}$ .

Notons  $\varphi: \mathcal{S}(G) \rightarrow \mathcal{S}_n$   
 $\sigma \mapsto b\sigma b^{-1}$ .

Pour tout  $\sigma, \sigma' \in \mathcal{S}(G)$ ,  $\varphi(\sigma\sigma') = b\sigma\sigma'b^{-1} = (b\sigma b^{-1})(b\sigma'b^{-1}) = \varphi(\sigma)\varphi(\sigma')$ , donc  $\varphi$  est un morphisme de groupes.

C'est même un isomorphisme, dont l'isomorphisme réciproque est  $\mathcal{S}_n \rightarrow \mathcal{S}(G)$   
 $\sigma \mapsto b^{-1}\sigma b$ .

$\varphi \circ \gamma$  est alors un morphisme injectif de  $G$  dans  $\mathcal{S}_n$ , donc  $G$  est isomorphe à  $(\varphi \circ \gamma)(G)$  qui est bien un sous-groupe de  $\mathcal{S}_n$ .

### 1.3 Théorème de Lagrange

7°) Soit  $x \in E$ .  $x = 1_G \times x$ , donc  $x R x$  :  $R$  est réflexive.

Soit  $x, y \in E$  tel que  $x R y$ . Il existe  $g \in G$  tel que  $y = g \times x$ .

Alors  $g^{-1} \times y = g^{-1} \times (g \times x) = x$ , donc  $y R x$ . Ceci montre que  $R$  est symétrique.

Soit  $x, y, z \in E$  tels que  $x R y$  et  $y R z$ . Il existe  $g, g' \in G$  tels que  $y = g \times x$  et  $z = g' \times y$ . Alors  $z = (g'g) \times x$ , donc  $x R z$ . Ceci montre que  $R$  est transitive.

Ainsi,  $R$  est bien une relation d'équivalence sur  $E$ .

Soit  $a, b \in E$ .  $b \in \bar{a} \iff [\exists g \in G, b = ga]$ , donc  $\bar{a} = \{ga/g \in G\}$ . On pourra noter  $\bar{a} = G \times a$ .

8°) Faisons opérer  $H$  sur  $G$  par translation à gauche (cf question 1.a).

Les orbites des éléments de  $G$  sous cette action constituent une partition de  $G$ , donc

(en notant  $|X|$  le cardinal d'un ensemble  $X$ ),  $|G| = \sum_{c \in G/R} |c|$ .

Soit  $c \in G/R$ . D'après la question précédente, il existe  $g \in G$

tel que  $c = Hg = \{hg/h \in H\}$ .

L'application  $H \rightarrow Hg$   
 $h \mapsto hg$  est une bijection dont la bijection réciproque est

$Hg \rightarrow H$   
 $x \mapsto xg^{-1}$ , donc  $|c| = |Hg| = |H|$ .

On en déduit que  $|G| = |G/R| \times |H|$ , ce qui permet de conclure.

---

## 2 Le groupe symétrique de degré $n$

### 2.1 Décomposition en produit de cycles

**9°)** Notons  $G = Gr(\sigma)$  : c'est le sous-groupe de  $\mathcal{S}_n$  engendré par  $\sigma$ .

On fait opérer  $G$  sur  $\mathbb{N}_n$  selon la question 3, en convenant que, pour tout  $s \in G$ , pour tout  $x \in \{1, \dots, n\}$ ,  $s \times x = s(x)$ .

Alors, pour  $a \in \{1, \dots, n\}$ ,  $\mathcal{O}(a) = \{s \times a / s \in G\}$ , donc c'est l'orbite de  $a$  sous l'action de  $G$ . D'après la question 7, ces orbites sont les classes d'équivalence d'une relation d'équivalence sur  $\mathbb{N}_n$ , donc elles constituent une partition de  $\mathbb{N}_n$ .

**10°)** Notons  $A = \{a_1, \dots, a_p\}$ . Soit  $a \in \{1, \dots, n\}$ .

Si  $a \notin A$ , alors  $\sigma(a) = a$ , donc  $\mathcal{O}(a) = \{a\}$ .

Sinon, il existe  $i \in \{1, \dots, p\}$  tel que  $a = a_i$ .

Convenons que, pour tout  $k \in \mathbb{Z}$  et  $j \in \{1, \dots, p\}$ ,  $a_k = a_j$

si et seulement si  $k \equiv j [p]$ . On peut alors montrer par récurrence sur  $k \in \mathbb{N}$  que, pour tout  $j \in \{1, \dots, p\}$ ,  $\sigma^k(a_j) = a_{j+k}$  et  $\sigma^{-k}(a_j) = a_{j-k}$ .

On en déduit que  $\mathcal{O}(a) = A$ .

En conclusion, les orbites du cycle  $(a_1 a_2 \dots a_p)$  sont  $A = \{a_1, \dots, a_p\}$  et les singletons  $\{a\}$  où  $a \in \mathbb{N}_n \setminus A$ .

**11°) a)** Notons  $p$  l'ordre de  $\sigma$  dans le groupe  $\mathcal{S}_n$ . Alors  $p \in \mathbb{N}^*$  et  $\sigma^p = Id_{\mathbb{N}_n}$ . En particulier,  $\sigma^p(a) = a$ , donc  $\{k \in \mathbb{N}^* / \sigma^k(a) = a\}$  est non vide, or c'est une partie de  $\mathbb{N}$ , donc elle possède un minimum, noté  $\ell$ .

**b)** Posons  $H = \{a, \sigma(a), \dots, \sigma^{\ell-1}(a)\}$ .

◇ Montrons d'abord que  $H = \mathcal{O}$ .

L'inclusion  $H \subset \mathcal{O}$  est claire. Réciproquement, soit  $k \in \mathbb{Z}$ . Par division euclidienne, on peut écrire que  $k = \ell q + r$  avec  $0 \leq r < \ell$ .

$\sigma^\ell(a) = a$ , donc par récurrence on en déduit que  $\sigma^{q\ell}(a) = a$ .

Ainsi,  $\sigma^k(a) = \sigma^r(\sigma^{q\ell}(a)) = \sigma^r(a) \in H$ .

◇ Soit maintenant  $i, j \in \{0, \dots, \ell - 1\}$  tels que  $i < j$ .

Il s'agit de montrer que  $\sigma^i(a) \neq \sigma^j(a)$ .

Raisonnons par l'absurde en supposant que  $\sigma^i(a) = \sigma^j(a)$ . Alors  $\sigma^{j-i}(a) = a$

et  $1 \leq j - i \leq \ell - 1$ . C'est impossible car  $\ell = \min(\{k \in \mathbb{N}^* / \sigma^k(a) = a\})$ .

**c)** D'après la question b),  $\ell = |H| = |\mathcal{O}| = p$ . Ainsi  $\sigma^p(a) = \sigma^\ell(a) = a$ , par construction de  $\ell$ .

**d)** Soit  $a, b \in \mathcal{O}$ . Il existe  $k \in \{0, \dots, p - 1\}$  tel que  $b = \sigma^k(a)$ .

Soit  $h \in \mathbb{N}$  :  $c_{\sigma^h(a)} = (\sigma^h(a) \sigma^{h+1}(a) \dots \sigma^{h+p-1}(a))$ , or  $\sigma^p(a) = a$ ,

donc  $\sigma^{p+h}(a) = \sigma^h(a)$ . Ainsi,  $c_{\sigma^h(a)} = (\sigma^{h+1}(a) \sigma^{h+2}(a) \dots \sigma^{h+p}(a)) = c_{\sigma^{h+1}(a)}$ .

La suite  $(c_{\sigma^h(a)})_{h \in \mathbb{N}}$  est donc constante. Ainsi,  $c_a = c_{\sigma^0(a)} = c_{\sigma^k(a)} = c_b$ .

**12°) a)** Commençons par caractériser les points fixes de  $\sigma$  :

Soit  $x \in \mathbb{N}_n$ . S'il existe  $i \in \mathbb{N}_r$  tel que  $x \in S_i$ , alors pour tout  $j \in \mathbb{N}_r \setminus \{i\}$ ,  $x \notin S_j$ , donc  $c_j(x) = x$ . On en déduit que  $\sigma(x) = c_i(x) \neq x$ .

---

Si  $x \notin \bigcup_{i=1}^r S_i$ , alors  $\sigma(x) = x$ .

Ainsi, l'ensemble  $\{x \in \mathbb{N}_n / \sigma(x) = x\}$  des points fixes de  $\sigma$  est égal à  $\mathbb{N}_n \setminus \bigcup_{i=1}^r S_i$ .

Raisonnons maintenant par double inclusion :

◇ Soit  $\mathcal{O}$  une orbite pour  $\sigma$  qui possède au moins 2 éléments.

Soit  $a \in \mathcal{O}$ . Ainsi,  $\mathcal{O} = \mathcal{O}(a)$  et  $c_{\mathcal{O}} = (a \ \sigma(a) \ \dots \ \sigma^{p-1}(a))$  où  $p = |\mathcal{O}| \geq 2$ .

Or  $\sigma(a) \neq a$  car  $p \geq 2$ , donc il existe  $i \in \{1, \dots, r\}$  tel que  $a \in S_i$ . Alors  $\sigma(a) = c_i(a)$ .

De plus,  $c_i(a) \in S_i$ , donc on a aussi  $\sigma(c_i(a)) = c_i(c_i(a))$ , c'est-à-dire  $\sigma^2(a) = c_i^2(a)$ . Par récurrence sur  $k$ , on peut ainsi montrer que, pour tout  $k \in \mathbb{N}$ ,  $\sigma^k(a) = c_i^k(a)$ .

Ainsi,  $c_i^p(a) = a$  et  $c_i = c_{\mathcal{O}}$ .

On a donc montré que  $\{c_{\mathcal{O}} / \mathcal{O}$  est une orbite pour  $\sigma$  telle que  $|\mathcal{O}| \geq 2\} \subset \{c_1, \dots, c_r\}$ .

◇ Réciproquement, soit  $i \in \mathbb{N}_r$ . Choisissons un élément  $a$  de  $S_i$ . Ainsi,  $\sigma(a) \neq a$ , donc  $\mathcal{O}(a)$  possède au moins deux éléments.

$a \in S_i$ , donc on a encore, pour tout  $k \in \mathbb{N}$ ,  $c_i^k(a) = \sigma^k(a)$ , donc à nouveau,  $c_i = c_{\mathcal{O}(a)}$ .

**b)** En reprenant les notations du a), on a vu que pour tout  $x \in S_i$ , lorsque  $j \neq i$ ,

$c_j(x) = x$ , donc  $\left(\prod_{k=1}^r c_k\right)(x) = c_i(x)$ , même si l'on modifie l'ordre des facteurs de ce

produit. Ainsi, un produit de cycles à supports disjoints est toujours commutatif.

La question a) prouve la partie unicité du théorème.

Pour démontrer l'existence, notons  $\mathcal{O}_1, \dots, \mathcal{O}_r$  les orbites pour  $\sigma$  qui possèdent au

moins deux éléments. Il s'agit de montrer que  $\sigma = \prod_{i=1}^r c_{\mathcal{O}_i}$ , ce qui est bien un produit

de cycles dont les supports sont deux à deux disjoints (d'après la question 9).

Posons  $s = \prod_{i=1}^r c_{\mathcal{O}_i}$ . Soit  $a \in \mathbb{N}_n$ .

Premier cas : Supposons que  $a \notin \bigcup_{i=1}^r \mathcal{O}_i$ . Alors  $\mathcal{O}(a)$  est un singleton, donc  $\sigma(a) = a$ .

On a aussi  $s(a) = a$ , donc dans ce cas,  $\sigma(a) = s(a)$ .

Second cas : Supposons qu'il existe  $j \in \mathbb{N}_r$  tel que  $a \in \mathcal{O}_j$ .

Alors  $s(a) = c_{\mathcal{O}_j}(a) = \sigma(a)$  d'après la question 11.d).

Ainsi, pour tout  $a \in \mathbb{N}_n$ ,  $s(a) = \sigma(a)$ , donc  $\sigma = s = \prod_{i=1}^r c_{\mathcal{O}_i}$  ce qui termine la

démonstration du théorème.

## 2.2 Signature d'une permutation

**13°)** Pour tout  $f \in \mathcal{F}(\mathbb{Q}^n, \mathbb{Q})$ ,  $Id_{\mathbb{N}_n} \times f = f$ .

Soit  $f \in \mathcal{F}(\mathbb{Q}^n, \mathbb{Q})$  et  $\sigma, \sigma' \in \mathcal{S}_n$ . Soit  $(x_1, \dots, x_n) \in \mathbb{Q}^n$ .

$[\sigma \times (\sigma' \times f)](x_1, \dots, x_n) = (\sigma' \times f)(x_{\sigma(1)}, \dots, x_{\sigma(n)})$ .

Posons  $(x_{\sigma(1)}, \dots, x_{\sigma(n)}) = (y_1, \dots, y_n)$ . Ainsi,

$[\sigma \times (\sigma' \times f)](x_1, \dots, x_n) = (\sigma' \times f)(y_1, \dots, y_n) = (y_{\sigma'(1)}, \dots, y_{\sigma'(n)})$ , or pour tout  $i \in \{1, \dots, n\}$ ,  $y_i = x_{\sigma(i)}$ , donc  $y_{\sigma'(i)} = x_{\sigma(\sigma'(i))}$ .

Ainsi,  $[\sigma \times (\sigma' \times f)](x_1, \dots, x_n) = (x_{\sigma(\sigma'(1))}, \dots, x_{\sigma(\sigma'(n))}) = [(\sigma\sigma') \times f](x_1, \dots, x_n)$ .

Ceci démontre que  $\sigma \times (\sigma' \times f) = (\sigma\sigma') \times f$ , donc il s'agit bien d'une action du groupe  $\mathcal{S}_n$  sur l'ensemble des fonctions de  $\mathbb{Q}^n$  dans  $\mathbb{Q}$ .

On considère l'application  $\Delta : \mathbb{Q}^n \rightarrow \mathbb{Q}$   
 $(x_1, \dots, x_n) \mapsto \prod_{1 \leq i < j \leq n} (x_j - x_i)$ .

**14°) a)** Soit  $x = (x_1, \dots, x_n) \in \mathbb{Q}^n$ . Notons  $(x'_1, \dots, x'_n) = (x_{\tau(1)}, \dots, x_{\tau(n)})$ . Ainsi  $x'_k = x_n$ ,  $x'_n = x_k$  et, pour tout  $i \in \mathbb{N}_n \setminus \{k, n\}$ ,  $x'_i = x_i$ .

$(\tau \times \Delta)(x_1, \dots, x_n) = \Delta(x'_1, \dots, x'_n) = \prod_{1 \leq i < j \leq n} (x'_j - x'_i)$ . Ainsi,

$$\begin{aligned} (\tau \times \Delta)(x) &= (x'_n - x'_k) \prod_{\substack{1 \leq i < j < n \\ k \notin \{i, j\}}} (x'_j - x'_i) \prod_{j=k+1}^{n-1} (x'_j - x'_k) \prod_{i=1}^{k-1} (x'_k - x'_i) \prod_{\substack{1 \leq i \leq n-1 \\ i \neq k}} (x'_n - x'_i) \\ &= (x_k - x_n) \prod_{\substack{1 \leq i < j < n \\ k \notin \{i, j\}}} (x_j - x_i) \prod_{j=k+1}^{n-1} (x_j - x_n) \prod_{i=1}^{k-1} (x_n - x_i) \prod_{\substack{1 \leq i \leq n-1 \\ i \neq k}} (x_k - x_i) \\ &= \left[ \prod_{\substack{1 \leq i < j < n \\ k \notin \{i, j\}}} (x_j - x_i) \right] \left[ (-1)^{n-1-k} \prod_{j=k+1}^{n-1} (x_n - x_j) \right] \left[ \prod_{i=1}^{k-1} (x_n - x_i) \right] \\ &\quad \left[ \prod_{i=1}^{k-1} (x_k - x_i) \right] \left[ (-1)^{n-k-1} \prod_{i=k+1}^{n-1} (x_i - x_k) \right] \left[ (-1) \times (x_n - x_k) \right], \\ &= -(x_n - x_k) \prod_{\substack{1 \leq i < j < n \\ k \notin \{i, j\}}} (x_j - x_i) \prod_{j=k+1}^{n-1} (x_n - x_j) \prod_{i=1}^{k-1} (x_n - x_i) \times \\ &\quad \prod_{i=1}^{k-1} (x_k - x_i) \times \prod_{i=k+1}^{n-1} (x_i - x_k), \end{aligned}$$

donc on obtient  $(\tau \times \Delta)(x) = -\Delta(x)$ , pour tout  $x \in \mathbb{Q}^n$ ,

ce qui démontre que  $\tau \times \Delta = -\Delta$ .

**b)** Soit  $\tau$  une transposition de  $\mathcal{S}_n$ . Il existe  $a, b \in \mathbb{N}_n$  tels que  $a < b$  et  $\tau = (a \ b)$ . Si  $b = n$ , d'après la question précédente,  $\tau \times \Delta = -\Delta$ .

Supposons maintenant que  $b < n$ . Alors  $(a \ b) = (b \ n)(a \ n)(b \ n)$ . En effet,

$[(b \ n)(a \ n)(b \ n)](b) = [(b \ n)(a \ n)](n) = a$  et on vérifie de même que lorsque  $x \in \{a, n\}$ ,

$[(b \ n)(a \ n)(b \ n)](x) = (a \ b)(x)$ . C'est en outre évident lorsque  $x \in \mathbb{N}_n \setminus \{a, b, n\}$ , car  $x$  est un point fixe de toutes les transpositions utilisées.

Ainsi,  $\tau\Delta = [(b \ n)(a \ n)(b \ n)] \times \Delta$ , puis d'après les question 13 et 14.a,

$\tau\Delta = [(b \ n)(a \ n)] \times (-\Delta)$ .

Or, pour tout  $\sigma \in \mathcal{S}_n$  et  $f \in \mathcal{F}(\mathbb{Q}^n, \mathbb{Q})$ , pour tout  $(x_1, \dots, x_n) \in \mathbb{Q}^n$ ,

$(\sigma \times (-f))(x_1, \dots, x_n) = -(\sigma \times f)(x_1, \dots, x_n)$ , donc  $\sigma \times (-f) = -\sigma \times f$ .

---

On en déduit alors que  $\tau \times \Delta = (-1)^3 \Delta = -\Delta$ .

**15°)** Supposons qu'il existe  $k$  transpositions  $\tau_1, \dots, \tau_k$  telles que  $\sigma = \tau_1 \tau_2 \cdots \tau_k$ .

Posons  $\sigma' = \tau_1 \tau_2 \cdots \tau_{k-1}$ .

Ainsi  $\sigma = \sigma' \tau_k$  et  $\sigma \times \Delta = \sigma' \times (\tau_k \times \Delta) = \sigma' \times (-\Delta) = -(\sigma' \times \Delta)$ .

Par récurrence sur  $k$ , on peut donc montrer que  $\sigma \times \Delta = (-1)^k \Delta$ .

En particulier,  $(\sigma \times \Delta)(1, \dots, n) = (-1)^k \Delta(1, \dots, n)$ ,

c'est-à-dire  $(-1)^k \prod_{1 \leq i < j \leq n} (j - i) = \prod_{1 \leq i < j \leq n} (\sigma(j) - \sigma(i))$ , ce qu'il fallait démontrer.

**16°) a)** Soit  $c$  un cycle de longueur  $\ell$ , avec  $2 \leq \ell \leq n$ .

Il existe  $c_1, \dots, c_\ell \in \mathbb{N}_n$  tels que  $c = (c_1 \ c_2 \ \cdots \ c_\ell)$ .

Posons  $d = (c_1 \ c_2)(c_2 \ c_3) \cdots (c_{\ell-1}, c_\ell)$  et vérifions que  $c = d$ .

Soit  $x \in \mathbb{N}_n$ . Lorsque  $x \in \mathbb{N}_n \setminus \{c_1, \dots, c_\ell\}$ ,  $c(x) = x = d(x)$ .

Supposons qu'il existe  $i \in \mathbb{N}_\ell$  tel que  $x = c_i$ .

*Premier cas :* Supposons que  $i < \ell$ .

Pour tout  $j > i$ ,  $(c_j, c_{j+1})(x) = x$ ,

donc  $d(x) = (c_1 \ c_2) \cdots (c_{i-2}, c_{i-1})(c_{i+1}) = c_{i+1} = c(x)$ .

*Second cas :* Supposons que  $i = \ell$ .

Pour tout  $j \in \{2, \dots, \ell\}$ ,  $(c_{j-1} \ c_j)(c_j) = c_{j-1}$ , donc  $d(c_\ell) = c_1 = c(c_\ell)$ .

Ainsi, pour tout  $x \in \mathbb{N}_n$ , on a bien  $d(x) = c(x)$ .

Ceci démontre que la signature de  $c$  est égale à  $(-1)^{\ell-1}$ .

**b)** Soit  $\sigma \in \mathcal{S}_n$ . On sait qu'il existe des cycles  $c_1, \dots, c_p$  à supports deux à deux disjoints tels que  $\sigma = c_1 \cdots c_p$ . D'après la question précédente, si l'on décompose chaque cycle en produit de transpositions, en notant  $\ell_i$  la longueur du cycle  $c_i$ ,

$$\varepsilon(\sigma) = (-1)^{\ell_1-1} \times \cdots \times (-1)^{\ell_p-1} = (-1)^{\sum_{i=1}^p \ell_i - p}.$$

Les orbites de  $\sigma$  constituent une partition de  $\mathbb{N}_n$ , donc  $n = \sum_{i=1}^p \ell_i + s$ , où  $s$  désigne

le nombre d'orbites de cardinal 1. Ainsi,  $\varepsilon(\sigma) = (-1)^{n-s-p}$ , or  $s + p = m$  est bien le nombre d'orbites de  $\sigma$ .