DS 4 : un corrigé

Barème

Exercice 1 : 3, Exercice 2 : 3, Exercice 3 : 3.
Problème Partie I : 1, 2, 2, 4, 2, 3, 3.
Partie 2 : 2, 2, 4, 3, 2, 2, 3.
Partie 3 : 2, 4, 4, 4.

Exercices

Exercice 1 :

11 est un nombre premier et $7 \not\equiv 0[11]$, donc
d'après le petit théorème de Fermat, $7^{10} \equiv 1[11]$.
De plus, modulo 10, $7^2 = 49 \equiv -1$, donc $7^4 \equiv 1$ puis $7^7 \equiv 7^4 \times 7^2 \times 7 \equiv 3$. Ainsi, il existe $k \in \mathbb{N}$ tel que $7^7 = 3 + 10k$. Alors, modulo 11,
$7^{(7^7)} = 7^3 \times (7^{10})^k \equiv 7^3 \equiv (-4)^3 = -16 \times 4 \equiv -5 \times 4$.
Finalement, $\boxed{\text{le chiffre des unités de } 7^{(7^7)} \text{ en base 11 est égal à 2}}$.

Exercice 2 :

◇ Si α existe, en multipliant cette égalité par n on obtient que $\dfrac{1}{n(n+1)} = \alpha + \dfrac{n}{n+1} + \dfrac{1}{n}$ puis en faisant tendre n vers $+\infty$, on obtient $0 = \alpha + 1$. Ainsi, si α existe, alors $\alpha = -1$.
On vérifie que, pour tout $n \in \mathbb{N}^*$,
$\dfrac{-1}{n} + \dfrac{1}{n+1} + \dfrac{1}{n^2} = -\dfrac{1}{n(n+1)} + \dfrac{1}{n^2} = \dfrac{-n + (n+1)}{n^2(n+1)} = \dfrac{1}{n^2(n+1)}$.

◇ Soit $N \in \mathbb{N}^*$. $\displaystyle\sum_{n=1}^{N} \frac{1}{n^2(n+1)} = \sum_{n=1}^{N} \frac{1}{n^2} + \sum_{n=1}^{N} \left(\frac{1}{n+1} - \frac{1}{n}\right) = \left(\sum_{n=1}^{N} \frac{1}{n^2}\right) + \frac{1}{N+1} - 1$,

donc $\displaystyle\sum_{n=1}^{N} \frac{1}{n^2(n+1)} \underset{N\to+\infty}{\longrightarrow} \frac{\pi^2}{6} - 1$.

Ceci prouve que la série $\displaystyle\sum_{n\geq 1} \frac{1}{n^2(n+1)}$ converge et que $\boxed{\displaystyle\sum_{n=1}^{+\infty} \frac{1}{n^2(n+1)} = \frac{\pi^2}{6} - 1}$.

Exercice 3 :

Soit $k \in \mathbb{N}$. Notons $R(k)$ l'assertion suivante : pour tout $x \in \mathbb{R}_+^*$, $\frac{d^k}{dx^k}\left(\frac{1}{x}\right) = \frac{(-1)^k k!}{x^{k+1}}$.
Pour $k = 0$, $f^{(0)}(x) = f(x)$, d'où $R(0)$.
Pour $k \geq 0$, supposons $R(k)$. Alors, pour tout $x \in \mathbb{R}_+^*$,
$f^{(k+1)}(x) = \frac{d}{dx}\left(\frac{(-1)^k k!}{x^{k+1}}\right) = \frac{(-1)^{k+1}(k+1)!}{x^{k+2}}$.
Ainsi, d'après le principe de récurrence,
pour tout $k \in \mathbb{N}$ et $x \in \mathbb{R}_+^*$, $\frac{d^k}{dx^k}\left(\frac{1}{x}\right) = \frac{(-1)^k k!}{x^{k+1}}$.
Alors, d'après la formule de Leibniz, pour tout $x \in \mathbb{R}_+^*$,

$$\begin{aligned} f^{(n)}(x) &= \sum_{k=0}^{n} \binom{n}{k} \frac{d^k}{dx^k}\left(\frac{1}{x}\right) \frac{d^{n-k}}{dx^{n-k}}(e^{-x}) \\ &= \sum_{k=0}^{n} \binom{n}{k} \frac{(-1)^k k!}{x^{k+1}} (-1)^{n-k} e^{-x} \\ &= e^{-x}(-1)^n \sum_{k=0}^{n} \frac{n!}{(n-k)!} \frac{1}{x^{k+1}}. \end{aligned}$$

En particulier, $f^{(n)}(1) = \frac{(-1)^n n!}{e} \sum_{h=0}^{n} \frac{1}{(n-h)!}$, puis en posant $k = n - h$, on obtient $f^{(n)}(1) = \frac{(-1)^n n!}{e} \sum_{k=0}^{n} \frac{1}{k!}$.

Problème : Formule d'inversion de Rota

1°) Soit $x, y, z \in E$ tels que $x < y$ et $y < z$.
Alors $x \leq y$ et $y \leq z$, donc par transitivité de la relation d'ordre $\leq$, $x \leq z$.
Supposons que $x = z$. Alors $x \leq y$ et $y \leq x$, donc par antisymétrie de $\leq$, $x = y$, ce qui est faux. Ainsi, $x \neq z$ et $x \leq z$, ce qui montre que $x < z$.
La relation binaire $<$ est donc bien transitive.

2°) $\diamond$ Supposons qu'il existe une chaîne de longueur p joignant x à lui-même, notée $(x_i)_{0 \leq i \leq p}$. Pour tout $i \in \{0, \ldots, p-1\}$, $x_i < x_{i+1}$. Par récurrence sur i, à l'aide de la question 1, on montre que, pour tout $i \in \{0, \ldots, p-1\}$, $x_0 < x_{i+1}$. En particulier, pour $i = p - 1$ (on a bien $p - 1 \geq 0$, donc $p - 1 \in \{0, \ldots, p-1\}$), on obtient que $x = x_0 < x_p = x$, ce qui est faux. Ainsi, il n'existe aucune chaîne de longueur p joignant x à lui-même, ce qui prouve que $c_p(x, x) = 0$.
$\diamond$ Posons $p = 0$. Soit $x_0 \in E$. L'ensemble $\{0, \ldots, p-1\}$ est vide, donc (x_0) est une chaîne de longueur 0 joignant x à lui-même si et seulement si $x = x_0$ et $y = x_p = x_0$. Ainsi (x) est l'unique chaîne de longueur 0 joignant x à lui-même et $c_0(x, x) = 1$.

3°) $\diamond$ $\boxed{\text{On suppose que } \neg(x < y)}$.
En adaptant le premier point de la question précédente, on voit que s'il existe une chaîne de longueur p joignant x à y, avec $p \geq 1$, alors $x < y$, ce qui est faux. Ainsi, $\boxed{\text{lorsque } p \geq 1,\ c_p(x, y) = 0}$.
En adaptant le second point de la question précédente, lorsque $p = 0$, on voit qu'il existe une chaîne de longueur 0 joignant x à y si et seulement si $x = y$ et que dans ce cas elle est unique, donc $\boxed{c_0(x, x) = 1 \text{ et } c_0(x, y) = 0 \text{ lorsque } x \neq y.}$

$\diamond$ D'après le point précédent, $\boxed{\text{lorsque } \neg(x < y),\ c_1(x, y) = 0}$.
Supposons maintenant que $x < y$. Soit $x_0, x_1 \in E$. Alors (x_0, x_1) est une chaîne de longueur 1 joignant x à y si et seulement si $x_0 = x$, $x_1 = y$ et $x < y$. Ainsi (x, y) est l'unique chaîne joignant x à y ; $\boxed{\text{lorsque } x < y,\ c_1(x, y) = 1.}$

4°) $\diamond$ Posons $D = \displaystyle\bigcup_{\substack{z \in E \text{ tel que} \\ x \leq z < y}} C_p(x, z)$.
Lorsque $(x_0, \ldots, x_{p+1}) \in C_{p+1}(x, y)$, posons $f(x_0, \ldots, x_{p+1}) = (x_0, \ldots, x_p)$.
$x_p < x_{p+1} = y$, donc $f(x_0, \ldots, x_{p+1}) \in C_p(x, x_p) \subset D$. Ainsi, f est une application de $C_{p+1}(x, y)$ dans D.
Soit $X \in D$. Il existe $z \in E$ avec $x \leq z < y$ tel que $X \in C_p(x, z)$. Alors X est de la forme $(x_0, \ldots, x_p)$ avec $x = x_0 < x_1 < \cdots < x_p = z$. On pose alors $g(X) = (x_0, \ldots, x_p, y)$. Clairement, $g(X) \in C_{p+1}(x, y)$. Ainsi, g est une application de D dans $C_{p+1}(x, y)$.
Il est clair que pour tout $(x_0, \ldots, x_{p+1}) \in C_{p+1}(x, y)$,
$(g \circ f)(x_0, \ldots, x_{p+1}) = g(x_0, \ldots, x_p) = (x_0, \ldots, x_{p+1})$, donc $g \circ f = Id_{C_{p+1}(x,y)}$ et de même on montre que $f \circ g = Id_D$. Ceci démontre que f et g sont des bijections réciproques l'une de l'autre.

$\diamond$ Soit $z, z' \in E$ tels que $x \leq z < y$ et $x \leq z' < y$. Soit $(x_0, \ldots, x_p) \in C_p(x, z) \cap C_p(x, z')$. Alors $z = x_p = z'$. Ainsi, par contraposition, on a montré que, lorsque $z \neq z'$, alors $C_p(x, z) \cap C_p(x, z') = \emptyset$. donc la famille $(C_p(x, z))_{x \leq z < y}$ constitue une partition de D (contenant éventuellement des ensembles vides). Or $C_{p+1}(x, y)$ et D sont en bijection, donc ils ont le même cardinal. Ainsi $c_{p+1}(x, y) = |D| = \displaystyle\sum_{x \leq z < y} c_p(x, z)$.

$\diamond$ De même, lorsque $(x_0, \ldots, x_{p+1}) \in C_{p+1}(x, y)$, posons $h(x_0, \ldots, x_{p+1}) = (x_1, \ldots, x_{p+1})$.
En adaptant ce qui précède, on montre que h est une bijection de $C_{p+1}(x, y)$ dans $\displaystyle\bigcup_{\substack{z \in E \text{ tel que} \\ x < z \leq y}} C_p(z, y)$, qui est une réunion disjointe, donc en passant aux cardinaux, on obtient $c_{p+1}(x, y) = \displaystyle\sum_{x < z \leq y} c_p(z, y)$.

5°) Soit $x, y \in E$. Soit $p \in \mathbb{N}$. Supposons que $C_p(x, y)$ est non vide.
Il existe donc $(x_0, \ldots, x_p) \in E$ tels que $x_0 < \cdots < x_p$.
Soit $i, j \in \{0, \ldots, p\}$ tel que $i \neq j$. Sans perte de généralité, on peut supposer que $i < j$. Alors par transivité de la relation $<$, on a $x_i < x_j$, donc $x_i \neq x_j$. Ainsi, $\{x_0, \ldots, x_p\}$ est une partie de E de cardinal $p + 1$. Ceci montre que $C_p(x, y) \neq \emptyset \Longrightarrow p + 1 \leq N$. Par contraposée, lorsque $p \geq N$, $C_p(x, y) = \emptyset$ et $c_p(x, y) = 0$.

6°) $\diamond$ Soit $x \in E$. On a vu que $c_0(x,x) = 1$ et que, pour tout $p \geq 1$, $c_p(x,x) = 0$, donc $\boxed{\mu(x,x) = 1}$.

$\diamond$ Soit $x, y \in E$ avec $x < y$.

$$\begin{aligned}\sum_{x \leq z \leq y} \mu(x,z) &= \sum_{x \leq z \leq y} \sum_{p=0}^{N-1} (-1)^p c_p(x,z) = \sum_{p=0}^{N-1} (-1)^p \sum_{x \leq z \leq y} c_p(x,z) \\ &= \sum_{p=0}^{N-1} (-1)^p \Big(c_p(x,y) + \sum_{x \leq z < y} c_p(x,z) \Big),\end{aligned}$$

donc d'après la question 4, $\displaystyle\sum_{x \leq z \leq y} \mu(x,z) = \sum_{p=0}^{N-1} ((-1)^p c_p(x,y) - (-1)^{p+1} c_{p+1}(x,y))$.

Il s'agit d'une somme télescopique, donc

$\displaystyle\sum_{x \leq z \leq y} \mu(x,z) = (-1)^0 c_0(x,y) - (-1)^N c_N(x,y) = 0$, d'après les questions 3 et 5.

$\diamond$ On effectue un calcul similaire, en utilisant cette fois la relation

$\displaystyle\sum_{x \leq z \leq y} c_p(z,y) = c_p(x,y) + \sum_{x < z \leq y} c_p(z,y)$:

$$\begin{aligned}\sum_{x \leq z \leq y} \mu(z,y) &= \sum_{x \leq z \leq y} \sum_{p=0}^{N-1} (-1)^p c_p(z,y) = \sum_{p=0}^{N-1} (-1)^p \sum_{x \leq z \leq y} c_p(z,y) \\ &= \sum_{p=0}^{N-1} (-1)^p \Big(c_p(x,y) + \sum_{x < z \leq y} c_p(z,y) \Big) \\ &= \sum_{p=0}^{N-1} ((-1)^p c_p(x,y) - (-1)^{p+1} c_{p+1}(x,y)) = 0.\end{aligned}$$

7°) $\diamond$ Soit $x \in E$. $\displaystyle\sum_{y \leq x} \mu(y,x) g(y) = \sum_{y \leq x} \sum_{z \leq y} \mu(y,x) f(z) = \sum_{\substack{(y,z) \in E^2 \text{ tel que} \\ z \leq y \leq x}} \mu(y,x) f(z)$.

En effet, $\{(y,z) \in E^2 \ / \ z \leq y \leq x\} = \displaystyle\bigsqcup_{\substack{y \in E \text{ tel que} \\ y \leq x}} \{y\} \times \{z \in E \ / \ z \leq y\}$, donc l'égalité précédente est un cas particulier de sommation par paquets. Mais on a également $\{(y,z) \in E^2 \ / \ z \leq y \leq x\} = \displaystyle\bigsqcup_{\substack{z \in E \text{ tel que} \\ z \leq x}} \{y \in E \ / \ z \leq y \leq x\} \times \{z\}$,

donc $\displaystyle\sum_{y \leq x} \mu(y,x) g(y) = \sum_{z \leq x} \sum_{z \leq y \leq x} \mu(y,x) f(z) = \sum_{z \leq x} f(z) \sum_{z \leq y \leq x} \mu(y,x)$. Or d'après la question précédente, pour tout $z \in E$ tel que $z < x$, $\displaystyle\sum_{z \leq y \leq x} \mu(y,x) = 0$ et pour $z = x$,

$\displaystyle\sum_{z \leq y \leq x} \mu(y,x) = \sum_{x \leq y \leq x} \mu(y,x) = \mu(x,x) = 1$, donc $\displaystyle\sum_{y \leq x} \mu(y,x) g(y) = f(x)$, ce qu'il fallait démontrer.

$\diamond$ Pour tout $x, y \in E$, on convient (classiquement) que $x \geq y$ si et seulement si $y \leq x$. Alors $\geq$ est également une relation d'ordre.

Pour tout $x, y \in E$ et $p \in E$, il est clair que $(x_0, \dots, x_p)$ est une chaîne joignant x à y pour $\leq$ si et seulement si $(x_p, \dots, x_0)$ est une chaîne joignant y à x pour $\geq$.
Ainsi, en notant $c'_p(y, x)$ le nombre de chaînes de longueur p joignant y à x pour $\geq$, on a $c'_p(y, x) = c_p(x, y)$.
Notons μ' la fonction de Möbius associée à $\geq$.
Alors, pour tout $x, y \in E$, $\mu'(x, y) = \sum_{p \in \mathbb{N}} (-1)^p c'_p(x, y) = \mu(y, x)$.
On applique le point précédent en remplaçant $\leq$ par $\geq$. Il convient alors de remplacer g par h et μ par μ', donc $f(x) = \sum_{y \geq x} \mu'(y, x) h(y) = \sum_{y \geq x} \mu(x, y) h(y)$, ce qu'il fallait démontrer.

Partie II : Applications

8°)

8.a : Pour construire une chaîne $(x_0, \dots, x_p)$ de longueur p joignant i à j, il suffit de choisir $x_1, \dots, x_{p-1}$ tels que $i < x_1 < x_2 < \cdots < x_{p-1} < j$, c'est-à-dire qu'il suffit de choisir une partie de $p-1$ éléments $\{x_1, \dots, x_{p-1}\}$ parmi $\{i+1, i+2, \dots, j-1\}$ (qui est de cardinal $(j-1)-(i+1)+1 = j-i-1$) que l'on ordonne pour construire la chaîne $(x_1, \dots, x_{p-1})$. Ainsi, $c_p(i, j) = \begin{pmatrix} j-i-1 \\ p-1 \end{pmatrix}$.
Remarquons que le raisonnement reste valable lorsque $p > j - i$, mais dans ce cas il n'existe aucune partie de $p-1$ éléments parmi $\{i+1, i+2, \dots, j-1\}$, donc on obtient alors que $c_p(i, j) = 0$.

8.b : $\diamond$ Soit $i, j \in \mathbb{N}_n$. Alors $\mu(i, j) = \sum_{p=0}^{n-1} (-1)^p c_p(i, j)$.
Supposons d'abord que $i > j$. Alors pour tout $p \in \mathbb{N}$, $c_p(i, j) = 0$, donc $\mu(i, j) = 0$.
Supposons ensuite que $i = j$. Alors d'après la question 6, $\mu(i, i) = 1$.
Supposons que $j = i + 1$. Alors $c_0(i, i+1) = 0$, $c_1(i, i+1) = 1$ et pour tout $p \geq 2$, $c_p(i, i+1) = 0$, donc $\mu(i, i+1) = -1$.
Enfin, supposons que $j > i + 1$. Soit $p \in \mathbb{N}^*$. On sait que $c_0(i, j) = 0$, donc d'après 8.a, $\mu(i, j) = \sum_{p=1}^{j-i} (-1)^p \begin{pmatrix} j-i-1 \\ p-1 \end{pmatrix} = -\sum_{h=0}^{j-i-1} \begin{pmatrix} j-i-1 \\ h \end{pmatrix} (-1)^h$. Ainsi, d'après la formule du binôme de Newton, $\mu(i, j) = -(1-1)^{j-i-1} = 0$, car $j - i - 1 > 0$.
$\diamond$ Soit f une application de $\mathbb{N}_n$ dans $\mathbb{C}$.
Pour tout $i \in \mathbb{N}_n$, on pose $g(i) = \sum_{j=1}^{i} f(j)$ et $h(i) = \sum_{j=i}^{n} f(j)$.
Soit $i \in \mathbb{N}_n$. Alors la formule de Rota affirme que, $f(i) = \sum_{j=1}^{i} \mu(j, i) g(j) = \sum_{j=i}^{n} \mu(i, j) h(j)$,
c'est-à-dire que $\boxed{f(i) = g(i) - g(i-1) = h(i) - h(i+1)}$, en convenant que

$g(0) = 0 = h(n+1)$. Ces relations sont évidentes ...

9°) 9.a : $\diamond$ Soit $k \in \mathbb{N}$. Notons $R(k)$ l'assertion suivante :
Pour tout $A, B \in E$ telles que $A \subset B$ et $|B| - |A| = k$, $\mu(A, B) = (-1)^k$.
Supposons que $k = 0$. Soit $A, B \in E$ telles que $A \subset B$ et $|B| - |A| = 0$. Alors d'après le cours, $A = B$, donc d'après la question 6, $\mu(A, B) = \mu(A, A) = 1 = (-1)^0$, ce qui prouve $R(0)$.
Pour $k \in \mathbb{N}$, on suppose que $R(h)$ est vraie pour tout $h \in \{0, \ldots, k\}$.
Soit $A, B \in E$ telles que $A \subset B$ et $|B| - |A| = k+1$. D'après la question 6, $\displaystyle\sum_{\substack{D \in E \text{ tel que} \\ A \subset D \subset B}} \mu(A, D) = 0$, donc $\mu(A, B) = -\displaystyle\sum_{\substack{D \in E \text{ tel que} \\ A \subset D \subset B \text{ et } D \neq B}} \mu(A, D)$.
Soit $D \in E$ tel que $A \subset D \subset B$ avec $D \neq B$. Alors $|D| - |A| < |B| - |A| = k+1$, donc $|D| - |A| \leq k$. Alors, d'après l'hypothèse de récurrence forte, $\mu(A, D) = (-1)^{|D|-|A|}$.
On en déduit que $\mu(A, B) = -\displaystyle\sum_{k=|A|}^{|B|-1} \sum_{\substack{D \in E \text{ tel que} \\ A \subset D \subset B \text{ et } |D| = k}} (-1)^{k-|A|} = (-1)^{|B|-|A|} - (-1)^{|A|} M$,
où $M = \displaystyle\sum_{k=|A|}^{|B|} \sum_{\substack{D \in E \text{ tel que} \\ A \subset D \subset B \text{ et } |D| = k}} (-1)^k = \sum_{k=|A|}^{|B|} (-1)^k \Big| \{D \in E \ / \ A \subset D \subset B \text{ et } |D| = k\} \Big|$. Or, si k est un entier compris entre $|A|$ et $|B|$, pour choisir une partie D de cardinal k telle que $A \subset D \subset B$, il suffit de choisir les $k - |A|$ éléments de $D \setminus A$ parmi $B \setminus A$, donc $\Big| \{D \in E \ / \ A \subset D \subset B \text{ et } |D| = k\} \Big| = \begin{pmatrix} |B| - |A| \\ k - |A| \end{pmatrix}$.
Ainsi, $M = \displaystyle\sum_{k=|A|}^{|B|} (-1)^k \begin{pmatrix} |B| - |A| \\ k - |A| \end{pmatrix} = (-1)^{|A|} \sum_{h=0}^{|B|-|A|} \begin{pmatrix} |B| - |A| \\ h \end{pmatrix} (-1)^h$, donc d'après la formule du binôme de Newton, $M = (-1)^{|A|}(1-1)^{|B|-|A|} = 0$ car $|B| - |A| = k+1 \neq 0$.
Finalement, on a montré que $\mu(A, B) = (-1)^{k+1}$, ce qui prouve $R(k+1)$.
Ceci démontre la propriété de l'énoncé par récurrence forte.
$\diamond$ Soit f une application de $E = \mathcal{P}(S)$ dans $\mathbb{C}$.
Pour tout $A \in E$, on pose $g(A) = \displaystyle\sum_{B \in \mathcal{P}(A)} f(B)$ et $h(A) = \displaystyle\sum_{A \subset B} f(B)$.
Alors la formule de Rota affirme que,
pour tout $A \in E$, $f(A) = \displaystyle\sum_{B \in \mathcal{P}(A)} (-1)^{|A|-|B|} g(B) = \sum_{A \subset B} (-1)^{|B|-|A|} h(B)$.

9.b Soit $n \in \mathbb{N}$. On pose $S = \mathbb{N}_n$ et $E = \mathcal{P}(S)$.
Pour tout $A \in E$, posons $f(A) = x_{|A|}$ et $g(A) = y_{|A|}$.
Soit $A \in E$. $g(A) = y_{|A|} = \displaystyle\sum_{k=0}^{|A|} \begin{pmatrix} |A| \\ k \end{pmatrix} x_k = \sum_{k=0}^{|A|} \sum_{\substack{B \in \mathcal{P}(A) \text{ tel que} \\ |B| = k}} x_{|B|}$, donc par sommation par paquets, $g(A) = \displaystyle\sum_{B \in \mathcal{P}(A)} f(B)$. On peut donc appliquer la formule de Rota de la

question précédente : Pour tout $A \in E$, $f(A) = \sum_{B \in \mathcal{P}(A)} (-1)^{|A|-|B|} g(B)$,

donc $x_{|A|} = \sum_{k=0}^{|A|} \sum_{\substack{B \in \mathcal{P}(A) \text{ tel que} \\ |B|=k}} (-1)^{|A|-k} y_k = \sum_{k=0}^{|A|} \binom{|A|}{k} (-1)^{|A|-k} y_k$.

En particulier, avec $A = \mathbb{N}_n$, on obtient $x_n = (-1)^n \sum_{k=0}^{n} \binom{n}{k} (-1)^k y_k$.

10°) $\diamond$ Soit $u = (u_1, \ldots, u_m) \in E$, $v = (v_1, \ldots, v_m) \in E$ et $w = (w_1, \ldots, w_m) \in E$.
$supp(u) \subset supp(u)$, donc $u \leq u$: la relation $\leq$ est réflexive.
Supposons que $u \leq v$ et $v \leq u$. Alors $supp(u) = supp(v)$, donc pour tout $i \in \mathbb{N}_m$, $u_i = 1 \iff v_i = 1$ et par contraposition, $u_i = 0 \iff v_i = 0$. Ainsi, pour tout $i \in \mathbb{N}_m$, $u_i = v_i$, donc $u = v$. Ainsi la relation $\leq$ est antisymétrique.
Supposons que $u \leq v$ et $v \leq w$. Alors par transitivité de la relation d'inclusion, $supp(u) \subset supp(w)$, donc $u \leq w$. Ainsi, $\leq$ est également transitive. C'est bien une relation d'ordre.
$\diamond$ Soit $p \in \mathbb{N}$ et $u, v \in E$. Alors $(w_0, \ldots, w_p)$ est un chemin de longueur p joignant u à v si et seulement si dans $\mathcal{P}(\mathbb{N}_m)$ muni de la relation d'inclusion, $(supp(w_0), \ldots, supp(w_p))$ est un chemin de longueur p joignant $supp(u)$ à $supp(v)$: en particulier le sens réciproque est vrai car on a vu lors de l'antisymétrie que si $supp(w_0) = supp(u)$, alors $w_0 = u$ et, de même, si $supp(w_p) = supp(v)$, alors $w_p = v$.
De plus, pour tout $U \subset \mathbb{N}_m$, il existe un unique $u \in E$ tel que $U = supp(u)$, donc l'application qui à $(w_0, \ldots, w_p)$ associe $(supp(w_0), \ldots, supp(w_p))$ est une bijection de $C_p(u, v)$ dans $C_p(supp(u), supp(v))$ en utilisant la même notation C_p pour les deux relations d'ordre sur E et sur $\mathcal{P}(\mathbb{N}_m)$. On en déduit que $c_p(u, v) = c_p(supp(u), supp(v))$, puis d'après la définition de la fonction de Möbius que $\mu(u, v) = \mu(supp(u), supp(v))$. Alors, d'après la question précédente appliquée avec $S = \mathbb{N}_m$, $\mu(u, v) = (-1)^{|supp(v)|-|supp(u)|}$.
Soit f une application de E dans $\mathbb{C}$.
Pour tout $u \in E$, on pose $g(u) = \sum_{v \leq u} f(v)$ et $h(u) = \sum_{v \geq u} f(v)$.
Soit $u \in E$. Alors la formule de Rota affirme que

$$\boxed{f(u) = \sum_{v \leq u} (-1)^{|supp(u)|-|supp(v)|} g(v) = \sum_{v \geq u} (-1)^{|supp(u)|-|supp(v)|} h(v)}.$$

11°) $\diamond$ Soit $x, y \in \{0, 1\}$: $x \oplus y$ est vraie si et seulement si (x est vraie et y fausse) ou (x est fausse et y est vraie), donc $x \oplus y$ correspond au "ou exclusif" appliqué à x et y.
$\diamond$ Pour tout $x, y \in \{0, 1\}$, $x \oplus y \equiv x + y$ [2], donc pour tout $x, y, z \in \{0, 1\}$, $(x \oplus y) \oplus z \equiv x + y + z \equiv x \oplus (y \oplus z)$ [2], or $(x \oplus y) \oplus z$ et $x \oplus (y \oplus z)$ sont dans $\{0, 1\}$, donc ils sont égaux. Ceci prouve que la loi interne $\oplus$ est associative. Elle admet 0 comme élément neutre, donc la notation $\bigoplus_{v \leq u} f(v)$ est correctement définie.

Modulo 2, pour tout $u \in \{0, 1\}^m = E$, $g(u) \equiv \sum_{v \leq u} f(v)$, donc d'après la question précédente, $f(u) \equiv \sum_{v\leq u}(-1)^{|supp(u)|-|supp(v)|}g(v)$, or $-1 \equiv 1[2]$, donc modulo 2, on peut écrire $f(u) \equiv \sum_{v\leq u} g(v) \equiv \bigoplus_{v\leq u} g(v)$, or à nouveau $f(u)$ et $\bigoplus_{v\leq u} g(v)$ sont dans $\{0,1\}$, donc ils sont égaux.

12°) $\diamond$ Soit $I \in E$. Il suffit de montrer que $\bigcap_{i\in I} P_i = \bigsqcup_{I\subset J}\Big(\Big(\bigcap_{i\in J} P_i\Big)\bigcap\Big(\bigcap_{i\in\mathbb{N}_n\setminus J}(F\setminus P_i)\Big)\Big)$, la formule de l'énoncé s'en déduit alors immédiatement en passant au cardinal.
Dans ce but, posons pour tout $J \in E$, $Q_J = \Big(\bigcap_{i\in J} P_i\Big)\bigcap\Big(\bigcap_{i\in\mathbb{N}_n\setminus J}(F\setminus P_i)\Big)$.

Il est clair que, pour tout $J \in E$ tel que $I \subset J$, $Q_J \subset \bigcap_{i\in I} P_i$, donc $\bigcup_{I\subset J} Q_J \subset \bigcap_{i\in I} P_i$.

Réciproquement, soit $x \in \bigcap_{i\in I} P_i$. Ainsi, pour tout $i \in I$, $x \in P_i$ (c'est également vrai lorsque $I = \emptyset$). Notons $J = \{i \in \mathbb{N}_n \ / \ x \in P_i\}$. Alors $I \subset J$ et $x \in Q_J = \Big(\bigcap_{i\in J} P_i\Big)\bigcap\Big(\bigcap_{i\in\mathbb{N}_n\setminus J}(F\setminus P_i)\Big)$. Ainsi, $\bigcup_{I\subset J} Q_J \supset \bigcap_{i\in I} P_i$.
Soit maintenant $J, K \in E$. Supposons que $Q_J \cap Q_K \neq \emptyset$. Il existe $x \in Q_J \cap Q_K$. Alors $J = \{i \in \mathbb{N}_n \ / \ x \in P_i\} = K$.
Par contraposition, on a montré que $J \neq K \Longrightarrow Q_J \cap Q_K = \emptyset$.
Finalement on a bien montré que $\bigcap_{i\in I} P_i = \bigsqcup_{I\subset J} Q_J$, ce qui conclut.

$\diamond$ D'après la seconde formule de Rota de la question 9.b,
pour tout $I \in E$, $f(I) = \sum_{I\subset J}(-1)^{|J|-|I|}g(J)$.

En particulier avec $I = \emptyset$, on obtient que $\Big|\bigcap_{1\leq i\leq n}(F\setminus P_i)\Big| = \sum_{J\subset\mathbb{N}_n}(-1)^{|J|}\Big|\bigcap_{i\in J} P_i\Big|$,

or d'après les formules de Morgan, $\bigcap_{1\leq i\leq n}(F\setminus P_i) = F \setminus \bigcup_{1\leq i\leq n} P_i$,

donc $\Big|\bigcup_{1\leq i\leq n} P_i\Big| = |F| - \sum_{J\subset\mathbb{N}_n}(-1)^{|J|}\Big|\bigcap_{i\in J} P_i\Big| = \sum_{k=1}^{n}(-1)^{k+1}\sum_{\substack{J\subset\mathbb{N}_n \\ \text{tel que } |J|=k}} g(J)$: en effet, lorsque $|J| = 0$, $J = \emptyset$ et $\Big|\bigcap_{i\in\emptyset} P_i\Big| = |F|$.

Partie III : La fonction de Möbius arithmétique

13°) $\diamond$ Soit $p \in \mathbb{N}$. Si $(d_0, \ldots, d_p)$ est une chaîne de longueur p joignant r à s, alors $r = d_0$ divise strictement d_1 qui divise strictement $d_2, \ldots$, qui divise strictement $d_p = s$.
Par transitivité, cf question 1, $d_0 = r$ divise d_1, d_2, ..., $d_p = s$, donc
pour tout $i \in \mathbb{N}_p$, $\frac{d_i}{r} \in \mathbb{N}_n$ et $1 = \frac{d_0}{d_0}$ divise strictement $\frac{d_1}{d_0}$ qui divise strictement $\frac{d_2}{d_0}, \ldots$, qui divise strictement $\frac{d_p}{d_0} = \frac{s}{r}$. Ainsi, $(1, \frac{d_1}{d_0}, \ldots, \frac{s}{r})$ est une chaîne de longueur p joignant

1 à $\frac{s}{r}$. On a donc construit une application de $C_p(r,s)$ dans $C_p(1,\frac{s}{r})$. C'est une bijection dont la bijection réciproque est l'application qui à une chaîne $(1,k_1,\ldots,\frac{s}{r})$ de $C_p(1,\frac{s}{r})$ associe la chaîne $(r,k_1r,\ldots,s)$.

$\diamond$ On en déduit en passant aux cardinaux que, pour tout $p\in\mathbb{N}$, $c_p(r,s)=c_p(1,\frac{s}{r})$, donc en utilisant la définition de l'application μ, on obtient que $\mu(r,s)=\mu(1,\frac{s}{r})$.

14°) $\diamond$ Lorsque $s=1$, on a $\mu(1)=1=m(1)$, d'où $R(1)$.

Soit $s\in\mathbb{N}_n$ avec $s\geq 2$. Supposons que pour tout $r\in\{1,\ldots,s-1\}$, $\mu(r)=m(r)$.

D'après la question 6, $\mu(s)=-\sum\limits_{\substack{r\in\mathbb{N}_n \text{ tel que}\\ r|s \text{ et } r\neq s}}\mu(r)$.

Si $r\in\mathbb{N}_n$ vérifie $r|s$ avec $r\neq s$, alors $r<s$, donc d'après l'hypothèse de récurrence, $\mu(r)=m(r)$. Ainsi, $\mu(s)=-\sum\limits_{\substack{r\in\mathbb{N}_n \text{ tel que}\\ r|s \text{ et } r\neq s}}m(r)$.

Ecrivons la décomposition de s en produit de nombre premiers sous la forme $s=\prod\limits_{i=1}^{k}p_i^{v_i}$, où les $p_1,\ldots,p_k$ sont k nombres premiers deux à deux distincts et où pour tout $i\in\mathbb{N}_k$, $v_i\in\mathbb{N}^*$. Les diviseurs r de s pour lesquels $m(r)\neq 0$ sont exactement les nombres de la forme $r=\prod\limits_{i\in I}p_i$ où $I\subset\mathbb{N}_k$.

Premier cas : on suppose qu'il existe $i\in\mathbb{N}_k$ tel que $v_i\geq 2$. Alors tous les diviseurs de la forme précédente sont des diviseurs de s différents de s,

donc $\mu(s)=-\sum\limits_{I\subset\mathbb{N}_k}m\Big(\prod\limits_{i\in I}p_i\Big)=-\sum\limits_{h=0}^{k}\sum\limits_{\substack{I\subset\mathbb{N}_k\\ \text{tel que } |I|=h}}(-1)^h$,

puis $\mu(s)=-\sum\limits_{h=0}^{k}\binom{k}{h}(-1)^h=-(1-1)^k=0$, car $k\geq 1$ (car $s\geq 2$).

Second cas : on suppose que, pour tout $i\in\mathbb{N}_n$, $v_i=1$. Alors, lorsque $I=\mathbb{N}_k$, $\prod\limits_{i\in I}p_i=s$, donc ce n'est pas un diviseur strict de s.

Ainsi, $\mu(s)=-\sum\limits_{I\subset\mathbb{N}_k \text{ avec } I\neq\mathbb{N}_k}m\Big(\prod\limits_{i\in I}p_i\Big)=-\sum\limits_{I\subset\mathbb{N}_k}m\Big(\prod\limits_{i\in I}p_i\Big)+(-1)^k=(-1)^k$, d'après le calcul du premier cas. Ceci démontre que $\mu(s)=m(s)$ dans tous les cas.

$\diamond$ Soit f une application de $\mathbb{N}_n$ dans $\mathbb{C}$. On pose, pour tout $s\in\mathbb{N}_n$, $g(s)=\sum\limits_{d|s}f(d)$ et $h(s)=\sum\limits_{s|d}f(d)$. Alors la formule d'inversion de Rota devient :

pour tout $s\in\mathbb{N}_n$, $f(s)=\sum\limits_{d|s}\mu\Big(\frac{s}{d}\Big)g(d)=\sum\limits_{s|d}\mu\Big(\frac{d}{s}\Big)g(d)$.

15°) $\diamond$ *Lemme :* Pour tout $s \in \mathbb{N}_n$, notons $A_s = \{\frac{k}{s} \ / \ k \in \{1, \ldots, s\}\}$.
Alors $A_s = \bigsqcup_{r|s} \left\{\frac{d}{r} \ / \ d \in \{1, \ldots, r\} \text{ et } d \wedge r = 1\right\}$.

Démonstration : Soit $\alpha = \frac{k}{s} \in A_s$, où $k \in \mathbb{N}_s$. L'écriture irréductible de α est de la forme $\frac{d}{r}$, où $r|s$ avec $d \wedge r = 1$. De plus $\alpha \in]0, 1]$, donc $d \in \{1, \ldots, r\}$. Ainsi, $A_s \subset \bigcup_{r|s} \left\{\frac{d}{r} \ / \ d \in \{1, \ldots, r\} \text{ et } d \wedge r = 1\right\}$. L'inclusion réciproque est claire et l'écriture sous forme irréductible de α étant unique, cette réunion est bien disjointe.

$\diamond$ Pour tout $r \in \mathbb{N}_n$, posons $f(r) = \sum_{\substack{d \in \{1, \ldots, r\} \\ \text{tel que } d \wedge r = 1}} e^{2i\pi \frac{d}{r}}$.

Pour tout $s \in \mathbb{N}_n$, posons $g(s) = \sum_{d|s} f(s)$.

Alors d'après la question précédente, pour tout $r \in \mathbb{N}_n$, $f(r) = \sum_{d|r} \mu\left(\frac{r}{d}\right) g(d)$.

Soit $s \in \mathbb{N}_n$. $g(s) = \sum_{r|s} \sum_{\substack{d \in \{1, \ldots, r\} \\ \text{tel que } d \wedge r = 1}} e^{2i\pi \frac{d}{r}}$. Alors d'après le lemme, par sommation par paquets, $g(s) = \sum_{k=1}^{s} e^{2i\pi \frac{k}{s}}$, puis $g(s) = \sum_{k=0}^{s-1} \left(e^{\frac{2i\pi}{s}}\right)^k$. Lorsque $s \neq 1$, $e^{\frac{2i\pi}{s}} \neq 1$, donc en tant que somme d'une suite géométrique, $g(s) = \dfrac{1 - (e^{\frac{2i\pi}{s}})^s}{1 - e^{\frac{2i\pi}{s}}} = 0$ et $g(1) = 1$.

Alors pour tout $r \in \mathbb{N}_n$, $\sum_{\substack{d \in \{1, \ldots, r\} \\ \text{tel que } d \wedge r = 1}} e^{2i\pi \frac{d}{r}} = f(r) = \sum_{d|r} \mu\left(\frac{r}{d}\right) g(d) = \mu(r) g(1) = \mu(r)$, ce qu'il fallait démontrer.

16°) Pour tout $r \in \mathbb{N}_n$, notons $\varphi(r)$ le nombre d'entiers k de $\{1, \ldots, r\}$ tels que $k \wedge r = 1$ (φ est l'indicatrice d'Euler). D'après le lemme, pour tout $s \in \mathbb{N}_n$,
$s = |A_s| = \sum_{r|s} \varphi(r)$, donc d'après la formule d'inversion, cf question 14, pour tout $r \in \mathbb{N}_n$, $\varphi(r) = \sum_{d|r} \mu\left(\frac{r}{d}\right) d$.

Notons $D(r)$ l'ensemble des diviseurs de r et notons h l'application $\begin{array}{ccc} D(r) & \longrightarrow & D(r) \\ d & \longmapsto & \frac{r}{d} \end{array}$.
h est une involution sur $D(r)$, donc en remplaçant d par $h(d)$ dans la somme précédente, d'après la formule de changement de variable, on obtient $\varphi(r) = \sum_{\substack{d \in \{1, \ldots, r\} \\ \text{tel que } d \text{ divise } r}} \mu(d) \frac{r}{d}$.