ISM MP, Mathématiques
Année 2024/2025

Feuille d'exercices n°79

Exercice 1 (*)

Soit $\mathrm{G} = \left\{a + b\sqrt{2},\ (a,b) \in \mathbb{Q}^2\right\}$.

1. Montrer que G est un groupe pour l'addition.
2. Montrer $\mathrm{G}^* = \mathrm{G} \setminus \{0\}$ est un groupe pour la multiplication.

Corrigé : 1. Montrons que $(\mathrm{G}, +)$ est un sous-groupe de $(\mathbb{R}, +)$. On a $0 \in \mathrm{G}$ et

$$\forall (a,b,c,d) \in \mathbb{Q}^4 \qquad (a + b\sqrt{2}) - (c + d\sqrt{2}) = (a-c) + (b-d)\sqrt{2} \in \mathrm{G}$$

Ainsi $\boxed{(\mathrm{G}, +) \text{ est un groupe.}}$

2. Montrons que $(\mathrm{G}^*, \times)$ est un sous-groupe de $(\mathbb{R}^*, \times)$. On a $1 \in \mathrm{G}^*$. Soit $(a,b) \in \mathbb{Q}^2$ avec $(a,b) \neq (0,0)$. On a

$$(a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2 \quad \text{et} \quad a^2 - 2b^2 \neq 0 \text{ car } \sqrt{2} \notin \mathbb{Q}$$

Ainsi $$(a + b\sqrt{2}) \times \frac{a - b\sqrt{2}}{a^2 - 2b^2} = 1$$

Enfin $\forall (a,b,c,d) \in \mathrm{Q}^4 \qquad (a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$

et par intégrité $(a + b\sqrt{2})(c + d\sqrt{2}) \neq 0$

On conclut $\boxed{(\mathrm{G}^*, \times) \text{ est un groupe.}}$

Exercice 2 (*)

Soit $(\mathrm{G}, \star)$ un groupe tel que $x \mapsto x^2$ soit un morphisme de groupes. Montrer que G est abélien.

Corrigé : Notons $\varphi : \mathrm{G} \to \mathrm{G}, x \mapsto x^2$. Soit $(x,y) \in \mathrm{G}^2$. On a

$$\varphi(x \star y) = \varphi(x) \star \varphi(y) \iff x \star y \star x \star y = x^2 \star y^2 \iff y \star x \star y = x \star y^2 \iff y \star x = x \star y$$

Ainsi $\boxed{\text{Le groupe G est abélien.}}$

Exercice 3 (*)

Décrire les groupes d'ordre 5.

Corrigé : Soit G un groupe d'ordre 5. Il existe un élément $x \in \mathrm{G} \setminus \{e\}$. On a $o(x)$ diviseur de 5 et $o(x) = \mathrm{Card}\ \langle x \rangle > 1$ puisque $\{e, x\} \subset \langle x \rangle$. On en déduit $\mathrm{G} = \langle x \rangle$ et on conclut

$$\boxed{\text{Les groupes d'ordre 5 sont isomorphes à } \mathbb{Z}/5\mathbb{Z}.}$$

Exercice 4 (*)

Déterminer deux groupes d'ordre 6 non isomorphes.

Corrigé : Le groupe S_3 est d'ordre 6 et n'est pas abélien puisque

$$(1\ \ 2)\,(2\ \ 3) \neq (2\ \ 3)\,(1\ \ 2)$$

S'il n'est pas abélien, il n'est pas cyclique. Ainsi

$$\boxed{\text{Les groupes } \mathrm{S}_3 \text{ et } \mathbb{Z}/6\mathbb{Z} \text{ sont d'ordre 6 mais non isomorphes.}}$$

Exercice 5 (**)

1. Déterminer les morphismes de groupes de $\mathbb{Z}/3\mathbb{Z}$ vers $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.
2. Déterminer les morphismes de groupes de $\mathbb{Z}/6\mathbb{Z}$ vers $\mathbb{Z}/8\mathbb{Z}$.

Corrigé : Soit $\varphi : (\mathbb{Z}/n\mathbb{Z}, +) \to (\mathrm{G}, +)$ un morphisme de groupes. On a $\varphi(\bar{k}) = k\varphi(\bar{1})$ pour tout $k \in \mathbb{Z}$ ce qui signifie que φ est caractérisé par $\varphi(\bar{1})$.

1. Le groupe produit $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ est d'ordre 8. On a $o(\varphi(\bar{1}))|3$ et $o(\varphi(\bar{1}))|8$ d'où $o(\varphi(\bar{1}))|3\wedge 8 = 1$, *i.e.* $\varphi(\bar{1}) = \widehat{0}$. Ainsi

$$\boxed{\text{Le morphisme nul est l'unique morphisme de } \mathbb{Z}/3\mathbb{Z} \text{ vers } \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}.}$$

2. On a $o(\varphi(\bar{1}))|6 \wedge 8 = 2$. Ainsi, on a $2\varphi(\bar{1}) = \widehat{0}$ d'où $\varphi(\bar{1}) \in \left\{\widehat{0}, \widehat{4}\right\}$ d'où les morphismes candidats : le morphisme nul et $\bar{x} \mapsto \widehat{4x}$ qui est bien défini puisque pour $\bar{x} \in \mathbb{Z}/6\mathbb{Z}$ et $x \in \bar{x}$, on envoie $\bar{x} = x\bar{1} \mapsto x\widehat{4} = \widehat{4x}$ et le choix du représentant n'influe pas. La synthèse est immédiate et on conclut

$$\boxed{\text{Les morphismes de groupes de } \mathbb{Z}/6\mathbb{Z} \text{ vers } \mathbb{Z}/8\mathbb{Z} \text{ sont le morphisme nul et } \bar{x} \to \widehat{4x}.}$$

Exercice 6 (*)

Soit $n \geqslant 2$. Calculer $\displaystyle\sum_{\sigma\in\mathrm{S}_n} \varepsilon(\sigma)$

Corrigé : Soit τ une transposition de S_n. L'application $\varphi : \mathrm{S}_n \to \mathrm{S}_n, \sigma \mapsto \tau \circ \sigma$ est une permutation de S_n (c'est une involution). Par conséquent, on a

$$\sum_{\sigma\in\mathrm{S}_n} \varepsilon(\sigma) = \sum_{\sigma\in\mathrm{S}_n} \varepsilon(\tau\circ\sigma) = \sum_{\sigma\in\mathrm{S}_n} \varepsilon(\tau)\varepsilon(\sigma)$$

Or, la signature d'une transposition est égale à -1 et par conséquent

$$\sum_{\sigma\in\mathrm{S}_n} \varepsilon(\sigma) = -\sum_{\sigma\in\mathrm{S}_n} \varepsilon(\sigma)$$

Ainsi $\boxed{\displaystyle\sum_{\sigma\in\mathrm{S}_n} \varepsilon(\sigma) = 0}$

Variante : Pour $\mathrm{A} \in \mathscr{M}_n(\mathbb{R})$, on a $\det \mathrm{A} = \displaystyle\sum_{\sigma\in\mathrm{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)}$. Ainsi, notant J la matrice de $\mathscr{M}_n(\mathbb{R})$ constituée de 1, on a

$$\sum_{\sigma\in\mathrm{S}_n} \varepsilon(\sigma) = \det \mathrm{J}$$

La matrice J contient (au moins) deux colonnes identiques et n'est donc pas inversible. On retrouve alors le résultat précédent.

Exercice 7 (**)

Soit $(\mathrm{G}, \times)$ fini d'ordre n et k entier premier avec n. Montrer que pour tout $g \in \mathrm{G}$, il existe un unique $x \in \mathrm{G}$ tel que $g = x^k$.

Corrigé : On a $k \wedge n = 1$ d'où l'existence de $(u, v) \in \mathbb{Z}^2$ tel que $ku + nv = 1$. Soit $g \in \mathrm{G}$ et $x \in \mathrm{G}$ solution de $g = x^k$. Comme le groupe G est d'ordre n, on a $x^n = 1$. Puis, on obtient

$$g = x^k \iff g^u = x^{ku} = x^{ku}(x^n)^v = x^{ku+nv} \iff g^u = x$$

On conclut $\boxed{\text{Pour tout } g \in \mathrm{G}, \text{ il existe un unique } x \in \mathrm{G} \text{ tel que } g = x^k.}$

Exercice 8 (**)

Déterminer tous les morphismes de groupes de $(\mathbb{Q}, +)$ dans $(\mathbb{Z}, +)$.

Corrigé : Soit $f : (\mathbb{Q}, +) \to (\mathbb{Z}, +)$ un morphisme de groupes. Pour x rationnel, on a

$$\forall n \in \mathbb{N}^* \qquad f(x) = f\left(n\frac{x}{n}\right) = nf\left(\frac{x}{n}\right)$$

ce qui prouve que $f(x)$ est un entier naturel divisible par tout entier non nul d'où $f(x) = 0$. Ainsi

$$\boxed{\text{L'unique morphisme de groupes de } (\mathbb{Q}, +) \text{ dans } (\mathbb{Z}, +) \text{ est le morphisme nul.}}$$

Variante : Soit $f : (\mathbb{Q}, +) \to (\mathbb{Z}, +)$ un morphisme de groupes. L'ensemble $\mathrm{Im}\, f$ est un sous-groupe de $(\mathbb{Z}, +)$ donc il existe $n \in \mathbb{N}$ tel que $\mathrm{Im}\, f = n\mathbb{Z}$. Supposons $n \neq 0$. Comme $n \in \mathrm{Im}\, f$, il existe $x \in \mathbb{Q}$ tel que $f(x) = n$. Puis

$$2f\left(\frac{x}{2}\right) = f(x) = n \quad \Longrightarrow \quad f\left(\frac{x}{2}\right) = \frac{n}{2} \in \mathrm{Im}\, f$$

ce qui contredit $\mathrm{Im}\, f = n\mathbb{Z}$.

Exercice 9 (**)

Soit n entier avec $n \geqslant 2$ et d un diviseur de n. Montrer qu'il existe un unique sous-groupe de $(\mathbb{Z}/n\mathbb{Z}, +)$ de cardinal d.

Corrigé : Soit d diviseur de n. L'ensemble $\{\bar{0}\}$ est l'unique sous-groupe d'ordre 1 de $\mathbb{Z}/n\mathbb{Z}$. On suppose $d > 1$. On a $n = cd$ avec c entier non nul puis $d\bar{c} = \bar{0}$ et $\ell\bar{c} \neq \bar{0}$ pour $\ell \in [\![1\,;\, d-1]\!]$ puisque les $\bar{k}$ pour $k \in [\![0\,;\, n-1]\!]$ sont deux à deux distincts. On en déduit $o(\bar{c}) = d$ et par conséquent $\langle \bar{c} \rangle$ est un sous-groupe de $(\mathbb{Z}/n\mathbb{Z}, +)$ d'ordre d décrit par

$$\langle \bar{c} \rangle = \{k\bar{c}, k \in \mathbb{Z}\} = \{\bar{0}, \bar{c}, \ldots, (d-1)\bar{c}\}$$

Montrons l'unicité de ce sous-groupe. Soit H sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ de cardinal d. Pour $\bar{x} \in \mathrm{H}$ et $x \in \bar{x}$, on a $d\bar{x} = \bar{0}$ d'où $dx \equiv 0\ [n]$, *i.e.* $dx = kn$ avec $k \in \mathbb{Z}$ puis $dx = kdc$ autrement dit $x = kc$ d'où $\bar{x} \in \langle \bar{c} \rangle$. Il s'ensuit que $\mathrm{H} \subset \langle \bar{c} \rangle$ et par égalité des cardinaux, on conclut que $\mathrm{H} = \langle \bar{c} \rangle$. Ainsi

$$\boxed{\text{Pour } d \text{ diviseur de } n, \text{ il existe un unique sous-groupe de } \mathbb{Z}/n\mathbb{Z} \text{ de cardinal } d.}$$

Exercice 10 (**)

Soit $n \geqslant 3$. Montrer que S_n est engendré par les permutations suivantes :

1. $\begin{pmatrix}1 & 2\end{pmatrix}, \ldots, \begin{pmatrix}1 & n\end{pmatrix}$;
2. $\begin{pmatrix}1 & 2\end{pmatrix}, \begin{pmatrix}2 & 3\end{pmatrix}, \ldots, \begin{pmatrix}n-1 & n\end{pmatrix}$;
3. $\begin{pmatrix}1 & 2\end{pmatrix}, \begin{pmatrix}2 & 3 & \ldots & n\end{pmatrix}$.

Corrigé : 1. Soit $(i,j) \in [\![2\,;\, n]\!]^2$ avec $i \neq j$. On observe

$$\begin{pmatrix}i & j\end{pmatrix} = \begin{pmatrix}1 & i\end{pmatrix}\begin{pmatrix}1 & j\end{pmatrix}\begin{pmatrix}1 & i\end{pmatrix}$$

Toute transposition est donc engendré par $\left\{\begin{pmatrix}1, k\end{pmatrix},\ k \in [\![2\,;\, n]\!]\right\}$ et comme les transpositions engendrent S_n, on conclut

$$\boxed{\mathrm{S}_n = \left\langle \left\{ \begin{pmatrix}1 & k\end{pmatrix},\ k \in [\![2\,;\, n]\!] \right\} \right\rangle}$$

Remarque : On a utilisé le fait que les 2-cycles sont conjuguées pour avoir l'intuition de cette décomposition.

2. Soit $\mathrm{H} = \left\langle \left\{ \begin{pmatrix}1 & 2\end{pmatrix}, \begin{pmatrix}2 & 3\end{pmatrix}, \ldots, \begin{pmatrix}n-1 & n\end{pmatrix} \right\} \right\rangle$. On montre par récurrence $\begin{pmatrix}1 & k\end{pmatrix} \in \mathrm{H}$ pour $k \in [\![2\,;\, n]\!]$. L'initialisation est vraie pour $k = 2$. On suppose la propriété vraie au rang $k \in [\![2\,;\, n-1]\!]$ fixé. On a

$$\begin{pmatrix}1 & k+1\end{pmatrix} = \begin{pmatrix}1 & k\end{pmatrix}\begin{pmatrix}k & k+1\end{pmatrix}\begin{pmatrix}1 & k\end{pmatrix} \in \mathrm{H}$$

d'où l'hérédité et d'après le résultat de la première question, on conclut

$$\boxed{\mathrm{S}_n = \left\langle \left\{ \begin{pmatrix}1 & 2\end{pmatrix}, \begin{pmatrix}2 & 3\end{pmatrix}, \ldots, \begin{pmatrix}n-1 & n\end{pmatrix} \right\} \right\rangle}$$

3. On observe

$$\forall k \in [\![2\,;\, n-1]\!] \qquad \begin{pmatrix}2 & 3 & \ldots & n\end{pmatrix}\begin{pmatrix}1 & k\end{pmatrix}\begin{pmatrix}2 & 3 & \ldots & n\end{pmatrix}^{-1} = \begin{pmatrix}1 & k+1\end{pmatrix}$$

Par récurrence, on trouve $\begin{pmatrix}1 & k\end{pmatrix} \in \left\langle \left\{ \begin{pmatrix}1 & 2\end{pmatrix}, \begin{pmatrix}2 & 3 & \ldots & n\end{pmatrix} \right\} \right\rangle$ pour tout $k \in [\![2\,;\, n]\!]$ et avec le résultat de la première question, on conclut

$$\boxed{\mathrm{S}_n = \left\langle \left\{ \begin{pmatrix}1 & 2\end{pmatrix}, \begin{pmatrix}2 & 3 & \ldots & n\end{pmatrix} \right\} \right\rangle}$$

Exercice 11 (**)

Soit $(\Omega, \mathscr{A}, \mathbb{P})$ un espace probabilisé, n un entier non nul et $(\mathrm{X}_i)_{1 \leqslant i \leqslant n}$ une famille de variables aléatoires indépendantes avec $\mathrm{X}_i \sim \mathscr{U}_{[\![1\,;\, i]\!]}$ pour tout $i \in [\![1\,;\, n]\!]$. On pose

$$\sigma_n = \begin{pmatrix}1 & \mathrm{X}_1\end{pmatrix}\begin{pmatrix}2 & \mathrm{X}_2\end{pmatrix}\ldots\begin{pmatrix}n & \mathrm{X}_n\end{pmatrix}$$

Montrer que $\sigma_n \sim \mathscr{U}_{\mathrm{S}_n}$.

Corrigé : On procède par récurrence sur n. Le cas $n = 1$ est immédiat. Supposons la propriété vraie pour $n \geqslant 1$ fixé. Soit $\sigma \in \mathrm{S}_{n+1}$. On a

$$\begin{aligned}\mathbb{P}(\sigma_{n+1} = \sigma) &= \mathbb{P}\left(\begin{pmatrix}1 & \mathrm{X}_1\end{pmatrix}\ldots\begin{pmatrix}n & \mathrm{X}_n\end{pmatrix}\begin{pmatrix}n+1 & \mathrm{X}_{n+1}\end{pmatrix} = \sigma\right) \\ &= \mathbb{P}\left(\begin{pmatrix}1 & \mathrm{X}_1\end{pmatrix}\ldots\begin{pmatrix}n & \mathrm{X}_n\end{pmatrix} = \sigma\begin{pmatrix}n+1 & \mathrm{X}_{n+1}\end{pmatrix}\right)\end{aligned}$$

D'après la formule des probabilités totales, on a

$$\mathbb{P}(\sigma_{n+1} = \sigma) = \sum_{i=1}^{n+1} \mathbb{P}\left(\begin{pmatrix}1 & \mathrm{X}_1\end{pmatrix}\ldots\begin{pmatrix}n & \mathrm{X}_n\end{pmatrix} = \sigma\begin{pmatrix}n+1 & i\end{pmatrix}, \mathrm{X}_{n+1} = i\right)$$

Par indépendance, il vient

$$\mathbb{P}(\sigma_{n+1}=\sigma)=\sum_{i=1}^{n+1}\mathbb{P}\left(\begin{pmatrix}1 & \mathrm{X}_1\end{pmatrix}\dots\begin{pmatrix}n & \mathrm{X}_n\end{pmatrix}=\sigma\begin{pmatrix}n+1 & i\end{pmatrix}\right)\mathbb{P}(\mathrm{X}_{n+1}=i)$$

La permutation $\begin{pmatrix}1 & \mathrm{X}_1\end{pmatrix}\dots\begin{pmatrix}n & \mathrm{X}_n\end{pmatrix}$ admet $n+1$ comme point fixe. La permutation $\sigma\begin{pmatrix}n+1 & i\end{pmatrix}$ admet $n+1$ comme point fixe si et seulement $i=\sigma^{-1}(n+1)$. Par suite, on a

$$\mathbb{P}(\sigma_{n+1}=\sigma)=\mathbb{P}\left(\begin{pmatrix}1 & \mathrm{X}_1\end{pmatrix}\dots\begin{pmatrix}n & \mathrm{X}_n\end{pmatrix}=\sigma\begin{pmatrix}n+1 & \sigma^{-1}(n+1)\end{pmatrix}\right)\mathbb{P}(\mathrm{X}_{n+1}=\sigma^{-1}(n+1))$$

En confondant $\begin{pmatrix}1 & \mathrm{X}_1\end{pmatrix}\dots\begin{pmatrix}n & \mathrm{X}_n\end{pmatrix}$ et $\sigma\begin{pmatrix}n+1 & \sigma^{-1}(n+1)\end{pmatrix}$ avec leurs restrictions à $[\![1\,;n]\!]$ puisqu'elles admettent $n+1$ comme point fixe, on obtient

$$\mathbb{P}(\sigma_{n+1}=\sigma)=\frac{1}{n!}\times\frac{1}{n+1}=\frac{1}{(n+1)!}$$

Par récurrence, on conclut $\boxed{\sigma_n\sim\mathscr{U}_{\mathrm{S}_n}}$

Remarque : C'est le principe de l'algorithme de *Fisher-Yates* implémenté dans la méthode `numpy.random.shuffle` en python. Cet algorithme agit en place avec une complexité temporelle en $\mathrm{O}(n)$.

Exercice 12 (**)

Soit n entier non nul. Pour $\sigma\in\mathrm{S}_n$, on pose $\mathrm{M}_\sigma=\left(\delta_{i,\sigma(j)}\right)_{(i,j)\in[\![1\,;n]\!]^2}\in\mathscr{M}_n(\mathbb{R})$ et $f_\sigma\in\mathscr{L}(\mathbb{R}^n)$ l'application canoniquement associée. Déterminer la nature de l'application de $\dfrac{1}{n!}\displaystyle\sum_{\sigma\in\mathrm{S}_n}f_\sigma$ et préciser son noyau et son image.

Corrigé : Notons $f=\dfrac{1}{n!}\displaystyle\sum_{\sigma\in\mathrm{S}_n}f_\sigma$ puis $\mathrm{M}=\mathrm{mat}_{\mathscr{C}}f$ avec $\mathscr{C}$ base canonique de $\mathbb{R}^n$. Notant $\mathrm{M}=\left(m_{i,j}\right)_{1\leqslant i,j\leqslant n}$, on a

$$\forall(i,j)\in[\![1\,;n]\!]^2\qquad m_{i,j}=\frac{1}{n!}\sum_{\sigma\in\mathrm{S}_n}\delta_{i,\sigma(j)}=\frac{1}{n!}\,\mathrm{Card}\,\{\sigma\in\mathrm{S}_n\mid\sigma(j)=i\}=\frac{(n-1)!}{n!}=\frac{1}{n}$$

Notant $\mathrm{J}\in\mathscr{M}_n(\mathbb{R})$ la matrice constituée de 1, on a $\mathrm{M}=\dfrac{1}{n}\mathrm{J}$ et $\mathrm{J}^2=n\mathrm{J}$ d'où $\mathrm{M}^2=\mathrm{M}$. Sans difficulté, on trouve $\mathrm{Ker}\,\mathrm{M}:\displaystyle\sum_{i=1}^{n}x_i=0$ et $\mathrm{Im}\,\mathrm{M}=\mathrm{Vect}\,(u)$ avec $u=(1,\dots,1)$ et on conclut

$$\boxed{\text{L'application } f \text{ est le projecteur sur } \mathrm{Vect}\,(u) \text{ parallèlement à l'hyperplan } \sum_{i=1}^{n}x_i=0.}$$

Variante : Notons $\mathrm{E}=\mathbb{R}^n$, $\mathscr{B}=(e_i)_{1\leqslant i\leqslant n}$ da base canonique. Soit $\sigma\in\mathrm{S}_n$. Pour $x=\displaystyle\sum_{i=1}^{n}x_ie_i\in\mathrm{E}$,

on a $$f_\sigma(x)=f_\sigma\left(\sum_{i=1}^{n}x_ie_i\right)=\sum_{i=1}^{n}x_if(e_i)=\sum_{i=1}^{n}x_ie_{\sigma(i)}=\sum_{i=1}^{n}x_{\sigma^{-1}(e_i)}e_i$$

Ainsi $$f(x)=\frac{1}{n!}\sum_{\sigma\in\mathrm{S}_n}\sum_{i=1}^{n}x_{\sigma^{-1}(e_i)}e_i=\sum_{i=1}^{n}\left(\sum_{\sigma\in\mathrm{S}_n}x_{\sigma^{-1}(e_i)}\right)e_i$$

Or $$\sum_{\sigma\in\mathrm{S}_n}x_{\sigma^{-1}(e_i)}=\sum_{j=1}^{n}\sum_{\sigma\in\mathrm{S}_n\mid\sigma(j)=i}x_j=\sum_{j=1}^{n}x_j\,\mathrm{Card}\,\{\sigma\in\mathrm{S}_n\mid\sigma(j)=i\}=(n-1)!\sum_{j=1}^{n}x_j$$

Ainsi $$f(x) = \frac{1}{n}\left(\sum_{j=1}^{n} x_j\right)\left(\sum_{i=1}^{n} e_i\right)$$

On retrouve le résultat précédent.

Exercice 13 (**)

Soit n entier non nul. Déterminer un sous-groupe de $(\mathbb{R}, +)$ isomorphe à $(\mathbb{Z}^n, +)$.

Corrigé : Soient $p_1, \ldots, p_n$ des nombres premiers deux à deux distincts. On pose

$$\mathrm{H} = \left\{\sum_{i=1}^{n} \alpha_i \ln(p_i),\ (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n\right\}$$

On vérifie sans difficulté que H est sous-groupe de $(\mathbb{R}, +)$. Puis, on définit

$$\varphi\colon \begin{cases} \mathbb{Z}^n & \longrightarrow \mathrm{H} \\ (\alpha_1, \ldots, \alpha_n) & \longmapsto \displaystyle\sum_{i=1}^{n} \alpha_i \ln(p_i) \end{cases}$$

C'est clairement un morphisme de groupes additifs et pour $(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n$, on a

$$\varphi(\alpha_1, \ldots, \alpha_n) = 0 \iff \ln\left(\prod_{i=1}^{n} p_i^{\alpha_i}\right) = 0 \iff \prod_{i=1}^{n} p_i^{\alpha_i} = 1$$

On note $\mathrm{I} = \{i \in [\![\, 1\,;\, n\,]\!] \mid \alpha_i \geqslant 0\}$ et $\mathrm{J} = [\![\, 1\,;\, n\,]\!] \setminus \mathrm{I}$. Il vient

$$\varphi(\alpha_1, \ldots, \alpha_n) = 0 \iff \prod_{i\in\mathrm{I}} p_i^{\alpha_i} = \prod_{i\in\mathrm{J}} p_i^{-\alpha_i}$$

Par unicité de la décomposition en facteurs premiers, on en déduit

$$\prod_{i\in\mathrm{I}} p_i^{\alpha_i} = \prod_{i\in\mathrm{J}} p_i^{-\alpha_i} \iff \forall i \in [\![\, 1\,;\, n\,]\!] \qquad \alpha_i = 0$$

et on conclut

$$\boxed{\text{Le sous-groupe H de } (\mathbb{R}, +) \text{ est isomorphe à } (\mathbb{Z}^n, +).}$$

Remarque : On peut vérifier sans difficulté que $\mathrm{H} = \langle\{\ln(p_1), \ldots, \ln(p_n)\}\rangle$.