

DM 17. Corrigé

Partie I : Nombre de surjections entre ensembles finis

1°)

◇ Notons S l'ensemble des surjections de $\mathbb{N}_n$ sur $\mathbb{N}_m$ et notons P l'ensemble des partitions ordonnées de $\mathbb{N}_n$ en m classes.

Soit $f \in S$. Pour tout $x, y \in \mathbb{N}_n$, convenons que $x R y$ si et seulement si $f(x) = f(y)$. D'après l'exemple canonique du cours, R est une relation d'équivalence sur $\mathbb{N}_n$, donc ses classes d'équivalence constituent une partition de $\mathbb{N}_n$. Or la classe d'équivalence de x est $f^{-1}(\{f(x)\})$. f étant surjective, $\mathbb{N}_n/R = \{f^{-1}(\{i\})/i \in \mathbb{N}_m\}$. Ainsi, si l'on pose $\varphi(f) = (f^{-1}(\{1\}), \dots, f^{-1}(\{m\}))$, on définit une application de S dans P .

◇ Montrons que φ est bijective.

Soit $f, g \in S$ telles que $\varphi(f) = \varphi(g)$.

Soit $x \in \mathbb{N}_n$. $x \in f^{-1}(\{f(x)\}) = g^{-1}(\{f(x)\})$, donc $g(x) = f(x)$. Ainsi, $f = g$. Ceci prouve que φ est injective.

Soit $A = (A_1, \dots, A_m) \in P$. Si $x \in \mathbb{N}_n$, il existe un unique $i \in \mathbb{N}_m$ tel que $x \in A_i$. On peut donc poser $i = f(x)$. Ceci définit une application f de $\mathbb{N}_n$ dans $\mathbb{N}_m$, surjective car chaque A_i est non vide. Pour tout $i \in \mathbb{N}_m$, par définition de f ,

$f^{-1}(\{i\}) = \{x \in \mathbb{N}_n / f(x) = i\} = A_i$, donc $\varphi(f) = A$, ce qui prouve que φ est surjective.

◇ Notons P' l'ensemble des partitions de $\mathbb{N}_n$ en m classes. Notons Ψ l'application de P dans P' définie par $\Psi(A_1, \dots, A_m) = \{A_1, \dots, A_m\}$.

Soit $E = \{A_1, \dots, A_m\} \in P'$ et $B = (B_1, \dots, B_m) \in P$. $A_1, \dots, A_m$ sont deux à deux distincts, ainsi que $B_1, \dots, B_m$, donc $\Psi(B) = E \iff [\exists \sigma \in \mathcal{S}_m, \forall i \in \mathbb{N}_m, B_i = A_{\sigma(i)}]$.

On en déduit que $|\Psi^{-1}(E)| = |\mathcal{S}_m| = m!$, donc d'après le principe des bergers,

$|P| = m!|P'|$.

En conclusion, le nombre de surjections de $\mathbb{N}_n$ sur $\mathbb{N}_m$ est égal à $|S| = m!S_n^m$.

2°) D'après le cours, $|\mathbb{N}_m^{\mathbb{N}_n}| = m^n$. D'autre part, pour construire une application quelconque f de $\mathbb{N}_n$ dans $\mathbb{N}_m$, on peut choisir le nombre $k \in \{1, \dots, m\}$ de valeurs atteintes par f dans $\mathbb{N}_m$, puis l'ensemble A de ces valeurs atteintes, ce qui revient à choisir k éléments parmi m ($\binom{m}{k}$ choix), puis on choisit f parmi les surjections de $\mathbb{N}_n$ dans A ,

au nombre de $k!S_n^k$ d'après la question précédente. Ainsi, $m^n = \sum_{k=1}^m \binom{m}{k} (k!S_n^k)$.

3°) a) Pour tout $f \in \mathbb{N}_n^{\mathbb{N}_m}$,

$f \in E_{k_1} \cap \dots \cap E_{k_\ell} \iff \forall j \in \mathbb{N}_\ell, k_j \notin f(\mathbb{N}_n) \iff f(\mathbb{N}_n) \subset \mathbb{N}_m \setminus \{k_1, \dots, k_\ell\}$, donc le cardinal de $E_{k_1} \cap \dots \cap E_{k_\ell}$ est égal à celui de l'ensemble des applications de $\mathbb{N}_n$ dans $\mathbb{N}_m \setminus \{k_1, \dots, k_\ell\}$. Ainsi, d'après le cours, $|E_{k_1} \cap \dots \cap E_{k_\ell}| = (m - \ell)^n$.

b)

◇ Formule du crible : Soit $n \in \mathbb{N}^*$. Notons $R(n)$ l'assertion suivante : pour toute famille

$(F_1, \dots, F_n)$ de n ensembles finis, $|\bigcup_{k=1}^n F_k| = \sum_{A \subset \mathcal{P}(\mathbb{N}_n) \setminus \{\emptyset\}} (-1)^{|A|+1} \left| \bigcap_{i \in A} F_i \right|$.

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,

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

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

◇ f n'est pas une surjection de $\mathbb{N}_n$ dans $\mathbb{N}_m$ si et seulement si il existe $k \in \mathbb{N}_m$ tel que $k \notin f(\mathbb{N}_n)$, donc l'ensemble des surjections de $\mathbb{N}_n$ dans $\mathbb{N}_m$ est égal à $\mathbb{N}_m^{\mathbb{N}_n} \setminus \bigcup_{k \in \mathbb{N}_m} E_k$.

Ainsi, d'après la formule du crible ,

$$\begin{aligned} m!S_n^m &= m^n - \left| \bigcup_{k \in \mathbb{N}_m} E_k \right| \\ &= m^n - \sum_{k=1}^m (-1)^{k-1} \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq m} |E_{i_1} \cap \dots \cap E_{i_k}| \\ &= m^n - \sum_{k=1}^m (-1)^{k-1} \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq m} (m-k)^n \\ &= m^n - \sum_{k=1}^m (-1)^{k-1} (m-k)^n |\{(i_1, \dots, i_k) \in \mathbb{N}^k / 1 \leq i_1 < i_2 < \dots < i_k \leq m\}|, \end{aligned}$$

$$\text{donc } m!S_n^m = m^n + \sum_{k=1}^m (-1)^k (m-k)^n \binom{m}{k} = \sum_{k=0}^m (-1)^k (m-k)^n \binom{m}{k}.$$

Partie II : Formule d'inversion de Möbius

4°) Soit $f, g \in A$. Soit $n \in \mathbb{N}^*$.

Notons $E_1 = \{d \in \mathbb{N}_n / d \mid n\}$ et $E_2 = \{(d, d') \in \mathbb{N}_n^2 / dd' = n\}$. L'application φ de E_1 dans E_2 définie par $\varphi(d) = (d, \frac{n}{d})$ est une bijection, dont l'application réciproque est $(d, d') \mapsto d$. Pour tout $(d, d') \in E_2$, posons $a_{(d, d')} = f(d)g(d')$.

Ainsi, $(f \ T \ g)(n) = \sum_{\substack{1 \leq d \leq n \\ d \text{ divise } n}} a_{(d, \frac{n}{d})} = \sum_{d \in E_1} a_{\varphi(d)}$, donc en posant $c = \varphi(d)$, on obtient que

$$(f \ T \ g)(n) = \sum_{c \in E_2} a_c = \sum_{\substack{1 \leq d, d' \leq n \\ dd' = n}} f(d)g(d').$$

5°)

◇ $(f \ T \ g)(n) = \sum_{\substack{1 \leq d, d' \leq n \\ dd' = n}} f(d)g(d')$, donc en posant $(e, e') = (d', d)$, on obtient

$$(f \ T \ g)(n) = \sum_{\substack{1 \leq e', e \leq n \\ e'e = n}} f(e')g(e), \text{ puis en renommant les variables,}$$

$$(f \ T \ g)(n) = \sum_{\substack{1 \leq d', d \leq n \\ dd' = n}} f(d')g(d) = (g \ T \ f)(n). \text{ Ainsi, } f \ T \ g = g \ T \ f, \text{ donc } T \text{ est une loi}$$

interne commutative sur A .

◇ Notons $e : \mathbb{N}^* \rightarrow \mathbb{Z}$ l'unique application telle que $e(1) = 1$ et $e(n) = 0$ pour tout $n \geq 2$. Soit $f \in A$ et $n \in \mathbb{N}^*$.

$$(f \ T \ e)(n) = \sum_{\substack{1 \leq d, d' \leq n \\ dd' = n}} f(d)e(d') = f(n)e(1) = f(n), \text{ donc } f \ T \ e = f = e \ T \ f.$$

Ainsi e est l'élément neutre pour la loi T .

◇ Il reste à montrer que T est associative. Soit $f, g, h \in A$, soit $n \in \mathbb{N}^*$.

$$\begin{aligned} [f \ T \ (g \ T \ h)](n) &= \sum_{\substack{1 \leq d, d' \leq n \\ dd' = n}} f(d)(g \ T \ h)(d') \\ &= \sum_{\substack{1 \leq d, d' \leq n \\ dd' = n}} f(d) \sum_{\substack{1 \leq \alpha, \beta \leq d' \\ \alpha\beta = d'}} g(\alpha)h(\beta) \\ &= \sum_{\substack{1 \leq d, d', \alpha, \beta \leq n \\ dd' = n, \alpha\beta = d'}} f(d)g(\alpha)h(\beta) \quad (\text{par sommation par paquets}). \end{aligned}$$

Posons $F_1 = \{(d, d', \alpha, \beta) \in \mathbb{N}_n^4 / dd' = n, \alpha\beta = d'\}$ et $F_2 = \{(d, \alpha, \beta) \in \mathbb{N}_n^3 / d\alpha\beta = n\}$. L'application φ de F_1 dans F_2 définie par $\varphi(d, d', \alpha, \beta) = (d, \alpha, \beta)$ est une bijection, donc en posant $a_{(d, \alpha, \beta)} = f(d)g(\alpha)h(\beta)$ pour tout $(d, \alpha, \beta) \in F_2$, on obtient

$$[f \ T \ (g \ T \ h)](n) = \sum_{(d, d', \alpha, \beta) \in F_1} a_{\varphi(d, d', \alpha, \beta)} = \sum_{c \in F_2} a_c.$$

$$\text{Ceci montre que } [f \ T \ (g \ T \ h)](n) = \sum_{\substack{1 \leq d, d', d'' \leq n \\ dd'd'' = n}} f(d)g(d')h(d'').$$

Ainsi $f \ T \ (g \ T \ h)$ ne dépend pas de l'ordre de (f, g, h) .

En particulier, $f T (g T h) = h T (f T g)$, puis par commutativité, $f T (g T h) = (f T g) T h$. Ceci prouve l'associativité.

6°) a) Soit $n \in \mathbb{N}^*$ avec $n \geq 2$.

Soit d un diviseur de n . Ainsi, il existe $\beta_1, \dots, \beta_k \in \mathbb{N}$ tels que $d = \prod_{i=1}^k p_i^{\beta_i}$ avec $\beta_i \leq \alpha_i$ pour tout $i \in \mathbb{N}_k$. S'il existe $i \in \mathbb{N}_k$ tel que $\beta_i \geq 2$, alors $\mu(d) = 0$, donc les seuls diviseurs d de n pour lesquels $\mu(d) \neq 0$ sont de la forme $d = \prod_{i \in I} p_i$, où $I \subset \mathbb{N}_k$, et dans

ce cas, $\mu(d) = (-1)^{|I|}$.

L'application $I \mapsto \prod_{i \in I} p_i$ est donc une bijection de $\mathcal{P}(\mathbb{N}_k)$ dans l'ensemble des diviseurs

d de n tels que $\mu(d) \neq 0$. Ainsi, par changement de variable,

$$(\mu T z)(n) = \sum_{\substack{1 \leq d \leq n \\ d \mid n}} \mu(d) = \sum_{I \subset \mathbb{N}_k} (-1)^{|I|}, \text{ puis par sommation par paquets,}$$

$$(\mu T z)(n) = \sum_{h=0}^k \sum_{\substack{I \subset \mathbb{N}_k \\ |I|=h}} (-1)^h = \sum_{h=0}^k \binom{k}{h} (-1)^h = (1-1)^k \text{ d'après la formule du binôme}$$

de Newton. Or $k \geq 1$, car $n \geq 2$, donc $(\mu T z)(n) = 0$.

De plus $(\mu T z)(1) = \mu(1)z(1) = 1$, donc $\mu T z = e$.

T étant commutative, ceci prouve que z est l'inverse de μ pour la loi T .

b) Soit $f, g \in A$. Il s'agit de montrer que $f = g T z \iff g = \mu T f$:

Si $f = g T z$, alors $\mu T f = \mu T (g T z) = (\mu T z) T g = e T g = g$ et réciproquement, si $g = \mu T f$, alors $g T z = (f T \mu) T z = f T (\mu T z) = f T e = f$.

7°) a) $\diamond$ Soit φ un mot de longueur n . Alors pour tout $i \in \mathbb{N}_n$, $\varphi(i+n) = \varphi(i)$, donc $\varphi R \varphi$: R est une relation réflexive.

$\diamond$ Soit φ et φ' deux mots de longueur n tels que $\varphi R \varphi'$. Ainsi, il existe $p \in \mathbb{N}^*$ tel que, pour tout $i \in \mathbb{N}_n$, $\varphi'(i) = \varphi(i+p)$.

Il existe $q \in \mathbb{N}^*$ tel que $-p \equiv q [n]$. Alors, pour tout $i \in \mathbb{N}_n$, $\varphi(i) = \varphi'(i-p) = \varphi'(i+q)$, donc $\varphi' R \varphi$: R est une relation symétrique.

$\diamond$ Soit φ, φ' et φ'' trois mots de longueur n tels que $\varphi R \varphi'$ et $\varphi' R \varphi''$. Il existe $p, q \in \mathbb{N}^*$ tels que, pour tout $i \in \mathbb{N}_n$, $\varphi'(i) = \varphi(i+p)$ et $\varphi''(i) = \varphi'(i+q)$. Alors, pour tout $i \in \mathbb{N}_n$, $\varphi''(i) = \varphi(i+q+p)$, donc $\varphi R \varphi''$: R est une relation transitive.

$\diamond$ En conclusion, R est une relation d'équivalence.

b) $\diamond$ Lors de la définition d'une période p d'un mot circulaire $\overline{\varphi}$, l'énoncé sous-entend que la propriété " $\forall i \in \mathbb{N}_n, \varphi(i) = \varphi(i+p)$ " ne dépend que de $\overline{\varphi}$. Démontrons-le :

Soit φ, φ' deux mots de longueur n tels que $\varphi R \varphi'$: il existe $q \in \mathbb{N}^*$ tel que, pour tout $i \in \mathbb{N}_n$, $\varphi'(i) = \varphi(i+q)$.

Supposons de plus qu'il existe $p \in \mathbb{N}^*$ tel que, pour tout $i \in \mathbb{N}_n$, $\varphi(i) = \varphi(i+p)$.

Alors, pour tout $i \in \mathbb{N}_n$, $\varphi'(i) = \varphi(i+q) = \varphi(i+q+p) = \varphi'(i+p)$, ce qui fallait démontrer.

◇ Notons P l'ensemble des périodes de φ . D'après les définitions de l'énoncé, $n \in P$, donc P est une partie non vide de $\mathbb{N}^*$. À ce titre, elle possède bien un minimum, que l'on note p_0 .

◇ Par division euclidienne de n par p_0 , on peut écrire $n = p_0q + r$ avec $q \in \mathbb{N}$ et $0 \leq r < p_0$.

Pour tout $i \in \mathbb{N}_n$, $\varphi(i) = \varphi(i + n) = \varphi(i + r + p_0q) = \varphi(i + r)$, car on peut montrer par récurrence sur q que, pour tout $q \in \mathbb{N}^*$, p_0q est une période. Ainsi, si r est non nul, c'est un élément de P avec $r < p_0 = \min(P)$. C'est impossible, donc $r = 0$ et p_0 divise n .

c) Notons $\mathcal{M}_{p,n}$ l'ensemble des mots circulaires de longueur n et de période primitive p . Alors on peut vérifier que l'application $f : \mathcal{M}_{p,n} \longrightarrow \frac{\mathcal{M}_{p,p}}{\varphi|_{\mathbb{N}_p}}$ est correctement définie et que c'est une bijection. Ainsi, le nombre de mots circulaires de longueur n et de période primitive p ne dépend pas de n , tant que n est un multiple de p . On peut donc le noter $M(p)$, et $M \in A$.

Notons $f : \mathbb{N}^* \longrightarrow \mathbb{Z}$ définie par $f(n) = m^n$ et $g : \mathbb{N}^* \longrightarrow \mathbb{Z}$ définie par $g(p) = pM(p)$. Il s'agit donc de montrer que $g = \mu T f$, ou bien d'après la question 6.b, que $f = g T z$, c'est-à-dire que, pour tout $n \in \mathbb{N}^*$, $m^n = \sum_{\substack{1 \leq d \leq n \\ d | n}} dM(d)$.

Soit $n \in \mathbb{N}^*$. Pour tout $d \in \mathbb{N}^*$ tel que $d | n$, notons $M_{d,n}$ l'ensemble des éléments de $\mathbb{N}_m^{\mathbb{N}_n}$ dont le mot circulaire associé admet d pour période primitive.

Alors (1) : $\mathbb{N}_m^{\mathbb{N}_n} = \bigsqcup_{\substack{1 \leq d \leq n \\ d | n}} M_{d,n}$.

Par ailleurs, si l'on note F l'application $\begin{matrix} M_{d,n} & \longrightarrow & \mathcal{M}_{d,n} \\ \varphi & \longmapsto & \bar{\varphi} \end{matrix}$, pour tout $r \in \mathcal{M}_{d,n}$, $F^{-1}(\{r\})$ est de cardinal d : en effet, si $\bar{\varphi} = r$, les mots de la classe d'équivalence sont les $\varphi_k : i \longmapsto \varphi(i + k)$, où $k \in \{0, \dots, n-1\}$, mais $\varphi_k = \varphi_h$ avec $k \neq h$ si et seulement si $|k - h|$ est une période de $\bar{\varphi}$, donc $\bar{\varphi} = \{\varphi_0, \varphi_1, \dots, \varphi_{d-1}\}$ et ces éléments sont deux à deux distincts.

Ainsi, d'après le principe des bergers, $|M_{d,n}| = d|\mathcal{M}_{d,n}| = dM(d)$. Alors la formule (1) donne, en passant aux cardinaux, $m^n = \sum_{\substack{1 \leq d \leq n \\ d | n}} dM(d)$, ce qu'il fallait démontrer.

Partie III : Utilisation de fonctions génératrices

8°) Soit $m \in \mathbb{N}^*$ et $x \in \mathbb{R}$. Soit $N \in \mathbb{N}^*$.

D'après la question 3.b, qui est également valable lorsque $m > n$, car l'hypothèse $m \leq n$ n'est pas utilisée pour montrer cette question,

$$\sum_{n=0}^N S_n^m \frac{x^n}{n!} = \frac{1}{m!} \sum_{n=0}^N \frac{x^n}{n!} \sum_{k=0}^m (-1)^k \binom{m}{k} (m-k)^n = \frac{1}{m!} \sum_{k=0}^m (-1)^k \binom{m}{k} \sum_{n=0}^N \frac{[x(m-k)]^n}{n!},$$

donc

$$\begin{aligned} \sum_{n=0}^N S_n^m \frac{x^n}{n!} &\xrightarrow{N \rightarrow +\infty} \frac{1}{m!} \sum_{k=0}^m (-1)^k \binom{m}{k} e^{x(m-k)} \\ &= \frac{1}{m!} \sum_{k=0}^m (-1)^k \binom{m}{k} (e^x)^{m-k} \\ &= \frac{1}{m!} (e^x - 1)^m \end{aligned}$$

d'après la formule du binôme de Newton. Ceci prouve que la série $\sum S_n^m \frac{x^n}{n!}$ est convergente et que

$$\sum_{n=0}^{+\infty} S_n^m \frac{x^n}{n!} = \frac{1}{m!} (e^x - 1)^m.$$

9°) Soit $n \geq 3$. Notons $\mathcal{I}_n$ l'ensemble des injections de $\mathbb{N}_n$. Alors

$$(2) : \mathcal{I}_n = \bigsqcup_{1 \leq i \leq n} \mathcal{I}_{i,n} \text{ où } \mathcal{I}_{i,n} = \{f \in \mathcal{I}_n / f(n) = i\}.$$

Lorsque $i = n$, pour construire une involution f de $\mathcal{I}_{n,n}$, telle que $f(n) = n$, il suffit de construire sa restriction à $\mathbb{N}_{n-1}$ qui est une involution de $\mathcal{I}_{n-1}$, donc $|\mathcal{I}_{n,n}| = I_{n-1}$.

Lorsque $i \in \{1, \dots, n-1\}$, pour construire une involution f de $\mathcal{I}_{i,n}$, telle que $f(n) = i$ et donc $f(i) = n$, il suffit de construire sa restriction à $\mathbb{N}_{n-1} \setminus \{i\}$ qui est une involution sur un ensemble de cardinal $n-2$, donc $|\mathcal{I}_{i,n}| = I_{n-2}$. Ainsi, en passant aux cardinaux dans la formule (2), on obtient que $I_n = I_{n-1} + (n-1)I_{n-2}$.

$$10^\circ) \text{ Soit } n \in \mathbb{N}. \text{ D'après l'énoncé, } f^{(n)}(x) = \sum_{k=0}^{+\infty} a_k \frac{d^n}{dx^n}(x^k) = \sum_{k=n}^{+\infty} a_k \frac{k!}{(k-n)!} x^{k-n},$$

donc $f^{(n)}(0) = n!a_n$.

11°) Soit $n \in \mathbb{N}$. L'ensemble des involutions de $\mathbb{N}_n$ est inclus dans l'ensemble $\mathcal{S}_n$ des permutations de $\mathbb{N}_n$, donc $I_n \leq |\mathcal{S}_n| = n!$.

Soit $r \in]0, 1[$. Soit $N \in \mathbb{N}$. $\sum_{n=0}^N \frac{I_n}{n!} r^n \leq \sum_{n=0}^N r^n = \frac{1-r^{N+1}}{1-r} \leq \frac{1}{1-r}$, donc la suite

$\left(\sum_{n=0}^N \frac{I_n}{n!} r^n\right)_{N \in \mathbb{N}}$ est une suite majorée, mais elle est aussi croissante car $\frac{I_n}{n!} r^n \geq 0$, donc

elle est convergente, ce qui prouve que $S(r)$ est défini.

12°) Soit $x \in]-1, 1[$. Il existe $r \in]|x|, 1[$. D'après la question précédente, $S(r)$ est défini, donc d'après la question 10, l'application S est de classe C^∞ sur $] -r, r[$. En

particulier, S est dérivable en x et, toujours d'après la question 10,

$$S'(x) = \sum_{n=0}^{+\infty} \frac{I_n}{n!} \frac{d}{dx}(x^n) = \sum_{n=1}^{+\infty} I_n \frac{x^{n-1}}{(n-1)!} = \sum_{n=0}^{+\infty} I_{n+1} \frac{x^n}{n!}, \text{ donc}$$

$$S'(x) = I_1 + I_2x + \sum_{n=2}^{+\infty} (I_n + nI_{n-1}) \frac{x^n}{n!} = I_1 + I_2x + \sum_{n=2}^{+\infty} I_n \frac{x^n}{n!} + x \sum_{n=1}^{+\infty} I_n \frac{x^{n-1}}{(n-1)!}, \text{ or } I_1 = 1 \text{ et } I_2 = 2, \text{ donc } S'(x) = 1 + 2x + (S(x) - x) + xS(x) = (1+x) + S(x)(1+x) = (1+x)(S(x)+1).$$

13°) Notons $g : x \mapsto (S(x) + 1)e^{-x - \frac{x^2}{2}}$. g est dérivable sur $] -1, 1[$ et $g'(x) = e^{-x - \frac{x^2}{2}}(S'(x) + (S(x) + 1)(-1 - x)) = 0$, donc g est une application constante sur $] -1, 1[$. Or $g(0) = 1$, donc pour tout $x \in] -1, 1[$, $S(x) = e^{x + \frac{x^2}{2}} - 1$.

14°) Soit $n \in \mathbb{N}^*$.

Pour tout $x \in] -1, 1[$, $e^{x + \frac{x^2}{2}} - 1 = S(x) = \sum_{n=0}^{+\infty} \frac{I_n}{n!} x^n$, donc d'après la question 10,

$I_n = S^{(n)}(0)$, puis d'après la formule de Leibniz,

$$I_n = \sum_{k=0}^n \binom{n}{k} \left[\frac{d^{n-k}}{dx^{n-k}}(e^x) \times \frac{d^k}{dx^k}(e^{\frac{x^2}{2}}) \right](0) = \sum_{k=0}^n \binom{n}{k} \left[\frac{d^k}{dx^k}(e^{\frac{x^2}{2}}) \right](0).$$

Par ailleurs, $e^{\frac{x^2}{2}} = \sum_{n=0}^{+\infty} \left(\frac{x^2}{2}\right)^n \frac{1}{n!} = \sum_{n=0}^{+\infty} a_n x^n$, avec $a_{2n} = \frac{1}{2^n n!}$ et $a_{2n+1} = 0$, pour tout

$n \in \mathbb{N}$. Ainsi, toujours d'après la question 10, pour tout $k \in \mathbb{N}$, $\left[\frac{d^k}{dx^k}(e^{\frac{x^2}{2}}) \right](0) = k! a_k$,

$$\text{donc } I_n = \sum_{0 \leq 2k \leq n} \binom{n}{2k} (2k)! \frac{1}{2^k k!} = \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} \frac{n!}{2^k k! (n-2k)!}.$$

15°) Lorsque f est une involution de $\mathbb{N}_n$,

le nombre d'éléments de $\mathbb{N}_n$ non fixes par f est pair.

En effet, informellement, si a est un élément de $\mathbb{N}_n$ non fixe par f ,

alors $f(a) \neq a$ et $f(f(a)) = a \neq f(a)$, donc $f(a)$ est un second élément de $\mathbb{N}_n$ non fixe par f . Ainsi on peut regrouper par paires les éléments non fixes de f .

On peut formaliser ce raisonnement en utilisant la relation binaire R suivante sur $\mathbb{N}_n$: lorsque $x, y \in \mathbb{N}_n$, on convient que $x R y$ si et seulement si il existe $k \in \mathbb{Z}$ tel que $y = f^k(x)$, où f^k désigne f composée avec elle-même k fois lorsque $k \geq 0$ et où $f^k = (f^{-1})^{-k}$ lorsque k est négatif.

On vérifie que R est une relation d'équivalence. Lorsque x est un point fixe de f , la classe d'équivalence est égale à $\{x\}$ et sinon, $\bar{x} = \{x, f(x)\}$. Or les classes d'équivalence sont disjointes, donc si l'on note k le nombre de classes d'équivalence de cardinal 2, le nombre de points non fixes par f est égal à $2k$.

Ainsi, pour construire une involution f quelconque de $\mathbb{N}_n$, on commence par choisir $k \in \mathbb{N}$ tel que $2k \leq n$, où $2k$ va désigner le nombre d'éléments de $\mathbb{N}_n$ non fixes par f , puis on choisit l'ensemble I de ces points non fixes, ce qui revient à choisir $2k$ éléments

parmi n , soit $\binom{n}{2k}$ choix. Ensuite, on prend le minimum de I noté m_1 et on choisit son image par f dans I , notée m_2 (il y a $2k - 1$ choix de m_2), puis on applique le même procédé en remplaçant I par $I \setminus \{m_1, m_2\}$ (il y a $2k - 3$ choix) et l'on continue jusqu'à ce que l'ensemble des points non fixes restants soit vide. On obtient par ce procédé de construction toutes les involutions exactement une fois, donc $I_n = \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} \alpha_k$,

où $\alpha_k = \binom{n}{2k} (2k - 1)(2k - 3) \cdots 3$.

Or, pour tout $k \in \{0, \dots, \lfloor \frac{n}{2} \rfloor\}$, $a_k = \frac{n!}{(2k)!(n - 2k)!} \times \frac{(2k)!}{(2k)(2k - 2) \cdots 2} = \frac{n!}{(n - 2k)! 2^k k!}$.
On retrouve bien ainsi la formule de la question précédente.