

1.

1.1 Montrons que le produit « . » est bien défini. Tout d'abord, la somme $\sum_{k=-\infty}^{\infty} f(k)g(n-k)$ est finie pour tout $n \in \mathbb{Z}$

donné ; en effet, soit N_f et N_g des entiers tels que $n \leq N_f \Rightarrow f(n) = 0$ et $n \leq N_g \Rightarrow g(n) = 0$ (ils seront toujours désignés ainsi dans la suite), pour n donné on a que dans la somme ci-dessus k est limité à être $> N_f$ et $< n - N_g$. De plus, en conséquence, on a $(f.g)(n) = 0$ dès que $N_f + 1 > n - N_g - 1$, soit $n \leq N_f + N_g + 1$ et la formule définit bien une série de Laurent formelle. Remarquons au passage qu'on a la propriété $N_{f.g} \geq N_f + N_g + 1$.

Le changement d'indice $k \leftarrow n - k$ dans la somme (finie !) ci-dessus, qui correspond à un réarrangement de l'ordre des termes, montre que $(f.g)(n) = (g.f)(n)$ pour tout $n \in \mathbb{Z}$, donc le produit « . » est commutatif.

Par définition des lois, $\mathcal{L}$ est un sous-espace vectoriel de $\mathbb{C}^{\mathbb{Z}}$, de plus la distributivité de « . » par rapport à $+$ ainsi que la propriété $\lambda.(f.g) = (\lambda f).g = f.(\lambda g)$ sont immédiates quand on les traduit pour chaque n .

Montrons l'associativité de « . ». On peut écrire, puisqu'il s'agit de sommes finies, le produit $f.g$ sous la forme suivante : $(f.g)(n) = \sum_{\substack{(k_1, k_2) \in \mathbb{Z}^2 \\ k_1 + k_2 = n}} f(k_1)g(k_2)$. On en déduit clairement l'égalité :

$$((f.g).h)(n) = \sum_{\substack{(k_1, k_2, k_3) \in \mathbb{Z}^3 \\ k_1 + k_2 + k_3 = n}} f(k_1)g(k_2)h(k_3) = (f.(g.h))(n) \quad , \quad \text{cqfd.}$$

Enfin, on vérifie que la série formelle notée 1 et définie par

$$\forall n \in \mathbb{Z} \quad 1(n) = \delta_{0n} = \begin{cases} 1 & \text{si } n = 0 \\ 0 & \text{sinon} \end{cases}$$

est bien un élément neutre pour « . » : $\forall n \in \mathbb{Z} \quad (1.f)(n) = (f.1)(n) = f(n)$.

En conclusion, $\mathcal{L}$ est bien muni ainsi d'une structure de $\mathbb{C}$ -algèbre commutative.

1.2 La somme existe car elle est finie par (ii), de plus elle est nulle pour tout $n \leq N$ par (i).

1.3 t^{-1} est définie comme série de Laurent formelle par $\forall n \in \mathbb{Z} \quad t^{-1}(n) = \delta_{-1,n} = \begin{cases} 1 & \text{si } n = -1 \\ 0 & \text{sinon} \end{cases}$. En effet, on vérifie alors

$$\forall n \in \mathbb{Z} \quad (t.t^{-1})(n) = (t^{-1}.t)(n) = \sum_{k=-\infty}^{\infty} \delta_{1,k} \delta_{-1,n-k} = \delta_{0,n} = 1(n) \quad .$$

Par récurrences (croissante et décroissante) sur $k \in \mathbb{Z}$, on vérifie alors de même que t^k est défini par $\forall n \in \mathbb{Z} \quad t^k(n) = \delta_{k,n}$. Ainsi, la famille $(f(k).t^k)_{k \in \mathbb{Z}}$ vérifie les conditions (i) et (ii) de l'énoncé :

(ii) car $\forall n \in \mathbb{Z} \quad (f(k).t^k)(n)$ est nul sauf pour le terme $k = n$.

(i) car $\forall k \leq N_f \quad f(k) = 0$ donc $f(k).t^k(n) = 0$ pour tout $n \leq N_f$.

De plus, par définition de la somme $\sum_{k=-\infty}^{\infty} f(k)t^k$, on a $\forall n \in \mathbb{Z} \quad \left(\sum_{k=-\infty}^{\infty} f(k)t^k \right)(n) = \sum_{k=-\infty}^{\infty} (f(k)t^k)(n) = f(n)$, ce

qui traduit bien $\sum_{k=-\infty}^{\infty} f(k)t^k = f$.

1.4 Vérifions tout d'abord les propriétés (i) et (ii) pour la famille $(u^k)_{k \in \mathbb{N}^*}$. Pour cela, la remarque faite en 1.1 sur le produit $f.g$ montre que $N_u \geq 0 \Rightarrow \forall f \in \mathcal{L} \quad N_{f.u} \geq N_f + 1$, d'où par une récurrence immédiate sur $k \in \mathbb{N}^*$, $N_{u^k} \geq k - 1$. En d'autres termes, $\forall k \geq 1 \quad u^k(n) = 0$ dès que $k \geq n + 1$. Donc $(u^k(n))_{k \geq 1}$ est nulle pour $n \leq 0$ d'où (i) et n'a qu'un nombre fini de termes non nuls pour $n \geq 1$ d'où (ii).

Montrons maintenant l'égalité $u.\left(\sum_{k=1}^{\infty} u^k\right) = \sum_{k=2}^{\infty} u^k$. La valeur des deux expressions en $n \leq 0$ est nulle, il suffit de montrer l'égalité en $n \geq 1$. D'après ci-dessus on ne manipule que des sommes finies, et on peut écrire :

$$\begin{aligned} \left(u.\left(\sum_{k=1}^{\infty} u^k\right)\right)(n) &= \sum_{j=1}^{n-1} u(j) \cdot \left(\sum_{k=1}^{n-1} u^k(n-j)\right) \quad (\text{il faut } n-j \geq 1 \text{ et } k \leq n-j \leq n-1) \\ &= \sum_{k=1}^{n-1} \left(\sum_{j=1}^{n-1} u(j) \cdot u^k(n-j)\right) \quad (\text{réarrangement d'une somme finie}) \\ &= \sum_{k=1}^{n-1} u^{k+1}(n) \quad (\text{définition du produit } u \cdot u^k) \\ &= \sum_{k=2}^{\infty} u^k(n) \quad , cqfd. \end{aligned}$$

On en déduit, par distributivité dans l'anneau $\mathcal{L} : (1-u) \cdot \left(1 + \sum_{k=1}^{\infty} u^k\right) = 1 + \sum_{k=1}^{\infty} u^k - u - \sum_{k=2}^{\infty} u^k = 1$,
d'où le résultat demandé puisque la loi « $\cdot$ » est commutative.

1.5 Soit f non nul dans $\mathcal{L}$. Par définition, il existe un entier N tel que $n \leq N-1 \Rightarrow f(n) = 0$ et $f(N) \neq 0$. On peut écrire alors

$$f = \sum_{k=N}^{\infty} f(k)t^k = f(N)t^N(1-u) \quad ,$$

avec $u = -\sum_{k=1}^{\infty} \frac{1}{f(N)} f(k+N)t^k$. u vérifie les conditions du **1.4**, donc $(1-u)$ est inversible, or $f(N)t^N$ aussi, donc finalement f est inversible. $\mathcal{L}$ étant commutative et admettant des inverses pour tous ses éléments non nuls, $\mathcal{L}$ est un corps.

1.6 La série u est supposée non nulle, donc u^k existe pour tout $k \in \mathbb{Z}$. Si $f(k) = 0$ pour $k \leq 0$ (i.e. si $N_f \geq 0$), la suite $f(k)u^k$ vérifie les propriétés (i) et (ii) de l'énoncé : cela se voit comme en **1.4** puisque pour $k \geq 1$, $\forall n \in \mathbb{Z}$ $u^k(n) = 0$ dès que $k > n$. Donc l'écriture $\sum_{k=1}^{\infty} f(k)u^k$ définit bien une série de Laurent formelle.

Dans le cas général où $N_f < 0$, la série $\sum_{k \in \mathbb{Z}} f(k)u^k$ est alors bien définie comme somme *finie* des séries de Laurent formelles $f(k)u^k$, $N_f + 1 \leq k \leq 0$, et $\sum_{k=1}^{\infty} f(k)u^k$.

1.7 Pour $F.G$, il s'agit du théorème sur le produit de Cauchy de deux séries entières de rayons de convergence > 0 . Soit $R_U > 0$ et $R_F > 0$ les rayons de convergence respectifs des séries $F(z)$ et $U(z)$. On a, par application répétée du résultat ci-dessus, que pour tout $k \geq 0$ la série $U^k(z)$ est de rayon de convergence au moins R_U , avec $U^k(z) = \sum_{n=k}^{\infty} u^k(n)z^n$. On a l'absolue convergence pour $|z| < R_U$ de ces séries. Par continuité en 0 de la série entière

«des modules», $v(z) = \sum_{n=1}^{\infty} |u(n)|z^n$, qui vérifie $v(0) = 0$, il existe $\alpha > 0$ tel que pour $|z| < \alpha$ on ait $0 \leq |v(|z|)| < R_F$.

Enfin, par inégalités triangulaires répétées, on a $|u^k(n)| \leq v^k(n)$ pour tout $k \geq 1$ et tout $n \geq 0$. Comme la série $F(v)$ est absolument convergente pour $v < R_F$, il s'ensuit que la série double $\sum_{k \geq 0} \sum_{n \geq k} |f(k)| \cdot |u^k(n)| |z|^n$ est sommable pour $|z| < \alpha$. La série double sans les modules est donc sommable et on peut appliquer le théorème d'interversion des Σ :

$$\begin{aligned} \forall z \in \mathbb{C} \quad |z| < \alpha \implies F(U(z)) &= \sum_{k=0}^{\infty} f(k)U^k(z) = \sum_{k=0}^{\infty} \sum_{n=k}^{\infty} f(k)u^k(n)z^n \\ &= \sum_{n=0}^{\infty} \sum_{k=0}^n f(k)u^k(n)z^n = \sum_{n=0}^{\infty} (f \circ u)(n)z^n \quad , \end{aligned}$$

la dernière égalité résultant de la définition même de $f \circ u \in \mathcal{L}$.

1.8 La stabilité par composition pour la loi $\circ$ résulte de la définition **1.6** : en effet, si $f(k) = 0$ pour $k \leq 0$, alors a fortiori

$$(f \circ u)(n) = 0 \text{ pour } n \leq 0, \text{ de plus, } (f \circ u)(1) = \sum_{k=1}^{\infty} (f(k)u^k)(1) = f(1).u(1) \text{ est non nul si } f(1) \neq 0 \neq u(1).$$

On voit clairement (et par **1.3**) que l'élément neutre pour $\circ$ est la série de Laurent formelle $t \in \mathcal{G} : t \circ f = f \circ t = f$. L'associativité de la loi $\circ$ résulte de l'associativité (bien connue!) de cette loi dans l'algèbre des polynômes. D'une part en effet, si une série de Laurent formelle de $\mathcal{G}$ est, de plus, cofinale à 0, c'est un polynôme, et la définition de $\circ$ dans $\mathcal{G}$ coïncide alors avec celle de $\circ$ dans $\mathbb{C}[X]$.

D'autre part, montrons le lemme suivant :

Lemme : si $h \in \mathcal{G}$, la valeur $h^k(n)$, pour $n \geq k \geq 1$, ne dépend que des valeurs $h(j)$, $1 \leq j \leq n$.

Ce lemme se démontre par récurrence sur k , la proposition étant déjà clairement vraie pour $k = 1$. Supposons la proposition vraie pour k , et considérons $h^{k+1}(n)$ avec $n \geq k+1 \geq 2$. Comme h et h^k sont dans $\mathcal{G}$, le produit se calcule

avec seulement des valeurs $h(p)$ et $h^k(q)$ où $p \geq 1$ et $q \geq 1$: $h^{k+1}(n) = \sum_{j=1}^{n-1} h(j)h^k(n-j)$. Par hypothèse de récurrence,

on ne voit apparaître dans le deuxième membre ci-dessus que des fonctions polynômiales en les $h(p)$, $1 \leq p \leq n$, cqfd.

Ainsi, pour montrer l'égalité

$$(A) \quad \forall n \geq 1 \quad ((f \circ g) \circ h)(n) = (f \circ (g \circ h))(n),$$

(où f, g, h sont des séries de Laurent formelles dans $\mathcal{G}$, cette égalité étant déjà trivialement vraie pour $n = 0$), il suffit de vérifier l'égalité des coefficients de t^n dans l'égalité de polynômes obtenus en tronquant les séries f, g, h à partir du terme « de degré » $n+1$, puisque les coefficients $f(k), g(k), h(k)$ avec $k > n$ n'interviennent pas dans le calcul des deux membres de (A) ci-dessus. Cela résulte de ce que $f, f \circ g, g, g \circ h, h$ sont des éléments de $\mathcal{G}$, de ce que, pour un élément u de $\mathcal{G}$, $(f^k)(n) = 0$ dès que $k > n$, et enfin du lemme ci-dessus.

En d'autres termes, si on note $u|_n$, pour $n \geq 1$, la série formelle tronquée $\sum_{k=1}^n u(k)t^k$, on aura :

$$\begin{aligned} ((f \circ g) \circ h)(n) &= ((f \circ g)|_n \circ h|_n)(n) \\ &= ((f|_n \circ g|_n) \circ h|_n)(n) \\ &= (f|_n \circ (g|_n \circ h|_n))(n) \quad (\text{propriété sur les polynômes}) \\ &= (f \circ (g \circ h))(n), \text{ cqfd.} \end{aligned}$$

Démontrons maintenant l'existence d'un inverse à gauche : pour f donnée telle que $n \leq 0 \Rightarrow f(n) = 0$ et $f(1) \neq 0$, cherchons par récurrence sur n une série de Laurent formelle u telle que $u(n) = 0$ pour $n \leq 0$ et vérifiant

$$(u \circ f)(z) = z \iff \forall n \in \mathbb{Z} \quad (u \circ f)(n) = \delta_{1,n} \quad (I).$$

La relation (I) est satisfaite pour $n \geq 0$, et l'est pour $n = 1$ si et seulement si $f(1).u(1) = 1 \Leftrightarrow u(1) = \frac{1}{f(1)}$, qui est bien $\neq 0$. Supposons qu'on ait construit u vérifiant (I) jusqu'à l'ordre $n-1 \geq 1$. Pour n , la relation (I) se traduit par $\sum_{k=1}^n u(k)f^k(n) = 0$, puisque, là encore, les termes où $k \geq n+1$ n'interviennent pas. Or, par une récurrence facile, on voit que $f^n(n) = (f(1))^n \neq 0$, donc (I) est équivalente à

$$u(n) = \frac{1}{f^n(n)} \sum_{k=1}^{n-1} u(k)f^k(n).$$

Cette relation permet de construire la suite $u(n)$ par récurrence sur $n \geq 1$. On a donc bien l'existence d'un inverse à droite pour $\circ$ pour tout $f \in \mathcal{G}$.

Mais, puisque $\circ$ est associative, les inverses à gauche sont tous égaux aux inverses à droite :

$$u \circ f = t \text{ et } v \circ u = t \Rightarrow v \circ u \circ f = f \circ v = v, \text{ d'où } f \circ u = t.$$

En conclusion, $\mathcal{G}$ est un groupe pour « $\circ$ ».

1.9 Commençons par vérifier la formule $(f.g)' = f'.g + f.g'$. On se donne les séries de Laurent formelles $f = \sum_{n=-N_f}^{\infty} f(n)t^n$

et $g = \sum_{n=-N_g}^{\infty} g(n)t^n$. Par définition, pour tout $n \in \mathbb{Z}$:

$$\begin{aligned} (f.g)'(n) &= (n+1) \sum_{(j,k) / j+k=n+1} f(j)g(k) = (n+1) \sum_{j=-N_f}^{j=n+1+N_g} f(j)g(n+1-j) \\ (f'.g + f.g')(n) &= \sum_{j=-N_f-1}^{j=n+N_g} (j+1)f(j+1)g(n-j) + \sum_{j=-N_f}^{j=n+1+N_g} f(j)(n+1-j)g(n+1-j) \end{aligned}$$

En faisant le changement $j \leftarrow j+1$ dans la première somme de la deuxième égalité, on retrouve les mêmes termes $f(j)g(n+1-j)$ dans les deux sommes et l'égalité $(f.g)' = f'.g + f.g'$ se voit alors clairement.

La définition donne de plus $1' = 0$ (car $1'(n) = (n+1).1(n+1)$ est nul si $n = -1$ à cause du $(n+1)$ et aussi si $n \neq -1$ à cause du $1(n+1)$), ainsi que $(f^1)' = 1 \times f' \times f^0$. On en déduit comme en analyse classique que $(f^n)' = n f^{n-1}.f'$ par récurrence sur n , $n \geq 0$.

Enfin, pour $n \in \mathbb{Z}_-^*$, pour $f \neq 0$, en posant $n = -m$, de

$$(f^m.f^{-m})' = 1' = 0 = (f^m)' . f^{-m} + f^m (f^{-m})'$$

on déduit du cas $m \in \mathbb{N}^*$ que $(f^{-m})' = -f^{-m}.m.f^{m-1}.f'.f^{-m} = -m f^{-m-1}f'$, cqfd.

1.10 Montrons d'abord le *Lemme* : $\forall (F, u) \in \mathcal{L} \times \mathcal{G} \quad (F \circ u)' = (F' \circ u).u'$.

Pour tout $n \in \mathbb{Z}$, on a d'une part :

$$\begin{aligned} (F \circ u)'(n) &= (n+1).(F \circ u)(n+1) \\ &= (n+1) \left(\sum_{k=-N_F}^{\infty} F(k)u^k \right) (n+1) \\ &= (n+1) \left(\sum_{k=-N_F}^{\text{Max}(n+1,0)} F(k)u^k \right) (n+1) \\ &= \left(\sum_{k=-N_F}^{\text{Max}(n+1,0)} F(k)u^k \right)'(n) \\ &= \left(\sum_{k=-N_F}^{\text{Max}(n+1,0)} k F(k)u^{k-1}.u' \right)(n) , \end{aligned}$$

car à n fixé la somme finie suffit et par linéarité (évidente) de la dérivation.

Mais d'autre part, dans le calcul de $(F' \circ u.u')(n) = \left(\sum_{k=-N_F}^{\infty} k F(k)u^{k-1}.u' \right)(n)$ la somme sur k peut aussi aller jusqu'à

$\text{Max}(0, n+1)$ seulement, car on a $N_{u'} \geq -1$ et donc pour tout $k \geq 1$, $N_{u'.u^{k-1}} \geq k-1$. Le lemme est donc démontré.

Vérifions la formule de l'énoncé dans le cas où $f(z) = \frac{1}{z}$. On a $f(-1) = 1$ et $(u'.(f \circ u))(-1) = \left(\frac{u'}{u} \right)(-1)$. Mais le

coefficient de $\frac{1}{z}$ dans $\frac{u'(z)}{u(z)}$ est clairement $\frac{u'(0)}{u(1)} = 1$ par définition de u' , cqfd.

Dans le cas général, on écrit $f(z) = f(-1)\frac{1}{z} + F'(z)$ où F' est une série de Laurent formelle «primitive» définie par

$\begin{cases} F(n) = \frac{1}{n}f(n-1) & \text{si } n \neq 0 \\ F(0) = 0 & \text{(par exemple)} \end{cases}$. On en déduit, par distributivité, et grâce au lemme :

$$(u'.(f \circ u))(-1) = f(-1)\left(\frac{u'}{u}\right)(-1) + (F' \circ u)'(-1) = f(-1) ,$$

en effet, on constate par la définition que $\forall g \in \mathcal{L} \quad g'(-1) = 0$.

1.11 On applique la question précédente à la série formelle $f(z) = \frac{u^{<-1>}(z)}{z^{k+1}}$. On a $f(-1) = u^{<-1>}(k)$, $(f \circ u)(z) = \frac{(u^{<-1>} \circ u)(z)}{u^{k+1}(z)}$, d'où enfin

$$(u' \cdot f \circ u)(z) = \frac{z \cdot u'(z)}{u^{k+1}(z)} = -\frac{1}{k} \cdot z \cdot (u^{-k})'(z) .$$

On en déduit le coefficient de $\frac{1}{z}$:

$$(u' \cdot f \circ u)(-1) = -\frac{1}{k} (u^{-k})'(-2) \stackrel{def}{=} -\frac{1}{k} (-2+1) u^{-k}(-1) = \frac{1}{k} u^{-k}(-1) .$$

1.12 Remarquons tout d'abord que $u = t \cdot e^t$ est bien dans $\mathcal{G}$ (les puissances de t commencent à 1 avec $u(1) = 1 \neq 0$).

Ici $u^{-k}(t) = \frac{1}{t^k} e^{kt} = \sum_{n=0}^{\infty} \frac{(kt)^n}{t^k \cdot n!}$, donc le coefficient de t^{-1} est $u^{-k}(-1) = \frac{k^{k-1}}{(k-1)!}$. La formule d'inversion de Lagrange

donne alors : $u^{<-1>}(t) = \sum_{k=1}^{\infty} \frac{k^{k-1}}{k!} t^k$.

La règle de d'Alembert donne avec

$$\frac{u^{<-1>}(n+1)}{u^{<-1>}(n)} = \frac{(n+1)^{n+1}}{n^{n-1}} \frac{1}{n+1} = \left(1 + \frac{1}{n}\right)^{n-1} \longrightarrow e ,$$

que le rayon de convergence de $u^{<-1>}$ est $\frac{1}{e}$.

2.

2.1 σ agit sur chacune de ses orbites à la manière d'un cycle, de plus les actions sur chaque cycle sont indépendantes, donc elles commutent entre elles.

Si i et j sont dans deux orbites distinctes de σ , on a par exemple $\sigma = (i, i_1, \dots, i_p) \circ (j, j_1, \dots, j_q) \circ c_3 \circ \dots \circ c_k$, d'où $\sigma \circ \tau = (i, j_1, \dots, j_q, j, i_1, \dots, i_p) \circ c_3 \circ \dots \circ c_k$ et on voit que $\sigma \circ \tau$ a un cycle de moins : $O(\sigma\tau) = O(\sigma) - 1$ dans ce cas. Si i et j sont dans la même orbite de σ , on a par exemple $\sigma = (i, i_1, \dots, i_p, j, j_1, \dots, j_q) \circ c_2 \circ \dots \circ c_k$, d'où $\sigma \circ \tau = (i, j_1, \dots, j_q) \circ (j, i_1, \dots, i_p) \circ c_2 \circ \dots \circ c_k$ et on voit que $\sigma \circ \tau$ a un cycle de plus : $O(\sigma\tau) = O(\sigma) + 1$ dans ce cas.

2.2 C'est évident : il existe par définition des décompositions de σ_1 et σ_2 en respectivement $|\sigma_1|$ et $|\sigma_2|$ transpositions, donc $\sigma_1 \sigma_2$ peut s'écrire comme produit de $|\sigma_1| + |\sigma_2|$ transpositions et par minimalité, $|\sigma_1 \sigma_2| \leq |\sigma_1| + |\sigma_2|$.

2.3 Un cycle de longueur p , $c = (i_1, i_2, \dots, i_p)$ s'écrit comme produit de $p-1$ transpositions :

$$c = \tau(i_1, i_2) \circ \tau(i_2, i_3) \circ \dots \circ \tau(i_{p-1}, i_p) .$$

On en déduit, puisqu'une permutation σ est le produit de ses cycles, et que la somme des longueurs p des cycles de σ est n , qu'une permutation σ peut se décomposer en produit de $n - O(\sigma)$ transpositions, d'où déjà $|\sigma| \leq n - O(\sigma)$. L'autre inégalité se démontre par récurrence sur le nombre $|\sigma|$:

- $|\sigma| = 0$ signifie que $\sigma = e$, or $O(e) = n$, la formule est correcte.
- $|\sigma| = 1$ signifie que σ est une transposition, or pour une transposition τ , $O(\tau) = n-1$, la formule est correcte.
- Supposons maintenant que la formule soit correcte pour toutes les transpositions σ vérifiant $|\sigma| \leq k-1$, k entier donné ≥ 2 . Soit $\sigma \in S_n$ une permutation vérifiant $|\sigma| = k$, donc il existe une décomposition $\sigma = \tau_1 \circ \dots \circ \tau_{k-1} \circ \tau_k$. Posons $\sigma' = \sigma \circ \tau_k$. On a $\sigma' = \tau_1 \circ \dots \circ \tau_{k-1}$, donc $|\sigma'| \leq k-1$ et par hypothèse de récurrence, $|\sigma'| = n - O(\sigma')$. D'après **2.1** on a $O(\sigma') = O(\sigma) + \varepsilon$ avec $\varepsilon = \pm 1$, d'où $n - O(\sigma) - \varepsilon \leq k-1 = |\sigma| - 1$, soit encore $n - O(\sigma) \leq |\sigma| - 1 + \varepsilon \leq |\sigma|$, ce qu'il fallait démontrer.

2.4 On remarque que dans la démonstration par récurrence ci-dessus le cas $\varepsilon = -1$ est impossible puisque l'inégalité stricte $n - O(\sigma) < |\sigma|$ est impossible. Cela signifie par **2.1** que dans une décomposition minimale $\sigma = \tau_1 \circ \dots \circ \tau_k$, τ_k est une transposition portant sur deux éléments d'une même orbite de σ . Mais on a vu alors que les orbites de $\sigma' = \sigma \circ \tau_k$ sont des sous-orbites de σ , donc, de proche en proche, on voit que *toutes* les transpositions d'une décomposition minimale de σ portent sur des couples d'éléments appartenant toujours à une même orbite par σ .

Soit alors σ_1 et σ_2 dans S_n telles que $|\sigma_1| + |\sigma_1^{-1} \sigma_2| = |\sigma_2|$ et posons $p = |\sigma_1|$ et $q = |\sigma_2|$, d'où $q - p = |\sigma_1^{-1} \sigma_2|$. En écrivant $\sigma_2 = \sigma_1 \circ \sigma_1^{-1} \sigma_2$, on obtient une décomposition, minimale par hypothèse, de σ_2 à l'aide de décompositions minimales de σ_1 et de $\sigma_1^{-1} \sigma_2$: $\sigma_2 = \tau_1 \circ \dots \circ \tau_p \circ \tau_{p+1} \circ \dots \circ \tau_q$. De plus, on peut choisir (cf démo du **2.3**) d'écrire la décomposition $\tau_1 \circ \dots \circ \tau_p$ de σ_1 en mettant bout à bout des décompositions de chaque cycle $(i_1, i_2, \dots, i_k)$ de σ_1 sous la forme $(i_1, i_2)(i_2, i_3) \dots (i_{k-1}, i_k)$. Puisqu'on obtient ainsi une décomposition minimale de σ_2 , toutes ces transpositions τ_k , $1 \leq k \leq p$ portent sur des couples appartenant toujours aux mêmes orbites de σ_2 et on en déduit bien que toute orbite de σ_1 est incluse dans une orbite de σ_2 .

2.5 Soit c_1 et c_2 deux permutation circulaires, qu'on peut toujours noter sous la forme $c_1 = (1, c_1(1), \dots, c_1^{n-1}(1))$ et $c_2 = (1, c_2(1), \dots, c_2^{n-1}(1))$. L'application $h : \forall k \in [0, n-1] \quad c_1^k(1) \mapsto c_2^k(1)$ est une bijection de $[1, n]$ dans lui-même vérifiant $c_2 = h \circ c_1 \circ h^{-1}$. De plus, pour toute transposition $\tau = (ij)$, $h \circ \tau \circ h^{-1}$ est la transposition $\tau' = (h(i)h(j))$. On met donc ainsi en bijection les décompositions $c_1 = \tau_1 \circ \dots \circ \tau_{n-1}$ de c_1 avec celles de c_2 s'écrivant $c_2 = (h \circ \tau_1 \circ h^{-1}) \circ \dots \circ (h \circ \tau_{n-1} \circ h^{-1})$ (la bijection réciproque s'obtenant en prenant h^{-1} à la place de h). Donc w_n est le même cardinal pour c_1 ou pour c_2 .

Soit σ un cycle de S_n . D'après ci-dessus, la première transposition $\tau_1 = (ij)$ de toute décomposition $\sigma = \tau_{n-1} \circ \dots \circ \tau_1$ peut porter sur un élément $i \in [1, n]$ quelconque (grâce à une «rotation» h bien choisie), de plus, à i fixé, à chaque choix de $j \neq i$ correspond une bijection entre les décompositions $\sigma = \tau_{n-1} \circ \dots \circ \tau_2 \circ \tau_1$ et les décompositions de $\sigma' = \sigma \circ \tau_1$. Or on a vu (cf **2.1**) que σ' est un produit de deux cycles partiels c_1 et c_2 portant sur deux orbites disjointes : en notant $j = \sigma^{k+1}(i)$, $0 \leq k \leq n-2$, on a $c_1 = (i, \sigma^{k+2}(i), \dots, \sigma^{n-1}(i))$ et $c_2 = (\sigma(i), \dots, \sigma^{k+1}(i))$, c_1 est de longueur $n-k-1$, c_2 de longueur $k+1$. On a vu également que toute décomposition minimale de σ' s'obtient en juxtaposant une décomposition minimale de c_1 , $c_1 = \tau'_1 \circ \dots \circ \tau'_{n-k-2}$ avec une décomposition analogue $c_2 = \tau''_1 \circ \dots \circ \tau''_k$. Mais comme les orbites de c_1 et c_2 sont disjointes, toute transposition τ'_j commute avec toute transposition τ''_ℓ , donc deux décompositions de c_1 et c_2 génèrent en fait C_{n-2}^k décompositions de σ' différentes (par l'ordre des transpositions). Enfin, lorsque $i \in [1, n]$ et $j = \sigma^{k+1}(i)$, $0 \leq k \leq n-2$, varient, on retrouve deux fois (et deux fois seulement) la même décomposition pour σ puisque $\tau_1 = (ij) = (ji)$ est répété deux fois. En résumé, le nombre w_n des décompositions de σ vérifie la relation :

$$2 \times w_n = \underbrace{n}_{\text{choix de } i} \sum_{k=0}^{n-2} \underbrace{\sum_{j=\sigma^{k+1}(i)} C_{n-2}^k}_{\text{mélange des } \tau'_j \text{ avec les } \tau''_\ell} \underbrace{w_{k+1}}_{\text{choix des } \tau'_j} \cdot \underbrace{w_{n-k-1}}_{\text{choix des } \tau''_\ell}.$$

2.6 La relation ci-dessus s'écrit encore, en notant $w(n)$ le terme général de la série w :

$$\frac{2w_n}{(n-2)!} = n \sum_{k=0}^{n-2} \frac{w_{k+1}}{k!} \cdot \frac{w_{n-k-1}}{(n-k-2)!} = n \sum_{k=1}^{n-1} w(k)w(n-k).$$

On reconnaît-là un produit de Cauchy et une dérivation, si bien que le deuxième membre s'écrit encore $n.w^2(n) = ((w^2)')(n-1) = (2w.w')(n-1)$. Mais le premier membre s'écrit aussi $2(n-1)w(n)$, soit $2nw(n) - 2w(n)$: on reconnaît $nw(n) = (w')(n-1)$ ainsi que $w(n) = \left(\frac{w}{t}\right)(n-1)$. Comme la relation a lieu $\forall n \geq 2$, il y a donc égalité entre séries de Laurent formelles :

$$w' - \frac{w}{t} = w.w'.$$

2.7 w étant une série de Laurent formelle de $\mathcal{G}$, on peut considérer la série de Laurent formelle $h = \frac{we^{-w}}{t}$. Les règles de dérivation justifiées en **1**. (dérivation d'un produit, d'une puissance, d'une composée) avec la règle évidente $(e^z)' = e^z$ donnent

$$h' = -\frac{1}{t^2} \cdot (we^{-w} - t.w'e^{-w} + tw.w'e^{-w}) = -\frac{e^{-w}}{t} \cdot \left(\frac{w}{t} - w' + w.w'\right).$$

En vertu de **2.6**, on a que $h' = 0$, on en déduit clairement par la définition formelle de la dérivée que $h = h(0) = cste$. Comme $w(1) = w_1 = 1$, on a que le coefficient constant de h est $h(0) = 1$. Finalement la série de Laurent formelle w vérifie $\frac{w.e^{-w}}{t} = 1$, soit $t = w.e^{-w}$. Mais alors w est la série de Laurent formelle réciproque calculée en **1.12**, d'où par unicité d'une série formelle $w(n) = \frac{w_n}{(n-1)!} = \frac{n^{n-1}}{n!}$. On en déduit $w_n = n^{n-2}$.

3.

3.1 Fixons le sommet s_1 . Tout sommet s_k , $k \geq 2$, est relié à s_1 par au moins un chemin de longueur minimale $(s_1, \dots, s'_k, s_k)$. On peut choisir ainsi une application $k \mapsto a_k = \{s'_k, s_k\}$ de $[2, n]$ dans A . Il suffit donc de montrer que cette application est injective.

Supposons qu'il existe $j \neq k$ dans $[2, n]$ tels que $a_j = a_k$: nécessairement, puisque $s_j \neq s_k$ sont des extrémités de cette arête commune, $a_j = a_k = \{s_j, s_k\}$. Dans le chemin minimal $c_1 = (s_1, \dots, s_j, s_k)$ définissant a_k , le sous-chemin $(s_1, \dots, s_j)$ est minimal, donc il a même longueur que le chemin minimal $(s_1, \dots, s_k, s_j)$ définissant a_j , mais on voit alors que le chemin c_1 n'est pas minimal, il y a contradiction. On a mis en évidence une application $k \in [2, n] \mapsto a_k \in A$ injective et $\text{Card}(A) \geq n-1$.

Autre solution : par récurrence sur le nombre de sommets.

3.2 Appelons chemin sans retour un chemin dans le graphe de la forme $(s_{i_1}, \dots, s_{i_p})$ dont les sommets sont 2 à 2 distincts.

Leur ensemble est :

- non vide car $A \neq \emptyset$ par hypothèse ;
- fini car de cardinal majoré (grossièrement) par $2^n \cdot n!$;
- partiellement ordonné par la relation $\prec$ définie comme suit : $c_1 \prec c_2$ si et seulement si la suite des sommets de c_1 figure, dans cet ordre, comme sous-suite de la suite des sommets de c_2 .

Il existe donc dans cet ensemble un chemin sans retour maximal pour $\prec$: $c_M = (s_{i_1}, \dots, s_{i_p})$. Alors, nécessairement les extrémités s_{i_1} et s_{i_p} appartiennent à une seule arête. En effet, dans le cas contraire, comme le graphe est sans circuit, on pourrait prolonger c_M en un chemin strictement plus grand. On a donc mis en évidence l'existence de deux sommets au moins appartenant à une seule arête dans ce cas.

3.3 $(i) \Rightarrow (ii)$: l'implication est évidente dans le cas $n = 2$ et $n = 3$. Si $n \geq 4$, on se ramène au cas d'un graphe connexe sans circuit G' ayant $(n - 1)$ sommets en enlevant à G , d'après **3.2**, un sommet n'appartenant qu'à une arête et l'arête correspondante. Si par hypothèse de récurrence on admet que G' a $n - 2$ arêtes, G en a bien $n - 1$, donc l'implication est vraie par récurrence sur n .

$(ii) \Rightarrow (i)$: clair par **3.1**. En effet, si le graphe G , connexe, ayant n sommets et $n - 1$ arête avait un circuit $(a_1, a_2, \dots, a_k, a_1)$, le graphe G' obtenu en supprimant l'arête $\{a_1, a_2\}$ (et en conservant les mêmes sommets) resterait connexe : en effet, tout chemin «de connexité » de G donnerait un chemin «de connexité » de G' en remplaçant toute occurrence de l'arête $\{a_1, a_2\}$ par le sous chemin $(a_2, \dots, a_k, a_1)$ ou son image miroir $(a_1, a_k, \dots, a_2)$. Mais alors G' contredirait la propriété vue en **3.1**.

3.4 Existence de φ : puisque le graphe, connexe, est sans circuit, le chemin reliant s à tout autre sommet s' est unique. En notant celui-ci $(s, \dots, \varphi(s'), s')$, on définit ainsi une application $\varphi : S \setminus \{s\} \rightarrow S$. Notons que si $(s, s') \in A$, alors par définition $\varphi(s') = s$. Cette application convient, car déjà pour tout $u \in S \setminus \{s\}$ on a $\{u, \varphi(u)\} \in A$ par définition de φ . Réciproquement, soit $\{u, v\}$ une arête : si $u = s$, alors par unicité du chemin $s \rightarrow v$, nécessairement $u = s = \varphi(v)$; si $u \neq s \neq v$, les chemins reliant s à u et s à v sont nécessairement préfixes l'un de l'autre (sinon on met en évidence un circuit) donc, soit $u = \varphi(v)$, soit $v = \varphi(u)$. On a bien que l'ensemble des arêtes est $\{\{u, \varphi(u)\} , u \in S \setminus \{s\}\}$.

Unicité de φ : grâce à l'existence et l'unicité des chemins $s \rightarrow s'$ on peut définir une fonction profondeur $p : S \rightarrow \mathbb{N}$. On pose $p(s) = 0$, et pour tout $s' \neq s$ $p(s') = k$ si le chemin $c : s \rightarrow s'$ utilise k arêtes (i.e. $c = (s, a_1, \dots, a_{k-1}, s')$). Soit alors une fonction $\varphi : S \setminus \{s\} \rightarrow S$ vérifiant que $A = \{\{u, \varphi(u)\} , u \in S \setminus \{s\}\}$. On raisonne par récurrence sur la profondeur $k \geq 1$ pour montrer que $p(s') = k \Rightarrow p(\varphi(s')) = k - 1$.

Si $p(s') = 1$, $\{s, s'\}$ est une arête, donc nécessairement $s = \varphi(s')$ et $\varphi(s')$ est bien de profondeur 0 .

Soit s' de profondeur $k \geq 2$. Il existe un chemin $(s, \dots, s'', s')$ le reliant à s , donc un sommet s'' profondeur $k - 1$ tel que $\{s'', s'\} \in A$. Par hypothèse de récurrence, $\varphi(s'')$ est de profondeur $k - 2$, donc $\varphi(s'') \neq s'$. Donc, nécessairement, par hypothèse sur φ , c'est que $s'' = \varphi(s')$ et on a bien $\varphi(s')$ de profondeur $k - 1$, cqfd.

Mais alors, par définition de la profondeur, $\forall s' \neq s$ $p(\varphi(s')) = p(s') - 1$ implique que φ est justement l'application construite ci-dessus pour en montrer son existence, d'où l'unicité de φ .

3.5 Vient de la dérivation d'un déterminant. On sait que $f(x) = \det(C_1(x), \dots, C_n(x))$ (où $C_1, \dots, C_n$ sont des fonctions dérivables à valeurs dans $\mathbb{C}^n$) se dérive en

$$f'(x) = \sum_{i=1}^n \det(C_1(x), \dots, C_i e'(x), \dots, C_n(x)) \quad .$$

Ici, $C_i(x) = \begin{pmatrix} M_{1i} \\ \vdots \\ M_{ii} - x \\ \vdots \\ M_{ni} \end{pmatrix}$ se dérive en $C'_i = \begin{pmatrix} 0 \\ \vdots \\ -1 \\ \vdots \\ 0 \end{pmatrix}$ et donc, en appelant $C_1, \dots, C_n$ les colonnes de la matrices M ,

on a :

$$\begin{aligned} P'(0) &= \begin{vmatrix} -1 \\ 0 \\ \vdots \\ 0 \end{vmatrix} \begin{vmatrix} C_2 \end{vmatrix} \cdots \begin{vmatrix} C_n \end{vmatrix} + \begin{vmatrix} C_1 \end{vmatrix} \begin{vmatrix} 0 \\ -1 \\ \vdots \\ 0 \end{vmatrix} \cdots \begin{vmatrix} C_n \end{vmatrix} + \cdots \\ &\quad + \begin{vmatrix} C_1 \end{vmatrix} \cdots \begin{vmatrix} C_{n-1} \end{vmatrix} \begin{vmatrix} 0 \\ \vdots \\ 0 \\ -1 \end{vmatrix} \\ &= -\det M^{11} - \det M^{22} - \cdots - \det M^{nn} \quad , \end{aligned}$$

en développant à chaque fois suivant une colonne appropriée.

3.6 C'est clair : (*) s'écrit $M \times \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix} = 0$.

3.7 Soit $i \in [2, n]$ fixé. Notons $C_1, \dots, C_n$ les colonnes, dans $\mathbb{C}^{n-1}$, de la matrice M auxquelles on a enlevé chaque fois le i -ème élément. On a ainsi $\det M^{ii} = |C_1 \cdots \widehat{C_i} \cdots C_n|$ ($\widehat{C_i}$ signifie que la colonne C_i ne figure pas). Remplaçons dans ce déterminant la première colonne par la somme de toutes les colonnes (sauf la i -ème bien sûr !). En vertu de la relation (*) la première colonne est remplacée par $(-C_i)$. Puis, par interversion de colonnes (permutation des colonnes 1 et 2, puis 2 et 3, jusqu'à $i-2$ et $i-1$), on trouve finalement :

$$\det M^{ii} = -|C_i|C_2 \cdots C_n| = (-1)^{i-1} |C_2 \cdots C_i \cdots C_n|.$$

Sur cette dernière forme, on refait les mêmes opérations, mais sur les lignes, en écrivant $\det M^{ii} = (-1)^{i-1} \begin{vmatrix} L_1 \\ \vdots \\ \widehat{L_i} \\ \vdots \\ L_n \end{vmatrix}$.

Comme la matrice M est symétrique, la relation (*) dit que remplacer la première ligne par la somme des lignes (sauf la i -ème) revient à la remplacer par $-L_i$, puis le même nombre de permutations de lignes replace L_i en sa i -ème position, d'où finalement :

$$\det M^{ii} = -(-1)^{i-1} \begin{vmatrix} L_i \\ L_2 \\ \vdots \\ L_n \end{vmatrix} = \begin{vmatrix} L_2 \\ \vdots \\ L_i \\ \vdots \\ L_n \end{vmatrix}.$$

Sous cette dernière forme, on reconnaît l'égalité $\det M^{ii} = \det M^{11}$.

3.8 On utilise **3.5**. $P'(0)$ est le coefficient de degré 1 du polynôme caractéristique, c'est donc $-\sigma_{n-1}$, avec σ_{n-1} la $(n-1)$ -ème fonction symétrique élémentaire des valeurs propres : $\sigma_{n-1} = \sum_i (\lambda_1 \cdots \widehat{\lambda_i} \cdots \lambda_n)$. On en déduit, puisque tous

les $\det M^{ii}$ sont égaux : $\det(M^{ii}) = \frac{\sigma_{n-1}}{n}$.

Mais on sait que 0 est valeur propre, donc tous les termes sont nuls sauf éventuellement 1 dans la somme définissant σ_{n-1} , et finalement $\sigma_{n-1} = 0$ si 0 est valeur propre au moins double et sinon $\sigma_{n-1} = \prod_{\lambda \in \text{sp}(M) \setminus \{0\}} \lambda$.

3.9 La formule vient de la multilinéarité du déterminant. On commence par écrire $\det M^{nn}$ comme un déterminant $n \times n$ en appelant $C_1, \dots, C_{n-1}$ les colonnes (dans $\mathbb{C}^n$) de M :

$$\det M^{nn} = - \begin{vmatrix} M_{11} & \cdots & M_{1,n-1} & 0 \\ \vdots & & \vdots & \vdots \\ M_{n1} & \cdots & M_{n,n-1} & -1 \end{vmatrix} = - \begin{vmatrix} C_1 & \cdots & C_{n-1} & \begin{vmatrix} 0 \\ \vdots \\ -1 \end{vmatrix} \end{vmatrix}.$$

Mais en vertu de (*) on peut écrire chaque colonne C_j comme une combinaison linéaire des colonnes $\gamma_{ij} = e_i - e_j$, avec $i \neq j$:

$$\forall j \in [1, n-1] \quad C_j = \sum_{i, i \neq j} M_{ij} \gamma_{ij} = \sum_{i, i \neq j} M_{ij} (e_i - e_j).$$

Or la juxtaposition de colonnes $\gamma_{i,j}$, $1 \leq j \leq n-1$, et de la colonne $-e_n = \begin{pmatrix} 0 \\ \vdots \\ -1 \end{pmatrix}$ est précisément une matrice

de la forme $E_\varphi - I$, d'où par multi-linéarité :

$$\begin{aligned} \det M^{nn} &= - \det \left(\sum_{i, i \neq 1} M_{i1} \gamma_{i1}, \sum_{i, i \neq 2} M_{i2} \gamma_{i2}, \dots, \sum_{i, i \neq n-1} M_{i,n-1} \gamma_{i,n-1}, -e_n \right) \\ &= - \sum_{\varphi \in \mathcal{F}_n} M_{\varphi(1),1} \cdot M_{\varphi(2),2} \cdots M_{\varphi(n-1),n-1} \cdot \det(E_\varphi - I) \\ &= - \sum_{\varphi \in \mathcal{F}_n} \prod_{j=1}^{n-1} M_{j,\varphi(j)} \cdot \det(E_\varphi - I), \text{ c.q.f.d.} \end{aligned}$$

3.10 S'il existe un cycle par φ comme dans l'énoncé, alors le vecteur $x = e_{a_1} + \dots + e_{a_k}$ est invariant par E_φ . Donc E_φ admet 1 comme valeur propre et $\det(E_\varphi - I) = 0$.

Remarquons que ceci inclut le cas où $\exists i \in [1, n-1] \quad \varphi(i) = i$ (car alors 1 est valeur propre de E_φ de vecteur propre associé e_i , c'est le cas $k = 1$) et aussi le cas où $\varphi([1, n-1]) \subset [1, n-1]$ (car dans la suite de n éléments $(1, \varphi(1), \dots, \varphi^{n-1}(1))$ il y aura alors nécessairement deux valeurs égales).

On considère maintenant le cas où φ n'a pas de cycle.

Alors pour tout $i \in [1, n-1]$ on ne peut pas avoir de suite $(i, \varphi(i), \dots, \varphi^{n-1}(i), \varphi^n(i))$ puisque cette suite doit avoir ses éléments deux à deux distincts. Cela signifie en fait qu'il existe $k \in [1, n-1]$ tel que $\varphi^k(i) = n$. D'où

$$\forall i \in [1, n-1] \quad (E_\varphi)^n(e_i) = (E_\varphi)^{n-k} \circ (E_\varphi)^k(e_i) = (E_\varphi)^{n-k}(e_n) = 0.$$

Comme $E_\varphi^n(e_n) = 0$ aussi, on a bien que $E_\varphi^n = 0$.

On vient de voir que le graphe d'arêtes $\{i, \varphi(i)\}$, $i \in [1, n-1]$, est connexe puisque tous les sommets sont reliés au sommet n . Comme il y en a $n-1$, c'est un arbre.

Comme E_φ est nilpotente, 0 est sa seule valeur propre possible, donc son polynôme caractéristique est $(-1)^n X^n$. Il en résulte que $\det(E_\varphi - I) = (-1)^n$ dans ce cas.

3.11 D'après **3.4**, tout arbre de sommets $\{1, 2, \dots, n\}$ est associé de manière unique à une application $\varphi : [1, n-1] \rightarrow [1, n]$ (lorsqu'on choisit n comme racine de l'arbre), et la question précédente associe à tout terme *a priori* non nul du second membre de la formule **3.9** un arbre de T_n . Donc l'identité demandée n'est qu'une reformulation de la formule du **3.9** compte tenu de la valeur constante $(-1)^{n-1}$ de $\det(E_\varphi - I)$ lorsque celui-ci n'est pas nul.

3.12 Soit J la matrice $n \times n$ dont tous les éléments valent 1, et considérons la matrice $M = J - nI$. Clairement M vérifie les hypothèses de symétrie et $(*)$, donc l'identité du **3.11** s'applique. Mais ici tous les éléments M_{ij} valent 1, donc le second membre donne directement $-Card(T_n)$. La matrice J ayant 0 comme valeur propre d'ordre $n-1$ et n comme dernière valeur propre, son polynôme caractéristique est $(-1)^n X^{n-1}(X - n)$. Si on applique ceci pour une matrice d'ordre $n-1$ et avec $X = n$, on trouve

$$\det(M^{nn}) = (-1)^{n-1} n^{n-2} \cdot 1 = -n^{n-2}.$$

Finalement, $Card(T_n) = n^{n-2}$.

3.13 Montrons d'abord que le produit $\sigma = \tau(a_1) \dots \tau(a_{n-1})$ est un cycle d'ordre n lorsque $a_1, \dots, a_{n-1}$ sont les arêtes d'un arbre de T_n . On procède par récurrence sur n . Pour $n = 2$, il n'y a rien à démontrer, puisqu'une transposition est déjà un cycle d'ordre 2. Supposons donc que ce soit vrai jusqu'à l'ordre n , $n \geq 2$, et regardons un produit $\sigma = \tau(a_1) \dots \tau(a_{n-1}) \tau(a_n)$ lorsque $a_1, \dots, a_n$ sont les n arêtes d'un arbre A de T_{n+1} . Posons $a_n = \{i, j\}$ et considérons l'arbre A' obtenu à partir de A en supprimant l'arête a_n : A' n'est plus connexe, les sommets $s \in \{1, \dots, n, n+1\}$ se répartissent en deux sous-ensembles disjoints A_i ou A_j suivant qu'ils sont reliés respectivement à i ou à j dans A' . En effet, tout sommet s est relié à i dans A d'une seule manière par un chemin c : si c ne contient pas a_n , $s \in A_i$, sinon, par unicité, nécessairement, c se termine par a_n et ne contient qu'une fois a_n , donc $s \in A_j$. Comme les $\tau(a_k)$, $a_k \in A_i$, et les $\tau(a_\ell)$, $a_\ell \in A_j$ sont à supports disjoints, ils commutent, et on a :

$$\begin{aligned} \sigma &= \left(\prod_{a_k \in A_i} \tau(a_k) \right) \left(\prod_{a_\ell \in A_j} \tau(a_\ell) \right) \tau(a_n) \\ &= c_1 \circ c_2 \circ \tau(a_n), \end{aligned}$$

où par hypothèse de récurrence, c_1 et c_2 sont des cycles partiels de supports disjoints dont la réunion est $\{1, \dots, n, n+1\}$. D'après le **2.1**, $O(\sigma) = 1$, i.e. σ est un cycle d'ordre $n+1$.

L'injectivité de l'application énoncée est claire, car on pose par convention que deux produits de transpositions qui diffèrent par l'ordre des facteurs sont deux décompositions différentes (et elles sont a fortiori différentes si les facteurs différents!).

Pour montrer qu'il y a bijection entre Ω et F , il suffit donc de montrer que toute décomposition d'un cycle σ d'ordre n en produit de $n-1$ transpositions $\tau(a_k)$ se fait avec des transpositions de supports a_k constituant les arêtes d'un arbre de T_n . Pour cela, il suffit de voir que le graphe G des arêtes a_k est connexe (cf **3.3**). Soit $i \neq j$ deux sommets de $\{1, \dots, n\}$. i et j sont dans la même orbite par σ , donc $\exists k \geq 1$ tel que $j = \sigma^k(i)$. Or, pour $s \neq s'$ dans $\{1, \dots, n\}$, $\sigma = \tau(a_1) \circ \dots \circ \tau(a_n)$ et $s' = \sigma(s)$ signifie, par définition de la composition des transpositions, qu'il existe un chemin $(s = s_0, s_1, \dots, s_k = s')$ dans G . Il existe donc dans G un chemin de i à $s_1 = \sigma(i)$, puis de s_1 à $s_2 = \sigma(s_1)$, ... etc., jusqu'à $j = s_k = \sigma(s_{k-1})$. G est donc connexe, c'est un arbre, cqfd.

3.14 Tout cycle d'ordre n est déterminé par les $(n-1)$ images successives, distinctes, de 1, il y en a donc $(n-1)!$. Comme chacun d'eux donne naissance à w_n décompositions (cf **2.5**), le cardinal de $\mathcal{F}$ est $w_n \cdot (n-1)!$. De même, chaque arbre de T_n donne $(n-1)!$ énumérations de ses arêtes, donc $Card(\Omega) = Card(T_n) \cdot (n-1)!$. On en déduit $w_n = Card(T_n) = n^{n-2}$.

4.

4.1 La commutation des endomorphismes $\varepsilon_1, \varepsilon_2, \varepsilon_3$ provient de la commutation des symétries $\gamma_1, \gamma_2, \gamma_3$. On le vérifie de toutes façons en trouvant une base commune de diagonalisation. La base propre commune est :

$$\begin{aligned} u_1 &= e_1 + e_2 + e_3 + e_4 + e_5 + e_6 + e_7 + e_8 ; \\ u_2 &= e_1 - e_2 + e_3 - e_4 + e_5 - e_6 + e_7 - e_8 ; \\ u_3 &= e_1 + e_2 - (e_3 + e_4) + e_5 + e_6 - (e_7 + e_8) ; \\ u_4 &= e_1 - e_2 - e_3 + e_4 + e_5 - e_6 - e_7 + e_8 ; \\ u_5 &= e_1 + e_2 + e_3 + e_4 - (e_5 + e_6 + e_7 + e_8) ; \\ u_6 &= e_1 - e_2 + e_3 - e_4 - (e_5 - e_6 + e_7 - e_8) ; \\ u_7 &= e_1 + e_2 - (e_3 + e_4) - (e_5 + e_6 - (e_7 + e_8)) ; \\ u_8 &= e_1 - e_2 - e_3 + e_4 - (e_5 - e_6 - e_7 + e_8) ; \end{aligned}$$

On vérifie en effet que $\varepsilon_1, \varepsilon_2, \varepsilon_3$ ont dans la base des u_i des matrices diagonales, par exemple :

- pour ε_1 : $\text{diag}(1, -1, -1, 1, 1, -1, -1, 1)$;
- pour ε_2 : $\text{diag}(1, -1, 1, -1, 1, -1, 1, -1)$;
- pour ε_3 : $\text{diag}(1, 1, 1, 1, -1, -1, -1, -1)$;

4.2 Remarquons que puisqu'une arête s'écrit $\{i, j\}$ aussi bien que $\{j, i\}$, la matrice M est symétrique.

Pour un sommet du cube, les trois arêtes qui en partent ont pour extrémités les images de ce sommet par $\gamma_1, \gamma_2, \gamma_3$ (ce qui correspond aux trois directions des arêtes). Il en résulte que les «1» de la matrice M correspondent pour chaque colonne e_i à la somme $(\varepsilon_1 + \varepsilon_2 + \varepsilon_3)(e_i)$. A cause de la propriété (*), on est amené à mettre -3 sur la diagonale, d'où finalement $M = \varepsilon_1 + \varepsilon_2 + \varepsilon_3 - 3I$.

4.3 On voit grâce à la base des u_i que les valeurs propres de M sont 0 d'ordre 1, -4 d'ordre 3, -2 d'ordre 3, -6 d'ordre 1. Donc par **3.8**, $\det(M^{nn}) = -\frac{2^3 \cdot 4^3 \cdot 6}{8} = -84$.

D'autre part, la formule **3.11** appliquée à M donne dans le second membre une somme de 1 correspondant à des arbres couvrants du cube par définition, donc donne le nombre cherché. On en déduit que le nombre d'arbres couvrants est dans ce cas 84.

4.4 La généralisation se fait en remplaçant $\gamma_1, \gamma_2, \gamma_3$ par les n symétries hyperplanes de base et en considérant une matrice M_n d'ordre $p = 2^n$ analogue ayant des $-n$ sur la diagonale :

$$M_n = \varepsilon_1 + \dots + \varepsilon_n - nI_p .$$

Le problème est de calculer les valeurs propres de M_n , sachant, par **3.8** et **3.11** que le cardinal cherché est $R_n = \frac{1}{2^n} \prod_{\lambda \in sp(M_n) \setminus \{0\}} (-\lambda)$. Contentons-nous d'indiquer un moyen de passer de l'ordre n à l'ordre $n+1$. Si la

base propre commune à l'ordre n de $\varepsilon_1, \dots, \varepsilon_n$ est $X_1, X_2, \dots, X_p$ (avec $p = 2^n$, et ce dans la base des p sommets de l'hypercube), la base commune à l'ordre $n+1$ est de la forme

$$\begin{pmatrix} X_1 \\ X_1 \end{pmatrix}, \begin{pmatrix} X_2 \\ X_2 \end{pmatrix}, \dots, \begin{pmatrix} X_p \\ X_p \end{pmatrix}, \begin{pmatrix} X_1 \\ -X_1 \end{pmatrix}, \begin{pmatrix} X_2 \\ -X_2 \end{pmatrix}, \dots, \begin{pmatrix} X_p \\ -X_p \end{pmatrix} .$$

Si on considère que la symétrie supplémentaire γ_{n+1} est précisément $\begin{pmatrix} X \\ Y \end{pmatrix} \mapsto \begin{pmatrix} X \\ -Y \end{pmatrix}$ (d'où la matrice de ε_{n+1} est dans cette base $\text{diag}(1, 1, \dots, 1, -1, -1, \dots, -1)$), alors on voit que les valeurs propres de M_{n+1} se déduisent de celles de M_n par l'application

$$(\lambda_1, \lambda_2, \dots, \lambda_p) \mapsto (\lambda_1, \lambda_2, \dots, \lambda_p, \lambda_1 - 2, \lambda_2 - 2, \dots, \lambda_p - 2) .$$

Ainsi par exemple, les valeurs propres de M_4 sont : 0 d'ordre 1, -2 d'ordre 4, -4 d'ordre 6, -6 d'ordre 4, -8 d'ordre 1, d'où $R_4 = \frac{1}{2^4} (2^4 \cdot 4^6 \cdot 6^4 \cdot 8) = 2^{19} \cdot 3^4$.

*
* *