Interrogation 3
25 novembre 2022

Intégrales à paramètre, groupes, anneaux, polynômes

1 (/2) Montrer que : $\sum_{n=0}^{+\infty} \int_0^1 x^{2n}(1-x)\mathrm{d}x = \int_0^1 \frac{\mathrm{d}x}{1+x}$.
En déduire que $\sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} = \ln(2)$.

Soit $g_n : x \in [0,1[\mapsto x^{2n}(1-x)$. La série de fonctions $\sum g_n$ converge simplement sur $[0,1[$ vers la fonction $x \in [0,1[\mapsto \frac{1}{1+x}$. Cette dernière fonction est continue par morceaux, ainsi que les fonctions g_n.

De plus, pour tout $n \in \mathbb{N}$, $g_n \geqslant 0$, de sorte que, par théorème d'intégration terme à terme dans le cas positif :

$$\sum_{n=0}^{\infty} g_n(t)\,dt = \int_0^1 \frac{dt}{1+t} = \ln(2)$$

Or pour tout $N \in \mathbb{N}$,

$$\sum_{n=0}^{N} \int_0^1 g_n(t)\,dt = \sum_{n=0}^{N} \frac{1}{2n+1} - \frac{1}{2n+2} = \sum_{n=1}^{2N+2} \frac{(-1)^{n-1}}{n}$$

La série $\sum \frac{(-1)^{n-1}}{n}$ est convergente (son terme général est de signe alterné, et il décroît vers 0 en valeur absolue), et il vient donc bien

$$\sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} = \ln(2)$$

◇◇◇

2 (/1 + 2) Pour tout $n \in \mathbb{N}$, on pose $I_n = \int_0^1 \arctan(t)t^n\mathrm{d}t$. Montrer que (I_n) tend vers 0, puis trouver un équivalent de I_n.

Soit $f_n : t \in [0,1[\mapsto \arctan(t)t^n$. Toutes les fonctions f_n sont continues, ainsi que la limite simple de (f_n), qui est la fonction nulle. De plus, pour tout $(n,t) \in \mathbb{N} \times [0,1[$, $|f_n(t)| \leqslant \arctan(1) = \pi/4$, et $t \mapsto \pi/4$ est intégrable sur $[0,1[$, donc le théorème de convergence dominée permet d'affirmer que (I_n) tend vers 0.

***Remarque** – Il était facile en l'espèce de se passer du puissant théorème de convergence dominée, grâce à la majoration*

$$\forall (n,t) \in \mathbb{N} \times [0,1[, \quad |f_n(t)| \leqslant \frac{\pi\, t^n}{4}$$

dont on déduit $|I_n| \leqslant \frac{\pi}{4(n+1)}$.

Pour trouver un équivalent de I_n, on peut procéder au changement de variable $u = t^n$:

$$I_n = \int_0^1 \arctan(u^{1/n})u \times \frac{1}{n}u^{\frac{1}{n}-1}du = \frac{1}{n}\int_0^1 \arctan(u^{1/n})u^{\frac{1}{n}}du$$

Par la domination

$$\forall (u,n) \in]0,1] \times \mathbb{N}^*, \left|\arctan(u^{1/n})u^{\frac{1}{n}}\right| \leqslant \frac{\pi}{4}$$

(où $t \mapsto \frac{\pi}{4}$ est intégrable sur $]0,1]$), et convergence simple vers $t \mapsto \frac{\pi}{4}$, on obtient

$$I_n \underset{n\infty}{\sim} \frac{\pi}{4n}$$

On peut aussi effectuer une intégration par parties :

$$I_n = \left[\arctan(t)\frac{t^{n+1}}{n+1}\right]_0^1 - \frac{1}{n+1}\int_0^1 \frac{t^{n+1}}{1+t^2}dt = \frac{1}{n+1}\left(\frac{\pi}{4} - \int_0^1 \frac{t^{n+1}}{1+t^2}dt\right)$$

Or $\left(\int_0^1 \frac{t^{n+1}}{1+t^2}dt\right)$ tend vers 0 (par convergence dominée, ou par la majoration $\left|\frac{t^{n+1}}{1+t^2}\right| \leqslant t^{n+1}$, donnant $\left|\int_0^1 \frac{t^{n+1}}{1+t^2}dt\right| \leqslant \frac{1}{n+2}$), d'où

$$I_n \underset{n\infty}{\sim} \frac{\pi}{4(n+1)}$$

◇◇◇

Exercice 1 : Une suite d'intégrales

(/2) Soit $a > 1$. Pour tout $n \in \mathbb{N}^*$, et tout $t \geqslant 0$ on pose $f_n(t) = \left(1 + \frac{t}{n}\right)^n e^{-at}$, puis

$$I_n = \int_0^{+\infty} f_n(t)\mathrm{d}t$$

Montrer que chaque I_n est bien définie et que la suite (I_n) converge vers $\frac{1}{a-1}$.

◇◇◇

Chaque f_n est continue par morceaux (et même continue) sur $\mathbb{R}_+$. Une étude asymptotique élémentaire montre que (f_n) converge simplement vers $f : t \in \mathbb{R}_+ \mapsto \exp((1-a)t)$, qui est également continue (par morceaux).

De plus, l'inégalité $\ln(1+x) \leqslant x$ (valable pour tout $x \in \mathbb{R}_+$ et même tout $x \in]-1, +\infty[$), fournit la domination

$$\forall\, n \in \mathbb{N}, \forall\, t \in \mathbb{R}_+, \quad |f_n(t)| \leqslant f(t)$$

Comme f est intégrable (exemple d'une fonction exponentielle, avec $1-a<0$), le théorème de convergence dominée assure donc que les f_n sont intégrables[1]*, et que (I_n) converge vers $\int_0^{+\infty} f(t)dt = \frac{1}{a-1}$.*

Exercice 2 : Une intégrale à paramètre

On pose $g(x,t) = \frac{e^{-t}}{1+tx}$ pour tout $(x,t) \in \mathbb{R}_+^2$.

1 (/1) Vérifier que pour tout $x \geqslant 0$, $G(x) \overset{def}{=} \int_0^{+\infty} g(x,t)\mathrm{d}t$ est bien défini.

2 (/2) Montrer que G est de classe $\mathcal{C}^\infty$ sur $\mathbb{R}_+$.

3 (/1) Calculer $G^{(n)}(0)$ pour tout $n \in \mathbb{N}$.

Remarque – On aura le droit d'utiliser la fonction Γ d'Euler sans justification.

1. et que f l'est aussi, mais c'est la fonction par laquelle on domine ...

◇◇◇

1 *Soit $x \in \mathbb{R}_+$. La fonction $t \mapsto g(x,t)$ est continue (par morceaux), et*

$$\forall\, t \in \mathbb{R}_+, \quad |g(x,t)| \leqslant e^{-t}$$

Or $t \mapsto e^{-t}$ est intégrable sur $\mathbb{R}_+$, donc $G(x)$ est bien défini.

2 *Pour tout $t \in \mathbb{R}_+$, la fonction $x \mapsto g(x,t)$ est de classe $\mathcal{C}^\infty$.*

Pour tout $n \in \mathbb{N}$, tout $x \in \mathbb{R}_+$ et tout $t \in \mathbb{R}_+$:

$$\frac{\partial^n g}{\partial x^n}(x,t) = \frac{(-1)^n n!\, t^n e^{-t}}{(1+xt)^{n+1}}$$

et donc

$$\left|\frac{\partial^n g}{\partial x^n}(x,t)\right| \leqslant \varphi_n(t) \overset{def}{=} n! t^n e^{-t}$$

où φ_n est indépendante de x, intégrable sur $\mathbb{R}_+$ ($\varphi_n(t) = \mathrm{o}_{t\to+\infty}(1/t^2)$ et $t \mapsto 1/t^2$ est intégrable sur $[1,+\infty[$).

Signalons enfin que toutes les fonctions $t \mapsto \frac{\partial^n g}{\partial x^n}(x,t)$ (pour tout $n \in \mathbb{N}$ et tout $x \in \mathbb{R}_+$) sont continues par morceaux.

Par application du théorème itéré de Leibniz, on en déduit que G est de classe $\mathcal{C}^\infty$, et aussi que pour tout $(n,x) \in \mathbb{N} \times \mathbb{R}_+$:

$$G^{(n)}(x) = (-1)^n\, n! \int_0^{+\infty} \frac{t^n e^{-t}}{(1+xt)^{n+1}}\, dt$$

3 *D'après la formule ci-dessus, on a, pour tout $n \in \mathbb{N}$:*

$$G^{(n)}(0) = (-1)^n\, n! \int_0^{+\infty} t^n e^{-t}\, dt = (-1)^n\, n!\, \Gamma(n+1) = (-1)^n (n!)^2$$

Exercice 3 :

Soit x un réel strictement positif.

1 (/1) Montrer que, pour tout réel $x > 0$, l'intégrale $\int_0^{+\infty} \frac{e^{-t}-e^{-xt}}{t}\mathrm{d}t$ est absolument convergente.

On désigne désormais par F la fonction qui à $x > 0$ associe $F(x) = \int_0^{+\infty} \frac{e^{-t}-e^{-xt}}{t}\mathrm{d}t$.

2 (/2) Montrer que la fonction F est de classe $\mathcal{C}^1$ sur l'intervalle $]0,+\infty[$.

Calculer $F'(x)$ puis $F(x)$, pour tout $x \in]0,+\infty[$.

3 (/1) Soient a et b deux réels vérifiant $0 < a < b$.

Montrer que l'intégrale $\int_0^{+\infty} \frac{e^{-at}-e^{-bt}}{t}\mathrm{d}t$ est convergente et calculer sa valeur.

Indication – On pourra utiliser la fonction F étudiée précédemment.

4 Dans cette question, on considère l'intégrale $\int_0^{+\infty} \frac{e^{-xt}}{t}(1-e^{-t})^n \mathrm{d}t$, dans laquelle x est un réel strictement positif et n un entier supérieur ou égal à 1.

a (/1) Montrer que cette intégrale est convergente.

b (/1) Vérifier que, pour tout réel t strictement positif et tout entier n supérieur ou égal à 1, on a

$$(1-e^{-t})^n = -\sum_{k=0}^{n} \binom{n}{k} (-1)^k (1-e^{-kt})$$

c (/1) En déduire la valeur (exprimée comme une somme finie) de l'intégrale $\int_0^{+\infty} \frac{e^{-xt}}{t}(1-e^{-t})^n \mathrm{d}t$.

◇◇◇

1 *Posons, pour tout réel $x > 0$, $f(x,t) = \frac{e^{-t}-e^{-xt}}{t}$.*

Soit $x > 0$.

Régularité ▷ *La fonction $t \mapsto f(x,t)$ est continue par morceaux (et même continue) sur $\mathbb{R}_+^*$.*

Étude en 0 ▷

$$e^{-t} - e^{-xt} = 1 - t + \mathrm{o}_{t\to 0} - (1 - xt + \mathrm{o}_{t\to 0}(t)) = (x-1)t + \mathrm{o}_{t\to 0}(t)$$

donc $f(x,t)$ tend vers $x-1$ lorsque t tend vers 0 : $t \mapsto f(x,t)$ se prolonge par continuité en une fonction continue par morceaux (et même continue) sur $\mathbb{R}_+$, donc $\int_0^1 f(x,t)dt$ est absolument convergente.

Étude en $+\infty$ ▷ *Par croissances comparées, $f(x,t) = \mathrm{o}_{t\to+\infty}\left(\frac{1}{t^2}\right)$, or $\int_1^{+\infty} \frac{dt}{t^2}$ est absolument convergente, donc, par transmission de l'absolue convergence par équivalence, $\int_1^{+\infty} f(x,t)\,dt$ est absolument convergente.*

Conclusion ▷ *$\int_0^{+\infty} \frac{e^{-t}-e^{-xt}}{t}dt$ est donc bien absolument convergente.*

2

Appliquons le théorème de Leibniz (de dérivation sous l'intégrale), avec domination sur tout segment.

Vérifications portant sur la fonction f ▷ *Pour tout $x > 0$, $t \mapsto f(x,t)$ est continue par morceaux intégrable sur $\mathbb{R}_+^*$ (fait à la question précédente).*

Vérifications portant sur la fonction $\frac{\partial f}{\partial x}$ ▷ *La fonction $\frac{\partial f}{\partial x}$ est bien définie sur $\mathbb{R}_+^* \times \mathbb{R}_+^*$. De plus*

1. *Pour tout $(x,t) \in \mathbb{R}_+^* \times \mathbb{R}_+^*$, $\frac{\partial f}{\partial x}(x,t) = e^{-xt}$.*
2. *Pour tout $x \in \mathbb{R}_+^*$, $t \mapsto \frac{\partial f}{\partial x}(x,t)$ est continue par morceaux sur $\mathbb{R}_+^*$.*
3. *Pour tout $t \in \mathbb{R}_+^*$, $x \mapsto \frac{\partial f}{\partial x}(x,t)$ est continue sur $\mathbb{R}_+^*$.*

Hypothèse de domination ▷ *Pour tout segment $[a,b]$ inclus dans $\mathbb{R}_+^*$, pour tout $(x,t) \in [a,b] \times \mathbb{R}_+^*$:*

$$\left|\frac{\partial f}{\partial x}(x,t)\right| \leqslant e^{-at},$$

et $t \mapsto e^{-at}$ est (indépendante de x et) intégrable sur $\mathbb{R}_+^*$.

Conclusion ▷ *D'après le théorème de Leibniz, avec domination sur tout segment, F est bien de classe $\mathcal{C}^1$ sur $\mathbb{R}_+^*$. De plus, pour tout $x \in \mathbb{R}_+^*$, $F'(x) = \int_0^{+\infty} e^{-xt}dt = \frac{1}{x}$.*

Comme $F(1) = 0$, on en déduit que pour tout $x > 0$, $F(x) = \ln(x)$.

3 *Pour tout $t > 0$,*

$$\frac{e^{-at} - e^{-bt}}{t} = \frac{e^{-t} - e^{-bt}}{t} - \frac{e^{-t} - e^{-at}}{t}$$

Par convergence des intégrales définissant $F(a)$ et $F(b)$, on en déduit que $\int_0^{+\infty} \frac{e^{-at}-e^{-bt}}{t}dt$ est convergente, et égale à $F(b) - F(a) = \ln(b/a)$ d'après la question précédente.

Remarque *– On pouvait aussi effectuer le changement de variable $u = at$, cela nous ramenait également à F.*

4

a *L'intégrande se prolonge en une fonction continue sur $\mathbb{R}_+$, et $\frac{e^{-xt}}{t}(1-e^{-t})^n = \mathrm{o}_{t\to+\infty}(1/t^2)$, pour tout $x > 0$, donc $\int_0^{+\infty} \frac{e^{-xt}}{t}(1-e^{-t})^n dt$ converge bien.*

b *Binôme de Newton.*

c *Par linéarité de l'intégrale, et sachant que toutes les intégrales écrites sont bien convergentes, on a*

$$\begin{aligned}
\int_0^{+\infty} \frac{e^{-xt}}{t}(1-e^{-t})^n\,dt &= -\int_0^{+\infty} \sum_{k=0}^{n} \binom{n}{k}(-1)^k \frac{e^{-xt}}{t}\,(1-e^{-kt})\,dt \\
&= -\sum_{k=0}^{n} \binom{n}{k}(-1)^k \int_0^{+\infty} \frac{e^{-xt}}{t}\,(1-e^{-kt})\,dt \\
&= -\sum_{k=0}^{n} \binom{n}{k}(-1)^k \int_0^{+\infty} \frac{e^{-xt}-e^{-(x+k)t}}{t}\,dt \\
&= -\sum_{k=0}^{n} \binom{n}{k}(-1)^k \ln\left(\frac{x+k}{x}\right)
\end{aligned}$$

Exercice 4 : Irréductibilité de Φ_5

On considère le polynôme

$$\Phi_5 = X^4 + X^3 + X^2 + X + 1$$

1 (/1) Donner la décomposition en produit d'irréductibles (unitaires) dans $\mathbb{C}[X]$.

2 (/1) En déduire l'existence de réels α, β tels que la décomposition en produit d'irréductibles (unitaires) dans $\mathbb{R}[X]$ soit de la forme

$$\Phi_5 = (X^2 + \alpha X + 1)(X^2 + \beta X + 1)$$

3 (/2) Montrer que Φ_5 est irréductible sur $\mathbb{Q}$.

◇ ◇ ◇

1 $\Phi_5 = \prod_{k=1}^{4} \left(X - e^{2ik\pi/5}\right)$.

2 *Φ_5 n'a pas de racine réelle (donc pas de facteur irréductible de degré 1). On regroupe les racines conjuguées :*

$$\Phi_5 = \left(X^2 - 2\cos(2\pi/5)X + 1\right)\left(X^2 - 2\cos(4\pi/5)X + 1\right)$$

3 *En considérant les coefficients devant X^3 et devant X^2, on a $\alpha + \beta = 1$ et $\alpha\beta + 2 = 1$, donc $\alpha\beta = -1$.*

α et β sont les racines du polynôme $X^2 - X - 1$, donc α et β sont irrationnels (rappel : il est facile de déterminer les racines rationnelles d'un polynôme à coefficients entiers (ou plus généralement rationnels)).

Soit Q un facteur irréductible de Φ_5 dans $\mathbb{Q}[X]$. D'après la décomposition précédente, Q est multiple de $X^2+\alpha X+1$ ou de $X^2+\beta X+1$ (on utilise l'unicité de la décomposition dans $\mathbb{R}[X]$), où $\alpha, \beta \notin \mathbb{Q}$, donc $\deg(Q)$ vaut 3 ou 4. Ceci valant pour tout facteur irréductible, $\deg(Q) = 4$: Φ_5 est irréductible sur $\mathbb{Q}[X]$.

Exercice 5 : Groupes abéliens d'ordre pq

On considère deux nombres premiers p et q distincts, ainsi qu'un groupe abélien $(G, \cdot)$ d'ordre pq. On souhaite montrer que G est cyclique.

Soit $a \in G \setminus \{e_G\}$. Si $o(a) = pq$, c'est terminé. On suppose donc $o(a) \neq pq$, et il existe donc $b \in G \setminus < a >$.

1 (/2) Montrer que $G =< a, b >$ (*i.e.* G est le plus petit sous-groupe de G contenant a et b).

On pourra utiliser le théorème de Lagrange (version générale) : pour tout sous-groupe $\mathcal{H}$ d'un groupe fini $\mathcal{G}$, l'ordre de $\mathcal{H}$ divise l'ordre de $\mathcal{G}$.

2 (/2) Montrer que $G = \{a^i b^j, (i,j) \in [\![0, o(a)-1]\!] \times [\![0, o(b)-1]\!]\}$. Conclure.

3 (/2) Quels sont les ordres possibles des éléments de G, et combien G a-t-il d'éléments de chaque ordre ?

◇ ◇ ◇

1 *Notons $H =< a, b >$, d'ordre N. Puisque $< a >$ est un sous-groupe de H, $o(a)$ divise N (Lagrange au programme). Supposons par exemple $o(a) = p$ pour fixer les idées. Toujours par théorème de Lagrange, N divise pq. De plus, $< a >$ est strictement inclus dans H (puisque $b \notin < a >$), donc $N > p$. Ainsi, N est un multiple de p, un diviseur de pq, et est strictement plus grand que p : $N = pq$.*

2 *Puisque a et b commutent, $< a, b >= \{a^i b^j, (i,j) \in \mathbb{Z}^2\}$. En prenant les divisions euclidiennes de i et j par $o(a)$ et $o(b)$ respectivement, on a bien le résultat.*

Le sous-groupe $< a > \cap < b >$ de $< a >$ n'a que deux ordres possibles : 1 et p (puisque cet ordre divise $p = o(a)$). Si $< a > \cap < b >= 1$, alors $< a, b >$ est d'ordre $o(a)o(b)$, donc $o(b) = q$. On vérifie alors que ab est d'ordre pq (par exemple parce que p et q divisent cet ordre).

Si $< a > \cap < b >=< a >$, alors $< a >$ est un sous-groupe strict de $< b >$, donc $< b >$ est d'ordre pq : dans tous les cas, G est cyclique.

3 *G est cyclique d'ordre pq, donc il admet des éléments d'ordres 1, p, q et pq.*

Il n'admet qu'un seul élément d'ordre 1.

D'après ce qui précède, si $o(a) = p$, les seuls éléments d'ordre p sont les éléments non triviaux de $< a >$, donc G admet exactement $p-1$ éléments d'ordre p.

Par symétrie, il admet exactement $q-1$ éléments d'ordre q.

Il admet donc $pq - 1 - (p-1) - (q-1) = pq - p - q + 1 = (p-1)(q-1)$ éléments d'ordre pq.

Remarque *– On pouvait bien sûr retrouver ce dernier résultat par $\varphi(pq) = \varphi(p)\varphi(q) = (p-1)(q-1)$.*

Exercice 6 : Idempotents de $\mathbb{Z}/n\mathbb{Z}$

Soit $n \geqslant 2$ un entier, dont la décomposition primaire est

$$n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$$

(où les p_i sont des nombres premiers deux à deux distincts et où les α_i sont dans $\mathbb{N}^*$).

Un élément a de $\mathbb{Z}/n\mathbb{Z}$ est dit *idempotent* si $a^2 = a$. On note $\mathcal{I}$ leur ensemble

1 (/2) Montrer que si $a, b \in \mathcal{I}$, alors $ab \in \mathcal{I}$ et $1 - a \in \mathcal{I}$. Montrer que si $n \geqslant 3$, l'ensemble $\mathcal{I}$ n'est pas stable par addition.

2 (/2) Montrer que $\mathcal{I}$ est de cardinal 2^k.

Indication – On pourra utiliser le théorème des restes chinois.

3 (/2) D'après la question précédente, $\mathcal{I}$ est équipotent à $(\mathbb{Z}/2\mathbb{Z})^k$.

Proposer une structure d'anneau sur $\mathcal{I}$ afin que cet anneau $(\mathcal{I}, \oplus, \otimes)$ soit isomorphe à l'anneau produit $\big((\mathbb{Z}/2\mathbb{Z})^k, +, \times\big)$.

Remarque – On pourra prendre pour $\otimes$ la multiplication induite par celle sur $\mathbb{Z}/n\mathbb{Z}$.

◇◇◇

1 *Évident. Si $n \geqslant 3$, 1 est idempotent mais pas $2 = 1 + 1$, car $2^2 \not\equiv 2[n]$.*

2 *Par le théorème des restes chinois, on a un isomorphisme naturel d'anneaux entre $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{\alpha_k}\mathbb{Z}$, qui définit donc une bijection entre les deux ensembles d'idempotents. Dans le second anneau, un élément est un idempotent si et seulement si chacune de ses composantes en est un.*

Or dans $\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$, $\overline{a}$ est un idempotent si et seulement si $\overline{a} = \overline{a}^2$, si et seulement si $\overline{a}(1-\overline{a}) = \overline{0}$, si et seulement si $p_i^{\alpha_i}$ divise $a(a-1)$ dans $\mathbb{Z}$, si et seulement si $\overline{a} = \overline{0}$ ou $\overline{a} = \overline{1}$ (car p_i est premier, et car a et $a-1$ sont premiers entre eux).

On a donc exactement deux idempotents dans chaque $\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$, et donc 2^k idempotents au total.

3 *On a déjà une bijection naturelle : à chaque idempotent a de $\mathbb{Z}/n\mathbb{Z}$, on associe un élément $(\overline{\varepsilon_1}, \ldots, \overline{\varepsilon_k})$ dans $\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{\alpha_k}\mathbb{Z}$ par l'isomorphisme naturel, où chaque ε_i vaut 0 ou 1 : on associe alors $([\varepsilon_1], \ldots, [\varepsilon_n])$ où $[\varepsilon_i]$ est la classe de ε_i dans $\mathbb{Z}/2\mathbb{Z}$.*

Une fois qu'on a cette bijection φ, il suffit de transférer la structure. Ici, on a de la chance, car $\varphi(ab) = \varphi(a)\varphi(b)$ pour tous $a, b \in \mathcal{I}$, et en plus $\varphi(1-a) = \tilde{1} - \varphi(a)$ (où $\tilde{1} = ([1], \ldots, [1])$ est l'unité de $(\mathbb{Z}/2\mathbb{Z})^n$).

On veut en plus que $\varphi(a \oplus b) = \varphi(a) + \varphi(b)$. Dans $(\mathbb{Z}/2\mathbb{Z})^k$, l'addition est le ou exclusif XOR, donc on pose

$$\forall (e, f) \in \mathcal{I}, e \oplus f = e + f - 2ef$$

(on voulait avoir, dans chaque $\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$, et pour $\overline{a}, \overline{b} \in \{\overline{0}, \overline{1}\}$, $\overline{a} \oplus \overline{b} = \overline{0}$ si $\overline{a} = \overline{b}$, et $\overline{a} \oplus \overline{b} = \overline{1}$ sinon).