2 Solution proposée

I.A.1. La loi + est interne et commutative. Montrons qu'elle est associative. On a

$$\begin{aligned}
(x+y)+z &= [(\overline{x+y}) \setminus z] \quad [(x+y) \setminus \overline{z}] \\
&= \Big(\overline{(x \setminus \overline{y}) \quad (\overline{x} \setminus y)}\Big) \setminus z \quad [((x \setminus \overline{y}) \quad (\overline{x} \setminus y)) \setminus \overline{z}] \\
&= \big[\big((\overline{x \setminus \overline{y}}) \setminus (\overline{\overline{x} \setminus y})\big) \setminus z\big] \quad (x \setminus \overline{y} \setminus \overline{z}) \quad (\overline{x} \setminus y \setminus \overline{z}) \\
&= [((\overline{x} \quad y) \setminus (x \quad \overline{y})) \setminus z] \quad (x \setminus \overline{y} \setminus \overline{z}) \quad (\overline{x} \setminus y \setminus \overline{z}) \\
&= [((\overline{x} \setminus \overline{y}) \quad (x \setminus y)) \setminus z] \quad (x \setminus \overline{y} \setminus \overline{z}) \quad (\overline{x} \setminus y \setminus \overline{z}) \\
&= (\overline{x} \setminus \overline{y} \setminus z) \quad (x \setminus y \setminus z) \quad (x \setminus \overline{y} \setminus \overline{z}) \quad (\overline{x} \setminus y \setminus \overline{z})
\end{aligned}$$

Cette dernière expression est invariante par permutation circulaire, donc

$$(x+y)+z = (y+z)+x$$

et la commutativité de + permet d'obtenir $(x+y)+z = x+(y+z)$, ce qui prouve l'associativité.
L'élément neutre est car $x + = x$. Enfin le symétrique de x est x puisque $x + x =$.

I.A.2. $(\mathcal{P}(\Omega) \; + \;)$ est un espace vectoriel sur $\mathbb{F}_2$ puisque $(\mathcal{P}(\Omega) \; +)$ est un groupe abélien, et puisque la loi externe définie par $0 \times x =$ et $1 \times x = x$ vérifie bien les quatre axiomes d'un espace vectoriel :

a) $1 \times x = x$ (trivial)

b) $\Big(\lambda + \mu\Big) \times x = \Big(\lambda \times x\Big) + \big(\mu \times x\big)$. En effet

$$\begin{aligned}
\Big(0+1\Big) \times x &= \Big(0 \times x\Big) + \Big(1 \times x\Big) \text{ puisque } x = \quad + x \\
\text{et } \Big(1+1\Big) \times x &= \Big(1 \times x\Big) + \Big(1 \times x\Big) \text{ puisque } \quad = x + x
\end{aligned}$$

La propriété particulière de la loi de groupe + nous permettant de vérifier ce deuxième axiome est $x + x =$ vérifiée pour toute partie x.

c) $\lambda \times (x+y) = \Big(\lambda \times x\Big) + \Big(\lambda \times y\Big)$ (trivial)

d) $\lambda \times \big(\mu \times x\big) = \Big(\lambda\mu\Big) \times x$ (trivial)

Remarque : On aurait pu utiliser la bijection

$$\begin{array}{rccc}
\Psi : & \mathcal{P}(\Omega) & & \mathbb{F}_2^{\Omega} \\
& x & & \chi_x
\end{array}$$

qui à une partie x de Ω associe la fonction caractéristique χ_x, pour transporter la structure d'espace vectoriel de $\mathbb{F}_2^{\Omega}$ sur $\mathcal{P}(\Omega)$. On définit alors une loi interne et une loi externe dans $\mathcal{P}(\Omega)$ par transport de structure, et il suffit de vérifier que ces lois ne sont autre que la différence symétrique + et la multiplication que l'on vient d'introduire dans cette question. Cette méthode permet aussi de transporter la structure d'algèbre de $\mathbb{F}_2^{\Omega}$ sur $\mathcal{P}(\Omega)$, la multiplication interne étant alors égale à la loi intersection $\setminus$.

I.A.3. On sait que $\mathcal{P}(\Omega) = 2$ et que $\mathcal{P}(\Omega)$ est un $\mathbb{F}_2$-espace vectoriel. Nécessairement $\dim_{\mathbb{F}_2}(\mathcal{P}(\Omega)) =$. On retrouve ce résultat en exhibant une base de $\mathcal{P}(\Omega)$. Si $\Omega =$ t_1 t , et si l'on note x_i le singleton t_i , alors toute partie $x = t_{i_i}$ t_{i_k} de Ω s'écrit

$$x = \left(1\ x_{i_1}\right) + \quad + \left(1\ x_{i_k}\right)$$

et cela prouve que $(x_1$ $x\ )$ est un système générateur de $\mathcal{P}(\Omega)$. Ce système est une base de $\mathcal{P}(\Omega)$ parce qu'il est générateur et possède $\dim_{\mathbb{F}_2}(\mathcal{P}(\Omega)) =$ éléments.

Remarque : On peut vérifier directement que $(X_1$ $X\ )$ est libre en retournant à la définition, l'implication suivante étant immédiate :

$$\left(\lambda_1\ X_1\right) + \quad + \left(\lambda\ \ X\ \right) = \qquad \lambda_1 = \quad = \lambda\ = 0$$

I.A.4. L'application α est clairement symétrique. On a

$$\alpha\left(x + x\ \ y\right) = \overline{(x + x\ ) \setminus y} \underset{(1)}{=} \overline{(x \setminus y) + (x\ \setminus y)} \underset{(2)}{=} \overline{x \setminus y\ +\ x\ \setminus y\ - 2\ x \setminus x\ \setminus y}$$
$$= \overline{x \setminus y} + \overline{x\ \setminus y} = \alpha(x\ y) + \alpha\left(x\ \ y\right)$$

(1) provient de la distributivité de $\setminus$ sur $+$, et (2) peut se visualiser sur un diagramme de Venn. On a aussi

$$\alpha\left(0x\ y\right) = \overline{\ \setminus y} = 0 = 0 \times \alpha(x\ y) \text{ et } \alpha\left(1x\ y\right) = \overline{x \setminus y} = 1 \times \alpha(x\ y)$$

donc α est bilinéaire à gauche (et par conséquent aussi à droite). Pour démontrer que α est non dégénérée, il faut prouver

$$y \quad \alpha(x\ y) = \overline{x \setminus y} = 0 \qquad x =$$

Ecrire $\overline{x \setminus y} = 0$ signifie que le cardinal de l'intersection $x \setminus y$ est pair. On montre alors la contraposée de l'implication ci-dessus : si x était non vide, on pourrait choisir un éléments t dans x, et l'on aurait $\overline{x \setminus y} = 1$ pour $y = t$.

I.A.5. On a $\mathcal{D}(\Omega) =$ Ω . Comme est non dégénérée, on a

$$\dim \mathcal{H}(\Omega) + \dim \mathcal{D}(\Omega) = \dim \mathcal{P}(\Omega) = \quad \text{donc } \dim \mathcal{H}(\Omega) = \quad - 1$$

$\mathcal{H}(\Omega)$ est donc un hyperplan de $\mathcal{P}(\Omega)$ et l'on aura $\mathcal{H}(\Omega) = 2^{\ -1}$. Par ailleurs

$$x \quad \mathcal{H}(\Omega) \qquad \alpha(x\ \Omega) = 0 \qquad \overline{x \setminus \Omega} = 0 \qquad x \text{ pair.}$$

Le cardinal de $\mathcal{H}(\Omega)$ est donc aussi égal au nombre de parties de Ω de cardinal pair, et cela entraîne

$$C^0 + C^2 + \quad + C^{2k} + \quad + C\ = 2^{\ -1}$$

On a

$$\left(x \quad \operatorname{Ker} \alpha_{\ \mathcal{H}(\Omega)}\right) \qquad x \quad \mathcal{H}(\Omega) \text{ et } \left(\ y \quad \mathcal{H}(\Omega) \quad \alpha(x\ y) = \overline{x \setminus y} = 0\right)$$
$$x \text{ pair, et pour tout } y \text{ tel que } y \text{ soit pair on a } x \setminus y \text{ pair.} \quad (*)$$

Si x vérifie $(*)$ et si $x \qquad \Omega$, alors il existe $t \quad \Omega \quad x$. On choisit $t \quad x$ et l'on pose $y = \ t \ t \ $. Alors

$$x \setminus y \ = \left| x \setminus \left\{ t \ t \right\} \right| = \left| \left\{ t \right\} \right| = 1$$

en contradiction avec $(*)$. Cela prouve que $\operatorname{Ker} \alpha_{\mathcal{H}(\Omega)} \subset \qquad \Omega$. Comme l'inclusion réciproque est évidente, on aura

$$\operatorname{Ker} \alpha_{\mathcal{H}(\Omega)} = \qquad \Omega \ = \mathcal{D}(\Omega)$$

Remarque : On a $\mathcal{D}(\Omega) = \qquad \Omega \ \subset \mathcal{H}(\Omega) = \mathcal{D}(\Omega)$ ce qui prouve que $\mathcal{D}(\Omega) \setminus \mathcal{D}(\Omega) \ = \mathcal{D}(\Omega) = \qquad$, ce qui ne constitue pas une contradiction avec le fait que α est une forme bilinéaire symétrique non dégénérée.

I.B.1. Si $\mathcal{C} = \mathcal{C} \ $, alors $\dim \mathcal{C} \ + \dim \mathcal{C} = \dim \mathcal{P}(\Omega) = \quad$ entraîne $\dim \mathcal{C} \ = \frac{}{2}$. Ainsi $\mathcal{C} \ = 2^{\frac{}{2}}$ est pair et **I.A.5** donne $\mathcal{C} \subset \mathcal{H}(\Omega)$. En prenant l'orthogonal des deux membres, $\mathcal{C} \ \supset \mathcal{H}(\Omega)$ d'où $\mathcal{C} \supset \mathcal{D}(\Omega)$.

I.B.2. ▶ On a

$$P \ (X \ Y) = \left(X^2 + Y^2\right)^m = \sum_{k=0}^{m} C_m^k X^{2k} Y^{2(m-k)} = \sum_{k=0}^{m} C_m^k X^{2k} Y^{\ -2k}$$

et

$$P_{\mathcal{C}}(X \ Y) = \sum_{x \ \mathcal{C}} X^{\ x} Y^{\ -x} = \sum_{k=0}^{2m} N(k) \, X^k Y^{\ -k}$$

où $N(k) = \quad x \quad \mathcal{C} \quad x \ = k \ $. Comme $\mathcal{C}$ est auto-orthogonal, $\mathcal{C} \subset \mathcal{H}(\Omega)$ et tous les mots x de $\mathcal{C}$ seront de cardinal pair. Donc

$$P_{\mathcal{C}}(X \ Y) = \sum_{k=0}^{m} N(2k) \, X^{2k} Y^{\ -2k}$$

Trouver un code $\mathcal{C}$ tel que $P_{\mathcal{C}} = P \ $ revient donc à construire un sous-espace vectoriel $\mathcal{C}$ telle que

$$\begin{cases} k \quad 0 \quad m \quad N(2k) = C_m^k \\ k \quad \left\{0 \quad \left[\frac{m-1}{2}\right]\right\} \quad N(2k+1) = 0 \end{cases}$$

Construisons les éléments de $\mathcal{C}$ de la façon suivante : une partie x de $\mathcal{P}(\Omega)$ appartient à $\mathcal{C}$ si et seulement si il existe une partie $t_{i_1} \quad t_{i_k}$ de $t_1 \quad t_m$ telle que $x = \ t_{i_1} \quad t_{i_k} \ u_{i_1} \quad u_{i_k}$. Il est facile de voir que $\mathcal{C}$ est bien un sous-espace vectoriel. On a aussi $N(2k) = C_m^k$ et $N(2k+1) = 0$ pour tous k, par construction.

▶ Vérifions que $\mathcal{C}$ est auto-orthogonal. On a

$$\mathcal{C} \subset \mathcal{C} \qquad x \ y \quad \mathcal{C} \quad \overline{x \setminus y} = \overline{0} \qquad x \ y \quad \mathcal{C} \quad x \setminus y \ \text{ est pair}$$

et cette dernière affirmation est triviale puisque l'intersection de deux parties x et y de cardinaux pairs est encore une partie de cardinal pair. Comme $\quad t_1 \ u_1 \qquad t_m \ u_m \quad$ est

une base de $\mathcal{C}$, $\dim \mathcal{C} = m$ et l'inclusion $\mathcal{C} \subset \mathcal{C}$ entre deux espace de même dimension sera une égalité.

► Montrons que deux éléments $\mathcal{C}$ et $\mathcal{C}$ de $\Gamma(\Omega)$ sont isomorphes.
Si $\mathcal{C}$ $\Gamma(\Omega)$, alors $N(2k) = C_m^k$ pour tout k 0 m et $\mathcal{C} = 2^m$. En particulier si $k = 1$ il existe exactement m éléments de $\mathcal{C}$ de cardinal 2, notons-les :

$$t_1\ u_1 \qquad t_m\ u_m$$

On a $t_i\ u_i \setminus t_j\ u_j$ pour tous $i = j$. En effet $t_i\ u_i = t_j\ u_j$ par hypothèse, et $t_i\ u_i \setminus t_j\ u_j = t$ entrainerait $\alpha(\ t_i\ u_i \quad t_j\ u_j\ ) = \overline{t} = \overline{1}$, ce qui contredirait le fait que $\mathcal{C}$ est auto-orthogonal. Par conséquent

$$\Omega = t_1\ t_2 \quad t_m\ u_1\ u_2 \quad u_m$$

Comme $\dim \mathcal{C} = m$, comme le sous-espace vectoriel V de $\mathcal{P}(\Omega)$ engendré par les vecteurs $t_1\ u_1\ ,\ ,\ t_m\ u_m$ est de dimension m et comme $V \subset \mathcal{C}$, on déduit que ($t_1\ u_1 \qquad t_m\ u_m$) est une base de $\mathcal{C}$.
Le même raisonnement appliqué à $\mathcal{C}$ donne

$$\Omega = \{t_1\ t_2 \quad t_m\ u_1\ u_2 \quad u_m\}$$

et montre que ($t_1\ u_1 \qquad t_m\ u_m$) est une base de $\mathcal{C}$. Il est alors facile de vérifier que la permutation

$$\begin{array}{rll} s: & \Omega & \Omega \\ & t_i & t_i \\ & u_i & u_i \end{array}$$

est telle que $\overline{s}(\mathcal{C}) = \mathcal{C}$. En effet, tout mot x de $\mathcal{C}$ s'écrit

$$x = \underset{s\subset\ 1 \quad m}{\qquad\qquad} t_{i_s}\ u_{i_s}$$

et admettra pour image le mot

$$\overline{s}(x) = \underset{s\subset\ 1 \quad m}{\qquad\qquad} \{t_{i_s}\ u_{i_s}\}$$

qui appartient bien à $\mathcal{C}$. Ainsi $\overline{s}(\mathcal{C}) \subset \mathcal{C}$ et l'égalité des cardinaux donne $\overline{s}(\mathcal{C}) = \mathcal{C}$.

I.B.3.a. ► On a

$$\underset{h=1}{\overset{m}{\qquad}} \lambda_h\ _h = \qquad k \geq 2 \quad \lambda_k = \alpha\left(u_k \underset{h=1}{\overset{m}{\qquad}} \lambda_h\ _h\right) = \overline{0}$$

et donc aussi $\lambda_1 = \overline{0}$ en remplaçant.

► Comme m est pair, l'intersection de 2 éléments quelconques du système générateur de l'énoncé est de cardinal pair, donc $\mathcal{B} = (\mathcal{B}\ )$ et $\mathcal{B}$ est auto-orthogonal.

► $(\ _h)_{1\le h\le m}$ est un système libre à m éléments de $\mathcal{B}\ $, et $\dim(\mathcal{B}\ ) = m$ puisque $\mathcal{B}\ $ est auto-orthogonal. Donc $(\ _h)_{1\le h\le m}$ est une base de $\mathcal{B}\ $.

I.B.3.b. ► Si $\mu \subset \mathbb{N}_m$ et $\mu\ \subset \mathbb{N}_m$, alors

$$\begin{array}{l} \overline{\mu} + \overline{\mu\ } = \left(\overline{\mu}\quad \overline{\mu\ }\right)\ \ \left(\overline{\mu} \setminus \overline{\mu\ }\right) = \left(\overline{\mu}\quad \overline{\mu\ }\right) \setminus \overline{\left(\overline{\mu} \setminus \overline{\mu\ }\right)} = \left(\overline{\mu}\quad \overline{\mu\ }\right) \setminus (\mu\quad \mu\ ) \\ \mu + \mu\ = (\mu\quad \mu\ )\ \ (\mu \setminus \mu\ ) = (\mu\quad \mu\ ) \setminus \overline{(\mu \setminus \mu\ )} = (\mu\quad \mu\ ) \setminus \left(\overline{\mu}\quad \overline{\mu\ }\right) \end{array}$$

donc $\overline{\mu} + \overline{\mu\ } = \mu + \mu\ $, et

$$\begin{array}{l} \mu + \overline{\mu\ } = \underline{\left(\mu\quad \overline{\mu\ }\right) \setminus \overline{\left(\mu \setminus \overline{\mu\ }\right)}} = \left(\mu\quad \overline{\mu\ }\right) \setminus (\overline{\mu}\quad \mu\ ) = \left(\overline{\mu\ } \setminus \overline{\mu}\right)\quad (\mu \setminus \mu\ ) \\ \overline{\mu + \mu\ } = (\mu\quad \mu\ ) \setminus \overline{(\mu \setminus \mu\ )} = \overline{(\mu\quad \mu\ )}\quad (\mu \setminus \mu\ ) = \left(\overline{\mu\ } \setminus \overline{\mu}\right)\quad (\mu \setminus \mu\ ) \end{array}$$

donc $\mu + \overline{\mu\ } = \overline{\mu + \mu\ }$.

► Montrons que $\mathcal{B}\ $ est un sous-espace vectoriel de $\mathcal{P}(\Omega)$. Tout d'abord $\mathcal{B}\ $ est trivialement stable par multiplication par $\overline{0}$ ou $\overline{1}$. Ensuite il s'agit de vérifier que $\mathcal{B}\ $ est stable par addition. On envisage les 3 cas possibles :

a)

$$\begin{array}{rcl} x_\mu + x_\mu & = & t_h\quad h\quad \mu\ + \left\{t_h\quad h\quad \mu\ \right\} + \ u_h\quad h\quad \mu\ + \left\{u_h\quad h\quad \mu\ \right\} \\ & = & \left\{t_h\quad h\quad \mu + \mu\ \right\} + \left\{u_h\quad h\quad \mu + \mu\ \right\} \\ & = & x_{\mu+\mu}\quad \mathcal{B} \end{array}$$

b)

$$\begin{array}{rcl} y_\mu + y_\mu & = & t_h\quad h\quad \mu\ + \left\{t_h\quad h\quad \mu\ \right\} + \ u_h\quad h\quad \mathbb{N}_m\ \mu\ + \left\{u_h\quad h\quad \mathbb{N}_m\ \mu\ \right\} \\ & = & \left\{t_h\quad h\quad \mu + \mu\ \right\} + \left\{u_h\quad h\quad \overline{\mu} + \overline{\mu\ }\right\} \\ & = & \left\{t_h\quad h\quad \mu + \mu\ \right\} + \left\{u_h\quad h\quad \mu + \mu\ \right\}\ (\text{puisque } \overline{\mu} + \overline{\mu\ } = \mu + \mu\ ) \\ & = & x_{\mu+\mu}\quad \mathcal{B} \end{array}$$

c)

$$\begin{array}{rcl} x_\mu + y_\mu & = & t_h\quad h\quad \mu\ + \left\{t_h\quad h\quad \mu\ \right\} + \ u_h\quad h\quad \mu\ + \left\{u_h\quad h\quad \overline{\mu\ }\right\} \\ & = & \left\{t_h\quad h\quad \mu + \mu\ \right\} + \left\{u_h\quad h\quad \mu + \overline{\mu\ }\right\} \\ & = & \left\{t_h\quad h\quad \mu + \mu\ \right\} + \left\{u_h\quad h\quad \overline{\mu + \mu\ }\right\}\ (\text{puisque } \mu + \overline{\mu\ } = \overline{\mu + \mu\ }) \\ & = & y_{\mu+\mu}\quad \mathcal{B} \end{array}$$

► Montrons que $\mathcal{B}\ = \mathcal{B}\ $: On a déjà $\mathcal{B}\ \subset \mathcal{B}\ $. Réciproquement, $\mathcal{B}\ $ est un sous-espace vectoriel qui contient le système générateur $(\ _h)_{1\le h\le m}$ de $\mathcal{B}\ $ puisque :

$$\left\{\begin{array}{l} {}_1 = \ t_1\ t_2\quad t_m\ = y_\Omega \\ h\quad 2\quad m\quad {}_h = \ t_1\ t_h\ u_1\ u_h\ = x_{\ 1\,h} \end{array}\right.$$

Par conséquent $\mathcal{B}\ \supset \mathcal{B}\ $.

I.B.3.c. On a

$$Q\ \ (X\ Y) = \sum_{\substack{\mu\subset\mathbb{N}_m\\ \mu\ \text{pair}}} X^{\,x_\mu}\,Y^{\ -x_\mu} + \sum_{\substack{\mu\subset\mathbb{N}_m\\ \mu\ \text{pair}}} X^{\,y_\mu}\,Y^{\ -y_\mu}$$

On a aussi $x_\mu = 2\ \mu$, $y_\mu = m$,

$$\mu\subset\mathbb{N}_m \quad \mu = 2k \quad = C_m^{2k} \text{ et } \quad \mu\subset\mathbb{N}_m \quad \mu \ \text{ pair} \quad = 2^{m-1}$$

On déduit

$$Q\ \ (X\ Y) = \sum_{k=0}^{\frac{m}{2}} C_m^{2k} X^{4k} Y^{\ -4k} + 2^{m-1} X^m Y^{\ -m}$$

On retrouve le polynôme de l'énoncé puisque

$$\begin{aligned}
&\frac{1}{2}\left(\left(X^2+Y^2\right)^m + \left(X^2-Y^2\right)^m + (2XY)^m\right)\\
&= \frac{1}{2}\left(\sum_{k=0}^{m} C_m^k X^{2k} Y^{2m-2k} + \sum_{k=0}^{m} C_m^k\,(-1)^{m-k}\,X^{2k}Y^{2m-2k} \quad + 2^{m-1}X^mY^m\right.\\
&= \sum_{k=0}^{\frac{m}{2}} C_m^{2k} X^{4k} Y^{\ -4k} + 2^{m-1} X^m Y^{\ -m} = Q\ \ (X\ Y)
\end{aligned}$$

I.B.3.d. Les éléments de $\mathcal{B}$ sont de la forme x_μ ou y_μ, et l'on a $x_\mu = 2\ \mu$ avec μ pair, et $y_\mu = m$. Ainsi $\mathcal{B}$ sera pair si et seulement si m $4\mathbb{Z}$, i.e. $8\mathbb{Z}$.

I.B.3.e. ▶ On a

$$Q_{16}\,(X\ Y) = \sum_{(x\ x\ )\ \mathcal{C}\times\mathcal{C}} X^{\,x\ +x\ }\ Y^{\,\Omega\ -x\ +\Omega\ -x\ } = \left(Q_8\,(X\ Y)\right)^2 = Q_{16}\,(X\ Y)$$

▶ Montrons que $\bigcup_{y\ \mathcal{E}} y = \Omega$. Pour tout couple $(h\ j)$ $\mathbb{N}_m^2$ tel que $h = j$, on a $t_h\ t_j\ u_h\ u_j$ $\mathcal{E}$, donc

$$\Omega = \bigcup_{h=j} t_h\ t_j\ u_h\ u_j\ \subset \bigcup_{y\ \mathcal{E}} y \subset \Omega.$$

▶ Montrons que $\bigcup_{y\ \mathcal{E}} y = \Omega$. On a

$$\Omega = \ t_1\ t_2 \quad t_8\ u_1\ u_2 \quad u_8 \ = \underbrace{t_1\ t_2\ t_3\ t_4}_{\Omega}\ \underbrace{u_1\ u_2\ u_3\ u_4} \quad \underbrace{t_5\ t_6\ t_7\ t_8}_{\Omega}\ \underbrace{u_5\ u_6\ u_7\ u_8}$$

Si y $\mathcal{E}$ alors $x \setminus y = 2$ donc il existe $i\ j$ $1\ 2\ 3\ 4$ tels que $y \supset t_i\ t_j$. On montre alors que y ne peut pas couper Ω , ce qui prouvera l'inclusion $\bigcup_{y\ \mathcal{E}} y \subset \Omega$. Comme

l'inclusion réciproque est évidente (en effet $t_i\ t_j\ u_i\ u_j \quad \mathcal{E}$ par construction et pour tout couple $(i\ j)$), on en déduira l'égalité.

On a ainsi $y \supset t_i\ t_j$ et $y \quad \mathcal{B}_{16}$ donc $y = x + x$ avec $x \quad \mathcal{C}$ et $x \quad \mathcal{C}$. Les éléments de $\mathcal{C}$ sont de la forme (**I.B.3.b**) $x = x_\mu$ ou y_μ, et l'on envisage 2 cas :

- Si $x = x_\mu$ alors $y = x + x \supset t_i\ t_j\ u_i\ u_j$, et l'hypothèse $y = 4$ entraîne $y = t_i\ t_j\ u_i\ u_j \subset \Omega$
- Si $x = y_\mu$ alors $y \supset t_i\ t_j\ u_k\ u_l$ où l'on a posé $i\ j\ k\ l = 1\ 2\ 3\ 4$, et l'hypothèse $y = 4$ entraîne $y = t_i\ t_j\ u_k\ u_l \subset \Omega$.

▶ Si $\mathcal{B}_{16}$ et $\mathcal{B}_{16}$ étaient isomorphes, les parties à 4 éléments de $\mathcal{B}_{16}$ et $\mathcal{B}_{16}$ devraient se correspondre par une permutation. Si l'on pose

$$\begin{cases} \mathcal{E}_x = \{y \quad \mathcal{B}_{16} \quad y = 4 \text{ et } x \setminus y = 2\} \\ \mathcal{E}_x = \{y \quad \mathcal{B}_{16} \quad y = 4 \text{ et } x \setminus y = 2\} \end{cases}$$

il devrait exister une partie à 4 éléments x de Ω et une partie à 4 éléments x de Ω telles que les éléments de $\mathcal{E}_x$ se déduisent de ceux de $\mathcal{E}_x$ par une permutation. Alors $\mathcal{E}_x = \mathcal{E}_x$, ce qui est absurde puisque

$$\underset{y\ \mathcal{E}_x}{} y = \Omega \text{ tandis que } \underset{y\ \mathcal{E}_x}{} y = \Omega \text{ ou } \Omega \ .$$

I.B.4.a. On a

$$\begin{aligned} \underset{x\ \mathcal{C}}{} f(x) &= \underset{x\ \mathcal{C}\ y\ \mathcal{P}(\Omega)}{} (-1)^{\alpha(x\ y)} f(y) = \underset{y\ \mathcal{P}(\Omega)}{} \left(\underset{x\ \mathcal{C}}{} (-1)^{\alpha(x\ y)} \quad f(y) \right. \\ &= \underset{y\ \mathcal{C}}{} \left(\underset{x\ \mathcal{C}}{} (-1)^{\overline{0}} \quad f(y) + \underset{y\ \mathcal{C}}{} \left(\underset{x\ \mathcal{C}}{} (-1)^{\alpha(x\ y)} \quad f(y) \right. \right. \\ &= 2^{\dim \mathcal{C}} \underset{y\ \mathcal{C}}{} f(y) + \underset{y\ \mathcal{C}}{} \left(\underset{x\ \mathcal{C}}{} (-1)^{\alpha(x\ y)} \quad f(y) \right. \end{aligned}$$

et la formule sera démontrée si l'on prouve que $\underset{x\ \mathcal{C}}{} (-1)^{\alpha(x\ y)} = 0$. Soit $y \quad \mathcal{C}$ fixé. Il existe alors $x \quad \mathcal{C}$ tel que $\alpha(x\ y) = \overline{1}$. Par suite

$$H := \{x \quad \mathcal{C} \quad \alpha(x\ y) = \overline{1}\} = \{x \quad \mathcal{C} \quad \alpha(x - x\ y) = \overline{0}\}$$

est un sous-espace affine de direction le noyau de la forme linéaire non nulle $z \quad \alpha(z\ y)$. C'est donc un hyperplan affine de $\mathcal{P}(\Omega)$ et l'on aura $H = 2^{-1}$. Cela entraîne $\mathcal{P}(\Omega) \quad H = 2 \quad -2^{-1} = 2^{-1}$ puis $\underset{x\ \mathcal{C}}{} (-1)^{\alpha(x\ y)} = 0$.

I.B.4.b. La formule de la question précédente devient

$$\underset{x\ \mathcal{C}}{} f(x) = 2^{\dim \mathcal{C}} \underset{y\ \mathcal{C}}{} X^{\,y}\, Y^{\,-y}$$

Donc

$$\textbf{(MW)} \qquad 2^{\dim \mathcal{C}} \sum_{x \ \mathcal{C}} X^{\,x}\, Y^{\,-x} = \sum_{x \ \mathcal{C}} (Y-X)^{\,x}\, (X+Y)^{\,-x}$$

$$\sum_{x \ \mathcal{C}} f(x) = \sum_{x \ \mathcal{C}} (Y-X)^{\,x}\, (X+Y)^{\,-x}$$

Pour prouver **(MW)** il suffit ainsi de prouver l'égalité

$$f(x) = (Y-X)^{\,x}\, (X+Y)^{\,-x} \qquad (*)$$

pour tout $x \quad \mathcal{C}$. En utilisant les indications de l'énoncé,

$$\begin{aligned} f(x) &= \sum_{y \ \mathcal{P}(\Omega)} (-1)^{\alpha(x\,y)}\, X^{\,y}\, Y^{\,-y} \\ &= \sum_{y_1 \ \ x \text{ et } y_2 \subset \Omega \ x} (-1)^{\alpha(x\,y_1+y_2)}\, X^{\,y_1+\,y_2}\, Y^{\,-y_1-\,y_2} \\ &= S_1 \times S_2 \end{aligned}$$

où

$$S_1 = \sum_{y_1 \ \ x} (-1)^{\alpha(x\,y_1)}\, X^{\,y_1}\, Y^{\,x\,-\,y_1} \quad \text{et} \quad S_2 = \sum_{y_2 \subset \Omega \ x} (-1)^{\alpha(x\,y_2)}\, X^{\,y_2}\, Y^{\,-\,x\,-\,y_2}$$

Le nombre de parties de x à k éléments est C_x^k donc

$$S_1 = \sum_{k=0}^{x} (-1)^k\, C_x^k\, X^k Y^{\,x\,-k} = (Y-X)^{\,x}$$

Par ailleurs, comme $\alpha(x \ y_2) = \overline{0}$ pour tout $y_2 \subset \Omega \ x$, on obtient

$$S_2 = \sum_{k=0}^{-\,x} C^k_{\,-\,x}\, X^k Y^{\,-\,x\,-k} = (X+Y)^{\,-\,x}$$

L'égalité $(*)$ s'en déduit.

II.A.1.a. ▶ Si $v \quad V^G$ alors $p_G(v) = \frac{1}{G} \sum_{g \ G} g(v) = \frac{1}{G} \sum_{g \ G} v = v$ donc $v \quad \mathrm{Im}(p_G)$. Réciproquement, si $w \quad \mathrm{Im}(p_G)$ il existe $v \quad V$ tel que $w = p_G(v) = \frac{1}{G} \sum_{g \ G} g(v)$. Alors pour tout $h \quad G$,

$$h(w) = \frac{1}{G} \sum_{g \ G} h \circ g(v) = \frac{1}{G} \sum_{g \ G} g(v) = w$$

donc $w \quad V^G$. On a montré l'égalité $\mathrm{Im}(p_G) = V^G$.

▶ Si $v \quad V$ alors $p_G(v) \quad V^G$ et la première partie de la preuve ci-dessus montre que

$$p_G(p_G(v)) = p_G(v)$$

Autrement dit $p_G \circ p_G = p_G$ et p_G est un projecteur de V.

II.A.1.b. On a

$$\mathrm{Tr}\,(p_G) = \frac{1}{G} \sum_{g \ G} \mathrm{Tr}\,(g)$$

si bien que la formule de l'énoncé sera prouvée si l'on démontre que $\mathrm{Tr}\,(p_G) = \dim\left(V^G\right)$. L'application p_G est la projection sur $\mathrm{Im}\,(p_G) = V^G$ parallèlement à $\mathrm{Ker}\,(p_G)$. Soit $(v_1 \quad v_k)$ une base de V^G, et $(v_{k+1} \quad v_n)$ une base de $\mathrm{Ker}\,(p_G)$. La matrice de p_G dans la base $v = (v_1 \quad v_n)$ sera

$$\mathrm{Mat}\,(p_G; v) = \begin{matrix} 1 & & 0 & 0 & & 0 \\ \vdots & \ddots & & \vdots & & \vdots \\ 0 & & 1 & 0 & & 0 \\ 0 & & 0 & 0 & & 0 \\ \vdots & & \vdots & \vdots & \ddots & \vdots \\ 0 & & 0 & 0 & & 0 \end{matrix}$$

d'où $\mathrm{Tr}\,(p_G) = k = \dim\left(V^G\right)$.

II.A.1.c. Posons $G = \quad (G\,)$. La question **II.A.1.b** permet d'écrire

$$\dim\left(V^G\right) = \dim\left(V^G\right) = \frac{1}{G} \sum_{g \ G} \mathrm{Tr}\,(g) \qquad (*)$$

Chacun des éléments g de G s'écrit $g = \quad (g\,)$ où $g \quad G$ et l'on a

$$\{g \quad G \quad (g\ ) = g\} = \{g \quad G \quad (g\ g^{-1}) = Id\} = g \ \ (\mathrm{Ker}\ \ )$$

donc

$$\left|\{g \quad G \quad (g\ ) = g\}\right| = \left|g \ \ (\mathrm{Ker}\ \ )\right| = \mathrm{Ker}\ \ = \frac{G}{G}$$

En remplaçant dans $(*)$:

$$\dim\left(V^G\right) = \dim\left(V^G\right) = \frac{1}{G}\frac{1}{\mathrm{Ker}} \sum_{g \ G} \mathrm{Tr}\,(\ \ (g\,)) = \frac{1}{G} \sum_{g \ G} \mathrm{Tr}\,(\ \ (g\,))$$

Remarque : On obtient une amélioration de la question précédente qui montre que la formule reste vraie dans le cas général où l'action de G sur V n'est pas forcément fidèle.

II.A.2.a. ▶ On a clairement $\sigma_g\,(\lambda P + Q) = \lambda\sigma_g\,(P) + \sigma_g\,(Q)$ et $\sigma_g\,(PQ) = \sigma_g\,(P)\,\sigma_g\,(Q)$ pour tous scalaire λ et pour tous polynômes P et Q. On a aussi $\sigma_{Id} = Id_A$, donc σ_g est un homomorphisme d'algèbre de A dans A.

▶ Si M représente la matrice de g dans la base e, ce qu'on notera $M = \mathrm{Mat}\,(g; e)$, on a

$$\sigma_g\,(P)\,(X_1 \quad X_n) = P\,((X_1 \quad X_n)\,M)$$

ce que l'on notera plus simplement

$$\sigma_g(P) = P((X_1 \quad X_n)M)$$

Si $g\ g$ $\mathrm{Aut}(V)$ posons $N = \mathrm{Mat}(g\,;e)$. On a

$$\left(\sigma_g \circ \sigma_g\right)(P) = \sigma_g\left[\sigma_g\ (P)\right] = \sigma_g\ (P)(X_1 \quad X_n)M = P((X_1 \quad X_n)MN) = \sigma_{g\circ g}\ (P)$$

donc

$$g\ g \quad \mathrm{Aut}(V) \quad \sigma_{g\circ g} = \sigma_g \circ \sigma_g$$

Cela prouve que :

a) σ_g est un automorphisme de A. En effet, pour $g = g^{-1}$ on obtient

$$Id_A = \sigma_{Id} = \sigma_g \circ \sigma_{g^{-1}} \text{ et } Id_A = \sigma_{Id} = \sigma_{g^{-1}} \circ \sigma_g$$

de sorte que σ_g soit bijective, d'inverse $(\sigma_g)^{-1} = \sigma_{g^{-1}}$.

b) Ψ est un morphisme de groupes.

II.A.2.b. ► $X_1^{\alpha_1}X_2^{\alpha_2} \quad X_n^{\alpha_n}$ $\alpha_1 + \quad + \alpha_n = k$ est une base de A_k, et le nombre de n-uplets d'entiers $(\alpha_1 \quad \alpha_n)$ tels que $\alpha_1 + \quad + \alpha_n = k$ est C_{n-1+k}^k, donc $a_k = C_{n-1+k}^k$.

► Pour montrer l'inclusion $\sigma_g(A_k) \subset A_k$ il suffit, par linéarité, de montrer que

$$\sigma_g(X_1^{\alpha_1}X_2^{\alpha_2} \quad X_n^{\alpha_n}) \quad A_k$$

dès que $\alpha_1 + \quad + \alpha_n = k$. Comme chacun des polynômes $\left(\sum_{j=1}^{n} \gamma_{ji}X_j\right)^{\alpha_m}$ est homogène de degré α_m, le polynôme

$$\sigma_g(X_1^{\alpha_1}X_2^{\alpha_2} \quad X_n^{\alpha_n}) = \left(\sum_{j=1}^{n} \gamma_{j1}X_j\right)^{\alpha_1} \left(\sum_{j=1}^{n} \gamma_{jn}X_j\right)^{\alpha_n}$$

sera bien homogène de degré k. On aura de la même manière $\sigma_{g^{-1}}(A_k) \subset A_k$ d'où $A_k \subset \sigma_g(A_k)$ en composant des deux côtés par σ_g. En conclusion $\sigma_g(A_k) = A_k$.

II.A.3. On a $a_k(G) \leq a_k$ pour tout k, donc la convergence absolue de $\sum_{k=0}^{+} a_k z^k$ entrainera celle de $\sum_{k=0}^{+} a_k(G)\, z^k$. On a

$$\frac{a_{k+1}}{a_k} = \frac{C_{n+k}^{k+1}}{C_{n-1+k}^k} = \frac{(n+k)!}{(k+1)!\,(n-1)!}\ \frac{k!\,(n-1)!}{(n+k-1)!} = \frac{n+k}{k+1}$$

donc $\lim_{k\ +} \frac{a_{k+1}}{a_k} = 1$ et le rayon de convergence de la série entière $\sum_{k=0}^{+} a_k z^k$ sera $R = 1$. Celui de $\sum_{k=0}^{+} a_k(G)\, z^k$ sera donc ≥ 1.

II.A.4. $g^G = Id$ donc toutes les valeurs propres de g sont de module 1, et $\frac{1}{\det(Id-zg)}$ sera bien définie si $z=0$, ou si $\left|\frac{1}{z}\right| = 1$. En particulier la fonction $z \quad \frac{1}{\det(Id-zg)}$ sera C et définie sur le disque ouvert $z < 1$. Elle est donc développable en série entière sur ce disque et le rayon de convergence de $\sum_{k=0}^{+} r_k z^k$ sera ≥ 1.

II.A.4.b. Aucun des α_i n'est nul puisque g est bijective. Si $z < 1$,

$$\frac{1}{\det(Id-zg)} = \frac{1}{(1-z\alpha_1) \quad (1-z\alpha_n)} = \prod_{i=1}^{n} \sum_{k_i=0}^{+} (z\alpha_i)^{k_i} = \sum_{k=0}^{+} r_k z^k$$

avec

$$r_k = \sum_{\alpha_1 + \quad + \alpha_n = k} \alpha_1^{k_1} \quad \alpha_n^{k_n}$$

Par ailleurs $M = \mathrm{Mat}(g;e) = \mathrm{diag}(\alpha_1 \qquad \alpha_n)$ entraîne

$$\begin{aligned} g_k\left(X_1^{k_1} X_2^{k_2} \quad X_n^{k_n}\right) &= \sigma_g\left(X_1^{k_1} X_2^{k_2} \quad X_n^{k_n}\right) = (\alpha_1 X_1)^{k_1} \quad (\alpha_n X_n)^{k_n} \\ &= \left(\alpha_1^{k_1} \quad \alpha_n^{k_n}\right) X_1^{k_1} \quad X_n^{k_n} \end{aligned}$$

d'où

$$\mathrm{Tr}(g_k) = \sum_{\alpha_1 + \quad + \alpha_n = k} \alpha_1^{k_1} \quad \alpha_n^{k_n} = r_k$$

II.A.4.c. $g^G = Id$ et $\mathbb{C}$ est algébriquement clos, donc g annule le polynôme scindé $X^G - 1$ dont toutes les racines sont simples. Cela montre que g est diagonalisable. Il existe donc des automorphismes u et g de V tels que

$$g = u^{-1} g u \quad \text{et} \quad \mathrm{Mat}(g\,;e) = \mathrm{diag}(\alpha_1 \qquad \alpha_n)\,.$$

Alors

$$\begin{aligned} \frac{1}{\det(Id-zg)} = \frac{1}{\det(Id-zg\,)} &= \sum_{k=0}^{+} \mathrm{Tr}\left(g_k\right) z^k \quad \text{d'après } \textbf{II.A.4.b} \\ &= \sum_{k=0}^{+} \mathrm{Tr}(g_k)\, z^k \quad \text{car } g_k = u_k^{-1} g_k u_k \end{aligned}$$

Finalement $\mathrm{Tr}(g_k) = r_k$.

II.A.4.d. La question **II.A.1.c** implique

$$a_k(G) = \dim\left(A_k^G\right) = \frac{1}{G} \sum_{g \quad G} \mathrm{Tr}(g_k)$$

Alors, pour $z < 1$,

$$\Phi_G(z) = \sum_{k=0}^{+\infty} a_k(G)\, z^k = \sum_{k=0}^{+\infty} \frac{1}{G} \sum_{g \in G} \mathrm{Tr}(g_k)\, z^k = \frac{1}{G} \sum_{g \in G} \left(\sum_{k=0}^{+\infty} \mathrm{Tr}(g_k)\, z^k \right.$$

soit

$$\Phi_G(z) == \frac{1}{G} \sum_{g \in G} \frac{1}{\det(Id - zg)}$$

en utilisant **II.A.4.c**.

II.B.1. Il suffit de démontrer que $\sigma_\mu(P_\mathcal{C}) = P_\mathcal{C}$ et $\sigma_\rho(P_\mathcal{C}) = P_\mathcal{C}$. On a $\dim \mathcal{C} = \frac{n}{2}$ et $\mathcal{C} = \mathcal{C}^\perp$. La formule de Mac Williams donne

$$2^{\frac{n}{2}} \times P_\mathcal{C}(X\ Y) = P_\mathcal{C}(Y - X\ X + Y)$$

d'où

$$\begin{aligned} P_\mathcal{C}(X\ Y) &= \frac{1}{2^{\frac{n}{2}}} \sum_{x \in \mathcal{C}} (Y - X)^{w(x)}\, (X + Y)^{n - w(x)} \\ &= \sum_{x \in \mathcal{C}} \left(\frac{1}{\sqrt{2}} (Y - X) \right)^{w(x)} \left(\frac{1}{\sqrt{2}} (X + Y) \right)^{n - w(x)} = \sigma_\mu(P_\mathcal{C})(X\ Y) \end{aligned}$$

c'est-à-dire $\sigma_\mu(P_\mathcal{C}) = P_\mathcal{C}$. Par ailleurs

$$\sigma_\rho(P_\mathcal{C})(X\ Y) = \sum_{x \in \mathcal{C}} (-X)^{w(x)}\, (Y)^{n - w(x)} = \sum_{x \in \mathcal{C}} X^{w(x)}\, (Y)^{n - w(x)} = P_\mathcal{C}(X\ Y)$$

puisque $w(x)$ est pair dès que $x \in \mathcal{C}$, et cela donne bien $\sigma_\rho(P_\mathcal{C}) = P_\mathcal{C}$.

II.B.2. ▶ On a

$$\mu = \begin{pmatrix} \cos\frac{3\pi}{4} & \sin\frac{3\pi}{4} \\ \sin\frac{3\pi}{4} & -\cos\frac{3\pi}{4} \end{pmatrix} \quad \text{et} \quad \rho = \begin{pmatrix} \cos\pi & \sin\pi \\ \sin\pi & -\cos\pi \end{pmatrix}$$

On reconnaît des matrices de réflexions du plan euclidien (que l'on supposera orienté). Plus précisément :

$$\begin{cases} \mu = \text{réflexion d'axe la droite d'angle polaire } \frac{3\pi}{8} \text{ (modulo } \pi), \\ \rho = \text{réflexion d'axe la droite d'angle polaire } \frac{\pi}{2} \text{ (modulo } \pi), \end{cases}$$

et l'on en déduit que $\rho\mu$ est la rotation d'angle $2 \times \left(\frac{\pi}{2} - \frac{3\pi}{8}\right) = \frac{\pi}{4}$ (modulo 2π). L'automorphisme $\rho\mu$ sera donc d'ordre 8 et $H = 8$.

▶ Comme $\rho^2 = Id = \mu^2$, les éléments de G seront soit Id, soit des produits de l'une des 4 forme suivante :

$$(\mathcal{L}) \qquad \mu\rho\mu\ \ \mu\rho\mu\ ; \quad \mu\rho\mu\ \ \rho\mu\rho\ ; \quad \rho\mu\rho\ \ \mu\rho\mu \text{ ou encore } \rho\mu\rho\ \ \rho\mu\rho.$$

Montrer que H est distingué dans G revient donc à montrer que $x\,(\rho\mu)^k\,x^{-1}$ H pour tout k 0 1 7 et pour tout x G. Puisque x est de l'une des quatre formes ci-dessus, cela revient à prouver les quatre assertions suivantes :

$$\begin{array}{lll} \rho\,(\rho\mu)^k\,\rho^{-1} & H & (1) \\ \rho\,(\rho\mu)^k\,\mu^{-1} & H & (2) \\ \mu\,(\rho\mu)^k\,\mu^{-1} & H & (3) \\ \mu\,(\rho\mu)^k\,\rho^{-1} & H & (4) \end{array}$$

La vérification est facile puisque $(\mu\rho)^{-1} = \rho^{-1}\mu^{-1} = \rho\mu$. Si $k = 0$, on écrit :

$$\begin{aligned} (1) \qquad \rho\,(\rho\mu)^k\,\rho^{-1} &= \rho\,(\rho\mu) \quad (\rho\mu)\,\rho^{-1} = \mu\,(\rho\mu) \quad (\rho\mu)\,\rho \\ &= (\mu\rho)^k = (\rho\mu)^{-k} \quad H \end{aligned}$$

$$\begin{aligned} (2) \qquad \rho\,(\rho\mu)^k\,\mu^{-1} &= \rho\,(\rho\mu) \quad (\rho\mu)\,\mu^{-1} = \mu\,(\rho\mu) \quad (\rho\mu)\,\rho \\ &= (\mu\rho)^{k-1} = (\rho\mu)^{-(k-1)} \quad H \end{aligned}$$

$$\begin{aligned} (3) \qquad \mu\,(\rho\mu)^k\,\mu^{-1} &= \mu\,(\rho\mu) \quad (\rho\mu)\,\mu^{-1} \\ &= (\mu\rho)^k = (\rho\mu)^{-k} \quad H \end{aligned}$$

$$\begin{aligned} (4) \qquad \mu\,(\rho\mu)^k\,\rho^{-1} &= \mu\,(\rho\mu) \quad (\rho\mu)\,\rho^{-1} \\ &= (\mu\rho)^{k+1} = (\rho\mu)^{-(k+1)} \quad H \end{aligned}$$

Si $k = 0$, on vérifie (1) à (4) en suivant la même méthode.

▶ Dans G H, on a $\overline{\rho\mu} = \overline{Id}$. Tous les éléments g de G sont listés en $(\mathcal{L})$ ci-dessus, si bien que les seules classes possibles dans G H soient $\overline{Id}$, $\overline{\rho}$, $\overline{\mu}$ ou $\overline{\mu\rho}$. Mais $\rho = (\rho\mu)\,\mu$ entraîne $\overline{\rho} = \overline{\mu}$; et l'on a $\overline{\mu\rho} = \overline{\mu\rho\mu\mu} = \overline{\mu^2} = \overline{Id}$. On peut donc conclure à

$$G\ H = \left\{\overline{Id}\ \overline{\rho}\right\} \text{ et } G\ H\ = 2$$

Finalement

$$G\ =\ G\ H\ \times\ H\ = 2 \times 8 = 16.$$

▶ Le groupe G est la réunion disjointe des classes $\overline{Id} = H$ et $\overline{\rho} = \rho H$, donc

$$G = \quad Id\ \ \rho\mu\ \ (\rho\mu)^2 \qquad (\rho\mu)^7\ \ \rho\ \ (\rho\mu)\,\rho\ \ (\rho\mu)^2\,\rho \qquad (\rho\mu)^7\,\rho$$

Comme $\rho\mu$ est la rotation d'angle $\frac{\pi}{4}$ et comme ρ est une réflexion laissant invariant l'octogone régulier, on peut affirmer que G est le groupe diédral $D\,(8)$ de l'octogone régulier.

II.B.3.a. On a

$$\begin{aligned}
&\left(X^2-1\right)\left(X^8-1\right)\\
&=(X-1)^2(X+1)^2\left(X-e^{i\frac{\pi}{4}}\right)\left(X-e^{-i\frac{\pi}{4}}\right)\\
&\qquad\qquad\times\left(X-e^{i\frac{\pi}{2}}\right)\left(X-e^{-i\frac{\pi}{2}}\right)\left(X-e^{i\frac{3\pi}{4}}\right)\left(X-e^{-i\frac{3\pi}{4}}\right)\\
&=(X-1)^2(X+1)^2\left(X-e^{i\frac{\pi}{4}}\right)\left(X-e^{-i\frac{\pi}{4}}\right)(X-i)(X+i)\left(X-e^{i\frac{3\pi}{4}}\right)\left(X-e^{-i\frac{3\pi}{4}}\right)\\
&=(X-1)^2(X+1)^2\left(X-e^{i\frac{\pi}{4}}\right)\left(X-e^{-i\frac{\pi}{4}}\right)(X-i)(X+i)\left(X-e^{i\frac{3\pi}{4}}\right)\left(X-e^{-i\frac{3\pi}{4}}\right)
\end{aligned}$$

On aura donc une décomposition en éléments simples de la forme suivante dans $\mathbb{C}$:

$$\begin{aligned}
f(X)&=\frac{1}{\left(X^2-1\right)\left(X^8-1\right)}\\
f(X)&=\frac{a}{X-1}+\frac{b}{(X-1)^2}+\frac{c}{X+1}+\frac{d}{(X+1)^2}+\frac{e}{X-e^{i\frac{\pi}{4}}}+\frac{\overline{e}}{X-e^{-i\frac{\pi}{4}}}\\
&\qquad+\frac{f}{X-i}+\frac{\overline{f}}{X+i}+\frac{g}{X-e^{i\frac{3\pi}{4}}}+\frac{\overline{g}}{X-e^{-i\frac{3\pi}{4}}}\quad(*)
\end{aligned}$$

Les coefficients a et b sont obtenus en posant $h=X-1$ et en divisant 1 par le polynôme

$$\begin{aligned}
A(h)&=(X+1)\left(X^7+X^6+X^5+X^4+X^3+X^2+X+1\right)\\
&=(h+2)\left((h+1)^7+(h+1)^6+(h+1)^5+(h+1)^4+(h+1)^3+(h+1)^2+(h+1)+1\right)\\
&=h^8+10h^7+44h^6+112h^5+182h^4+196h^3+140h^2+64h+16
\end{aligned}$$

suivant les puissances décroissantes de h, et à l'ordre 2. On trouve :

$$1=A(h)\times\left(\frac{1}{16}-\frac{1}{4}h\right)+h^2R(h)$$

d'où

$$f(X)=\frac{1}{h^2A(h)}=\frac{1}{16h^2}-\frac{1}{4h}+$$

et

$$a=-\frac{1}{4}\text{ et }b=\frac{1}{16}$$

Comme $f(X)$ est paire, l'unicité de la décomposition en éléments simples et la comparaison des décompositions de $f(X)$ et de $f(-X)$ montrent que $c=-a=\frac{1}{4}$ et $d=b=\frac{1}{16}$.
Posons $f(X)=\frac{1}{(X^2-1)(X^8-1)}=\frac{A(X)}{B(X)}$. On a

$$B\ (X)=2X\left(X^8-1\right)+8\left(X^2-1\right)X^7=10X^9-8X^7-2X$$

Avec ces notations, on sait que les coefficients correspondant aux pôles simples sont donnés par :

$$e = \frac{A\left(e^{i\frac{\pi}{4}}\right)}{B\ \left(e^{i\frac{\pi}{4}}\right)} = \frac{1}{8i\quad\overline{2}}$$
$$f = \frac{A\,(i)}{B\ (i)} = \frac{1}{16i}$$
$$g = \frac{A\left(e^{i\frac{3\pi}{4}}\right)}{B\ \left(e^{i\frac{3\pi}{4}}\right)} = \frac{1}{8i\quad\overline{2}}$$

Enfin on calcule

$$\begin{aligned}\frac{e}{X-e^{i\frac{\pi}{4}}}+\frac{\overline{e}}{X-e^{-i\frac{\pi}{4}}} &= \frac{1}{8i\quad\overline{2}}\left(\frac{1}{X-e^{i\frac{\pi}{4}}}-\frac{1}{X-e^{-i\frac{\pi}{4}}}\right)\\ &= \frac{1}{8i\quad\overline{2}}\frac{e^{i\frac{\pi}{4}}-e^{-i\frac{\pi}{4}}}{X^2-\quad\overline{2}X+1}\\ &= \frac{1}{8i\quad\overline{2}}\frac{2i\sin\frac{\pi}{4}}{X^2-\quad\overline{2}X+1} = \frac{1}{8}\frac{1}{X^2-\quad\overline{2}X+1}\end{aligned}$$

$$\frac{f}{X-i}+\frac{\overline{f}}{X+i} = \frac{1}{16i}\left(\frac{1}{X-i}-\frac{1}{X+i}\right) = \frac{1}{8}\frac{1}{X^2+1}$$

et

$$\frac{g}{X-e^{i\frac{3\pi}{4}}}+\frac{\overline{g}}{X-e^{-i\frac{3\pi}{4}}} = \frac{1}{8i\quad\overline{2}}\left(\frac{1}{X-e^{i\frac{3\pi}{4}}}-\frac{1}{X-e^{-i\frac{3\pi}{4}}}\right) = \frac{1}{8}\frac{1}{X^2+\quad\overline{2}X+1}$$

En conclusion, la décomposition de $f\,(X)$ en éléments simples dans $\mathbb{R}\,(X)$ sera :

$$\begin{aligned}\frac{1}{(X^2-1)\,(X^8-1)} = \frac{\frac{-1}{4}}{X-1}+\frac{\frac{1}{16}}{(X-1)^2}+\frac{\frac{1}{4}}{X+1}+\frac{\frac{1}{16}}{(X+1)^2}\\ +\frac{\frac{1}{8}}{X^2-\quad\overline{2}X+1}+\frac{\frac{1}{8}}{X^2+1}+\frac{\frac{1}{8}}{X^2+\quad\overline{2}X+1}\end{aligned}$$

II.B.3.b. Si g est une réflexion, sa matrice est semblable à $\begin{pmatrix}1&0\\0&-1\end{pmatrix}$ donc

$$\det\left(Id-zg\right) = (1-z)\,(1+z) = 1-z^2$$

Si g est une rotation d'angle θ, sa matrice est semblable à $\begin{pmatrix}\cos\theta&-\sin\theta\\\sin\theta&\cos\theta\end{pmatrix}$ et

$$\det\left(Id-zg\right) = (1-z\cos\theta)^2+z^2\sin^2\theta = z^2-2\cos\theta z+1$$

Les questions **II.A.4.d** et **II.B.2.** permettent d'écrire

$$\Phi_G(z) = \frac{1}{G} \sum_{g \in G} \frac{1}{\det(Id - zg)} = \frac{1}{16} \left(\frac{8}{1-z^2} + \sum_{k=0}^{7} \frac{1}{z^2 - 2\cos\frac{k\pi}{4} z + 1} \right)$$

$$= \frac{1}{16} \left(\frac{8}{1-z^2} + \sum_{k=0}^{7} \frac{1}{\left(z - e^{i\frac{k\pi}{4}}\right)\left(z - e^{-i\frac{k\pi}{4}}\right)} \right)$$

d'où

$$\Phi_G(z) = \frac{1}{2(1-z^2)} + \frac{1}{16}\left(\frac{1}{(z-1)^2} + \frac{2}{\left(z - e^{i\frac{\pi}{4}}\right)\left(z - e^{-i\frac{\pi}{4}}\right)}\right.$$
$$\left. + \frac{2}{\left(z - e^{i\frac{\pi}{2}}\right)\left(z - e^{-i\frac{\pi}{2}}\right)} + \frac{2}{\left(z - e^{i\frac{3\pi}{4}}\right)\left(z - e^{-i\frac{3\pi}{4}}\right)} + \frac{1}{(z+1)^2}\right)$$

Finalement

$$\Phi_G(z) = \frac{\frac{1}{4}}{1-z} + \frac{\frac{1}{4}}{1+z} + \frac{\frac{1}{16}}{(z-1)^2} + \frac{\frac{1}{8}}{z^2 - \sqrt{2}z + 1} + \frac{\frac{1}{8}}{z^2+1} + \frac{\frac{1}{8}}{z^2 + \sqrt{2}z + 1} + \frac{\frac{1}{16}}{(z+1)^2}$$
$$= \frac{1}{(1-z^2)(1-z^8)}$$

d'après **II.B.3.a.** Comme le rayon de convergence de chacune des séries $\frac{1}{\det(Id-zg)}$ est ≥ 1 d'après **II.A.4.a.**, on peut affirmer que l'égalité ci-dessus est vraie pour tout complexe z tel que $|z| < 1$.

II.B.4. Les question **II.A.4.** et **II.B.3.b** donnent

$$\Phi_G(z) = \sum_{k=0}^{+\infty} a_k(G) z^k = \frac{1}{(1-z^2)(1-z^8)} = \left(\sum_{i=0}^{+\infty} z^{2i}\right) \times \left(\sum_{j=0}^{+\infty} z^{8j}\right)$$

d'où

$$a_k(G) = \#\{(i\ j) \in \mathbb{N}\times\mathbb{N} \mid 2i + 8j = k\}$$

Bien entendu $a_k(G) = 0$ si k est impair. Si k est pair, chaque $j \in \mathbb{N}$ détermine un unique $i \in \mathbb{Z}$ tel que $2i + 8j = k$, et la condition $i \geq 0$ s'écrit $\frac{k}{2} - 4j \geq 0$, ou encore $j \leq \frac{k}{8}$. Il y aura donc ici $\left[\frac{k}{8}\right] + 1$ couples $(i\ j)$ solution dans $\mathbb{N}\times\mathbb{N}$.

II.B.5. ▶ D'après **I.B.2** et **I.B.3** les polynômes P_2 et Q_8 sont les polynômes des poids de deux codes auto-orthogonaux. La question **II.B.1** montre alors que P_2 et Q_8 appartiennent à A^G. On a donc $A \subset A^G$. Si l'on note A_k la composante homogène de A de degré k, on déduit $A_k \subset A_k^G$.

▶ A_k est engendré par la famille

$$\mathcal{F} = \left\{ P_2^i Q_8^j \right\}_{(i\ j)\ \in \mathbb{N}\times\mathbb{N} \text{ et } 2i+8j=k}$$

de cardinal $a_k(G)$ d'après **II.B.4**. Si l'on montre que cette famille est libre, on pourra écrire

$$a_k(G) \leq \dim A_k \leq a_k(G)$$

pour conclure à $\dim A_k = a_k(G)$ et à $A = A^G$.

▶ Raisonnons par l'absurde et supposons que la famille $\mathcal{F}$ soit liée. Il existe alors des coefficients $\lambda_{i\,j}$ non tous nuls tels que

$$\sum_{\substack{(i\,j)\ \mathbb{N}\times\mathbb{N} \\ 2i+8j=k}} \lambda_{i\,j} P_2^i Q_8^j = 0$$

Soit i_0 le plus petit entier tel qu'il existe j avec $\lambda_{i_0\,j} = 0$. Soit j_0 le plus petit entier tel que $\lambda_{i_0\,j_0} = 0$. Il existe un polynôme T $\mathbb{C}[X\ Y]$ tel que

$$P_2^{i_0}\left(\lambda_{i_0\,j_0} Q_8^{j_0} + P_2 T\right) = 0$$

Comme $\mathbb{C}[X\ Y]$ est intègre, on déduit $\lambda_{i_0\,j_0} Q_8^{j_0} + P_2 T = 0$ donc en particulier

$$\lambda_{i_0\,j_0} Q_8^{j_0}(1\ i) + P_2 T\ (1\ i) = 0$$

Mais alors $P_2(1\ i) = 0$ et $Q_8^{j_0}(1\ i) = 16$ entraînent $\lambda_{i_0\,j_0} = 0$, ce qui est absurde.

II.B.6. Si $\mathcal{C}$ est un code auto-orthogonal de $\mathcal{P}(\Omega)$, alors

$$P_{\mathcal{C}}(X\ Y) \quad A^G = \mathbb{C}[P_2\ Q_8]$$

d'après **II.B.1** et la question précédente. Comme $Q_8 = P_2^4 - 4\Delta$, on déduit $\mathbb{C}[P_2\ Q_8] = \mathbb{C}[P_2\ \Delta]$, donc

$$P_{\mathcal{C}}(X\ Y) \quad \mathbb{C}[P_2\ \Delta].$$

Comme $P_{\mathcal{C}}$, P_2 et Δ sont des polynômes homogènes de degrés respectifs , 2 et 8, il existera une famille $\lambda_{i\,j}$ $_{(i\,j)\ \mathbb{N}\times\mathbb{N}\text{ et }2i+8j=}$ de complexes telle que

$$P_{\mathcal{C}}(X\ Y) = \sum_{\substack{(i\,j)\ \mathbb{N}\times\mathbb{N} \\ 2i+8j=}} \lambda_{i\,j} P_2^i \Delta^j$$

Si l'on suppose par l'absurde que tous les coefficients $\lambda_{i\,j}$ n'appartiennent pas à $\mathbb{Z}$, notons j_0 le plus petit entier tel qu'il existe i avec $\lambda_{i\,j_0}$ $\mathbb{Z}$. Cet indice i est alors unique puisque vérifie $2i + 8j_0 =$ (où est pair par hypothèse). Notons i_0 l'indice tel que $\lambda_{i_0\,j_0}$ $\mathbb{Z}$. On a

$$\Delta^{j_0} \sum_{\substack{2i+8j= \\ j\geq j_0}} \lambda_{i\,j} P_2^i \Delta^{j-j_0} = P_{\mathcal{C}}(X\ Y) - \sum_{\substack{2i+8j= \\ j<j_0}} \lambda_{i\,j} P_2^i \Delta^j =: H(X\ Y) \quad \mathbb{Z}[X\ Y]$$

Comme Y^{2j_0} divise Δ^{j_0}, on déduit que Y^{2j_0} divise $H(X\ Y)$. Notons $H(X\ Y) = Y^{2j_0} H_1(X\ Y)$ où $H_1(X\ Y)$ $\mathbb{Z}[X\ Y]$. On aura

$$X^{2j_0} Y^{2j_0} \left(X^2 - Y^2\right)^{2j_0} \sum_{\substack{2i+8j= \\ j \geq j_0}} \lambda_{i\ j} P_2^i \Delta^{j-j_0} = Y^{2j_0} H_1(X\ Y)$$

soit

$$X^{2j_0} \left(X^2 - Y^2\right)^{2j_0} \sum_{\substack{2i+8j= \\ j \geq j_0}} \lambda_{i\ j} P_2^i \Delta^{j-j_0} = H_1(X\ Y)$$

Il suffit de remplacer $(X\ Y)$ par $(1\ 0)$ et de se rappeler que $\Delta = X^2 Y^2 \left(X^2 - Y^2\right)^2$ pour obtenir

$$\sum_{2i+8j_0=} \lambda_{i\ j} P_2^i (1\ 0) = H_1(1\ 0)$$

ou encore (puisque $P_2(X\ Y) = X^2 + Y^2$) $\lambda_{i_0\ j_0} = H_1(1\ 0)$ $\mathbb{Z}$, ce qui est contraire à l'hypothèse.

III.A.1. L'ensemble

$$L^0 = \{ v \in \mathbb{Q} \mid \forall w \in L,\ v\ w \in \mathbb{Z} \}$$

est clairement un sous-groupe additif de $\mathbb{Q}$. Soit $e = (e_1 \quad e\ )$ une $\mathbb{Z}$-base de L. Soit $e^* = (e_1^* \quad e^*)$ la base duale de e. Comme $\mathbb{Q}$ est un espace vectoriel euclidien, on peut identifier tout vecteur v de $\mathbb{Q}$ avec la forme linéaire $l_v : x \mapsto v\ x$. Soit e_i l'unique vecteur tel que $e_i^* = l_{e_i}$. Alors $(e_1 \quad e\ )$ est une base de $\mathbb{Q}$ et si $w = \sum_{i=1} w_i e_i$,

$$\left(\begin{array}{l} w \in \mathbb{Q} \quad v\ w = \sum_{i=1} w_i (v\ e_i) \qquad l_v = \sum_{i=1} (v\ e_i)\, e_i^* \\ \qquad\qquad\qquad\qquad\qquad\qquad l_v = \sum_{i=1} (v\ e_i)\, l_{e_i} \qquad v = \sum_{i=1} (v\ e_i)\, e_i \end{array} \right.$$

Pour pouvoir affirmer que L^0 est un réseau et que $(e_1 \quad e\ )$ est une $\mathbb{Z}$-base de L^0, il suffit maintenant d'écrire

$$v \in L^0 \quad i \quad v\ e_i \in \mathbb{Z} \quad v = \sum_{i=1} (v\ e_i)\, e_i \in \mathbb{Z} e_1 \oplus \quad \oplus \mathbb{Z} e$$

III.A.2.a. Notons d'abord que si e est une $\mathbb{Z}$-base de L, ou bien si $\det\left(P_e^e\right) = \pm 1$, alors e est une base de $\mathbb{Q}$ et $P = P_e^e$ représente la matrice de passage de e vers e . Si $x \in \mathbb{Q}$, on note $X = {}^t(x_1 \quad x\ )$ le vecteur-colonne des coordonnées de x dans e, et $X = {}^t(x_1 \quad x\ )$ celui des coordonnées de x dans e . Par hypothèse P est à coefficients dans $\mathbb{Z}$, et l'on sait que $X = PX$.

▶ Si e est une $\mathbb{Z}$-base de L, alors

$$X = {}^t(x_1 \quad x\ ) \quad \mathbb{Z} \quad X = P^{-1}X \quad \mathbb{Z}$$

donc P^{-1}est à coefficients dans $\mathbb{Z}$. Comme P et P^{-1} sont à coefficients dans $\mathbb{Z}$, leurs déterminants seront dans $\mathbb{Z}$ et

$$(\det P) \times \left(\det P^{-1}\right) = 1$$

entraîne $\det P = \pm 1$.

▶ Réciproquement, si $\det P = \pm 1$ alors P est inversible dans l'ensemble $\mathcal{M}\ (\mathbb{Z})$ des matrices carrée de taille et à coefficients entiers puisque

$$P^{-1} = \frac{1}{\det P}\,{}^t\mathrm{com}\,(P) \quad \mathcal{M}\ (\mathbb{Z})$$

et donc le système $X = PX$ se résout en $X = P^{-1}X$ avec $X \quad \mathbb{Z}$ dès que $X \quad \mathbb{Z}$. Cela montre l'inclusion

$$L \subset \mathbb{Z}e_1 + \quad + \mathbb{Z}e$$

L'inclusion réciproque est vraie puisque $X \quad \mathbb{Z}$ entraîne $X = PX \quad \mathbb{Z}$. En conclusion $L = \mathbb{Z}e_1 + \quad + \mathbb{Z}e$ et e est bien une $\mathbb{Z}$-base de L.

III.A.2.b. Soient v et v deux bases orthonormales de $\mathbb{Q}$, et e, e deux $\mathbb{Z}$-base de L. On a

$$P_v^e \times P_e^e \times P_e^v = P_v^v$$

Comme $\det\left(P_v^v\right) = \pm 1$ (P_v^v est une matrice orthogonale puisque c'est la matrice de passage d'une base orthonormale vers une autre base orthonormale) et $\det\left(P_e^e\right) = \pm 1$ (d'après **III.A.2.a**) on déduit

$$\det\left(P_v^e\right) \times \det\left(P_e^v\right) = \pm 1$$

d'où

$$\det\left(P_v^e\right) = \pm\ \det\left(P_e^v\right)^{-1} = \pm \det\left(\left(P_e^v\right)^{-1}\right) = \pm \det\left(P_v^e\right)$$

Finalement $\det\left(P_v^e\right) = \left|\det\left(P_v^e\right)\right|$.

III.A.2.c. Soit v une base orthonormale de $\mathbb{Q}$. Si e est une $\mathbb{Z}$-base de L, on a vu en **III.A.1** que $e = (e_1 \quad e\ )$ est une $\mathbb{Z}$-base de L^0. On conserve les notations des question **III.A.1** et **III.A.2.**, et l'on pose

$$P_v^e = A = (a_{ij}) \quad \text{et} \quad P_v^e = B = (b_{ij})$$

On a

$$e_j = \sum_{i=1} a_{ij} v_i \qquad e_j \, v_k = a_{kj}$$

et

$$e_j = \sum_{i=1} b_{ij} v_i \qquad e_j \, e_k = e_j^* \left(e_k \right) = \delta_{jk} = \sum_{i=1} b_{ij} v_i \, e_k = \sum_{i=1} b_{ij} a_{ik}$$

Cela montre que $I = {}^t BA$, ou encore $B = {}^t A^{-1}$.On en déduit immédiatement

$$\mathrm{Vol}\left(L \right) \mathrm{Vol}\left(L^0 \right) = \left(\det\left(A \right) \right) \left(\det\left(B \right) \right) = \left(\det\left(A \right) \right) \left(\det\left(A^{-1} \right) \right) = 1$$

III.A.3.a. Si d désigne le dénominateur commun de toutes les coordonnées des vecteurs e_1, ..., e_s dans la base canonique $(b_1 \quad b\ )$ de $\mathbb{Q}\ $, alors

$$i \quad de_i \quad \mathbb{Z}b_1 \oplus \quad \oplus \mathbb{Z}b$$

donc

$$M \subset L = \left(\mathbb{Z} \frac{b_1}{d} \right) \oplus \quad \oplus \left(\mathbb{Z} \frac{b}{d} \right)$$

où L est le réseau de $\mathbb{Z}$-base $\left(\frac{b_1}{d} \quad \frac{b}{d} \right)$.

III.A.3.b. $M \setminus L_1$ est un sous-groupe du groupe monogène $L_1 = \mathrm{Gr}\left(e_1 \right)$. C'est donc un groupe monogène engendré par un certain vecteur u_1. Si l'on suppose que $M \setminus L_k$ est engendré par k vecteurs u_1, ..., u_k de $\mathbb{Q}\ $, la projection

$$\begin{array}{rll} p: & M \setminus L_{k+1} & \mathbb{Z}e_{k+1} \\ & x_1 e_1 + \quad + x_{k+1} e_{k+1} & x_{k+1} e_{k+1} \end{array}$$

est un morphisme de groupes et l'image $p\left(M \setminus L_{k+1} \right)$ est un sous-groupe du groupe monogène $L_{k+1} = \mathrm{Gr}\left(e_{k+1} \right)$. Elle est donc engendrée par un vecteur u_{k+1}. Soit u_{k+1} $M \setminus L_{k+1}$ tel que $p\left(u_{k+1} \right) = u_{k+1}$. On a

$$M \setminus L_{k+1} = \left(M \setminus L_k \right) + \mathbb{Z}u_{k+1}$$

En effet, l'inclusion $M \setminus L_{k+1} \supset \left(M \setminus L_k \right) + \mathbb{Z}u_{k+1}$ est triviale. Réciproquement, tout élément $x = x_1 e_1 + \quad + x_{k+1} e_{k+1}$ de $M \setminus L_{k+1}$ vérifie $p\left(x \right) = x_{k+1} e_{k+1} = \lambda u_{k+1} = \lambda p\left(u_{k+1} \right)$ pour un entier λ convenable. Par suite $p\left(x - \lambda u_{k+1} \right) = 0$ et cela signifie que $x - \lambda u_{k+1} \quad M \setminus L_k$, ou encore $x \quad \left(M \setminus L_k \right) + \mathbb{Z}u_{k+1}$. L'hypothèse récurrente au rang k montre que $M \setminus L_k = \mathbb{Z}u_1 + \quad + \mathbb{Z}u_k$, d'où

$$M \setminus L_{k+1} = \mathbb{Z}u_1 + \quad + \mathbb{Z}u_k + \mathbb{Z}u_{k+1}$$

et la propriété est démontrée au rang $k+1$.

Au rang on aura

$$M = M \setminus L = \mathbb{Z}u_1 + \quad + \mathbb{Z}u$$

de sorte que M soit bien engendré par vecteurs.

III.A.3.c. Si M contient un réseau de $\mathbb{Q}$, alors M contient à fortiori une base $(e_1 \quad e\ )$ de $\mathbb{Q}$, et la question précédente permet d'écrire

$$\mathbb{Z}e_1 \oplus \quad \oplus \mathbb{Z}e \ \subset M = \mathbb{Z}u_1 + \quad + \mathbb{Z}u$$

d'où

$$= \dim \mathrm{Vect}\left(e_1 \quad e\ \right) \leq \dim \mathrm{Vect}\left(u_1 \quad u\ \right)$$

Nécessairement la système $(u_1 \quad u\ )$ sera libre dans $\mathbb{Q}$, et l'on aura

$$M = \mathbb{Z}u_1 \oplus \quad \oplus \mathbb{Z}u$$

ce qui signifie que M est un réseau de $\mathbb{Q}$.

III.A.4. ▶ Vérifions que Λ est un sous-groupe additif de $\mathbb{Q}$.
Si $v = \sum_{1\leq j\leq} \lambda_j w_j$ et $v = \sum_{1\leq j\leq} \lambda_j w_j$ vérifient (a) et (b), alors $v - v = \sum_{1\leq j\leq} \left(\lambda_j - \lambda_j\right) w_j$, les $\lambda_j - \lambda_j$ sont tous de même parité, et

$$\sum_{1\leq j\leq} \left(\lambda_j - \lambda_j\right) \equiv \sum_{1\leq j\leq} \lambda_j - \sum_{1\leq j\leq} \lambda_j \equiv 0 \ (4)$$

Donc $v - v \quad \Lambda$. Bien entendu, Λ n'est pas vide car contient le vecteur nul.

▶ Si tous les λ_j sont multiples de 4, notons $\lambda_j = 4\mu_j$. Alors (a) et (b) sont vérifiés et

$$v = \sum_{1\leq j\leq} \lambda_j w_j = \sum_{1\leq j\leq} \mu_j \left(4w_j\right) \quad \Lambda$$

de sorte que le sous-groupe Λ contienne le réseau $\mathbb{Z}\left(4w_1\right) \oplus \quad \oplus \mathbb{Z}\left(4w\ \right)$. La question **III.A.3** montre que Λ est un réseau.

▶ Montrons l'égalité $\Lambda^0 = \Lambda$. Posons $v = \sum_{1\leq j\leq} \lambda_j w_j$ et $v = \sum_{1\leq j\leq} \lambda_j w_j$. On a

$$\left(v \quad \Lambda^0\right) \qquad v \quad \Lambda \quad v \ v = \sum_{1\leq j\leq} \lambda_j w_j \sum_{1\leq j\leq} \lambda_j w_j = \frac{1}{4} \sum_{1\leq j\leq} \lambda_j \lambda_j \quad \mathbb{Z}$$

$$\lambda_1 \quad \lambda \quad \mathbb{Z} \text{ vérifiant } (a) \text{ et } (b), \quad \sum_{1\leq j\leq} \lambda_j \lambda_j \quad 4\mathbb{Z} \qquad (*)$$

• Supposons que $v \quad \Lambda^0$. Pour $\lambda_j = 2$, $\lambda_k = -2$ et $\lambda_s = 0$ dès que $s \quad j \ k$, $(*)$ s'écrit $\lambda_j - \lambda_k \quad 2\mathbb{Z}$, et les λ_j sont tous de même parité. Si l'on prend $\lambda_1 = \quad = \lambda \ = 3$ dans $(*)$, on trouve $3 \sum_{1\leq j\leq} \lambda_j \quad 4\mathbb{Z}$ d'où $\sum_{1\leq j\leq} \lambda_j \equiv 0 \ (4)$. On a donc montré que v satisfaisait (a) et (b), autrement dit $\Lambda^0 \subset \Lambda$.

• Réciproquement, si $v \quad \Lambda$ il faut vérifier $(*)$ pour pouvoir affirmer que $v \quad \Lambda^0$ et conclure à $\Lambda^0 = \Lambda$. Si les suites (λ_j) et $\left(\lambda_j\right)$ vérifient (a) et (b), il s'agit de prouver que

$$\lambda_j \lambda_j \quad 4\mathbb{Z} \qquad (**)$$
$$1 \leq j \leq$$

On envisage 4 cas suivant les parités des λ_j et des λ_j. Si les λ_j et les λ_j sont pairs, $(**)$ est trivial. Si les λ_j sont pairs et les λ_j impairs, on note $\lambda_j = 2\mu_j$ et $\lambda_j = 2\mu_j + 1$ et l'on obtient

$$\lambda_j \lambda_j = \left(2\mu_j\right)\left(2\mu_j + 1\right) \equiv \left(2\mu_j\right) \equiv \lambda_j \equiv 0 \ (4)$$
$$1 \leq j \leq \quad 1 \leq j \leq \quad 1 \leq j \leq \quad 1 \leq j \leq$$

d'après (b). Le cas où les λ_j sont impairs et les λ_j pairs se résout de la même façon. Enfin, si les λ_j et les λ_j sont impairs et avec des notations évidentes, on a

$$\lambda_j \lambda_j = \left(2\mu_j + 1\right)\left(2\mu_j + 1\right) \equiv \left(2\mu_j + 2\mu_j + 1\right)$$
$$1 \leq j \leq \quad 1 \leq j \leq \quad 1 \leq j \leq$$
$$\equiv \lambda_j + \lambda_j + \equiv 0 \ (4)$$
$$1 \leq j \leq \quad 1 \leq j \leq$$

puisque (λ_j) et $\left(\lambda_j\right)$ vérifient (a) et (b), et puisque est un multiple de 4.

III.A.5. Le ppcm d des dénominateurs des coordonnées de tous les vecteurs d'une $\mathbb{Z}$-base de L dans la base canonique vérifie $L \subset \frac{1}{d}\mathbb{Z}$. Pour tout $v \quad L$ on a donc $d^2 \quad v \ ^2 = (dv) \ (dv) \quad \mathbb{Z}$, d'où $d^2 \quad v \ ^2 \quad \mathbb{N}$. L'ensemble $m \quad \mathbb{N}^* \quad m \quad v \ ^2 \quad \mathbb{N}$ inclus dans $\mathbb{N}$ n'est donc pas vide et possède un plus petit élément d_L.

Si $v \quad L$ et $v \ ^2 = \frac{k}{d_L}$, écrivons $v = \frac{1}{d}\left(n_1 \quad n\right)$ dans la base canonique. On a

$$\frac{n_i^2}{d^2} = \frac{k}{d_L} \qquad n_i \ \leq d \quad \overline{\frac{k}{d_L}} \qquad n_i \ \leq \ d \quad \overline{\frac{k}{d_L}}$$
$$i=0$$

Posons $N = \ d \quad \overline{\frac{k}{d_L}}$. Les -uplets $(n_1 \quad n)$ appartiennent donc à l'hypercube $[-N \ N]$, et cela entraîne $c_k(L) \leq (2N+1)$, ou encore

$$c_k(L) \leq \left(2d \quad \overline{\frac{k}{d_L}} + 1\right.$$

Montrons que la série $\sum_{k=0}^{+} c_k(L) \ e^{ik\pi z}$ converge absolument quand $z = a + ib$ et $b > 0$. On a

$$\left|c_k(L) \ e^{ik\pi z}\right| = c_k(L) \ \left|e^{k\pi(ai-b)}\right| = c_k(L) \ e^{-bk\pi} \leq \left(2d \quad \overline{\frac{k}{d_L}} + 1 \qquad e^{-bk\pi}\right.$$

Il existe donc α $\mathbb{R}_+^*$ tel que $\left|c_k(L)\, e^{ik\pi z}\right| \leq \left(\alpha \quad \overline{k}+1\right) \; e^{-bk\pi}$, et il est facile de voir que

$$\left(\alpha \quad \overline{k}+1\right) \; e^{-bk\pi} = o\left(\frac{1}{k^2}\right)$$

lorsque k tend vers $+\quad$. En effet

$$\left(\alpha \quad \overline{k}+1\right) \; e^{-bk\pi} \sim \alpha \;\; k^{\overline{2}}\, e^{-bk\pi}$$

et $\lim\limits_{k \; +} \left(\alpha \;\; k^{\overline{2}} e^{-bk\pi}\right) = 0.$ la série à termes positifs $\sum\limits_{k=0}^{+} \left(\alpha \quad \overline{k}+1\right) \; e^{-bk\pi}$ convergera donc, et cela entraîne la convergence de $\sum\limits_{k=0}^{+} c_k(L)\, e^{ik\pi z}$ par comparaison.

III.B.1. Si $e = (e_1 \qquad e \;)$ désigne la base canonique, on pose

$$v_1 = \frac{1}{2}(e_1 - e_2) \;\; ; \quad v_2 = \frac{1}{2}(e_1 + e_2) \;\; ; \quad ; \quad v_{2i-1} = \frac{1}{2}(e_{2i-1} - e_{2i}) \;\; ; \quad v_{2i} = \frac{1}{2}(e_{2i-1} + e_{2i}) \;\; ;$$

On définit ainsi une base orthogonales qui satisfait $v_i \; v_i = \frac{1}{2}$

III.B.2.a. On a ${}^t\left(P_e^v\right) P_e^v = (c_{ij})$ où $c_{ij} = v_i \; v_j$, de sorte que

$${}^t\left(P_e^v\right) P_e^v = \mathrm{Diag}\left(v_1 \; v_1 \qquad v \quad v \;\right) \text{ et } \left(\det P_e^v\right)^2 = \prod_{j=1} \left(v_j \; v_j\right).$$

III.B.2.b. La question précédente et **III.A.2.b** donnent

$$(\mathrm{Vol}(R))^2 = (\det P_e^v)^2 = \prod_{j=1} (v_j \; v_j) = \frac{1}{2} \text{ et } (\mathrm{Vol}(R))^2 = \left(\det P_e^v\right)^2 = \prod_{j=1} \left(v_j \; v_j\right)$$

d'où

$$\prod_{j=1} \left(v_j \; v_j\right) = \frac{1}{2} \qquad (1)$$

Si l'on pose $v_j = \sum\limits_{j=1} a_{kj} v_k$ où $a_{kj} \quad \mathbb{Z}$, alors

$$v_j \; v_j = \frac{1}{2} \sum_{j=1} a_{kj}^2 \geq \frac{1}{2} \qquad (2)$$

(1) et (2) impliquent $v_j \; v_j = \frac{1}{2}$ pour tout j, donc $\sum\limits_{j=1} a_{kj}^2 = 1$ pour tout j, et cela montre que tous les entiers a_{kj} sont nuls un qui vaut ± 1. Comme v est une base, il existera nécessairement des entiers ${}_j$ $(1 \leq j \leq \;)$.valant ± 1 tels que

$$\left\{v_1 \qquad v \;\right\} = \quad {}_1 v_1 \qquad v$$

Par conséquent l'image de l'ensemble $v_1 \quad v$ par la surjection canonique de R sur $R\ 2R$ sera égale à celle de $v_1 \quad v$.

III.B.3. On a $\Omega = \overline{v}_1 \quad \overline{v} \subset R\ 2R$. L'application

$$\Psi : \begin{array}{c} \mathcal{P}(\Omega) \\ \overline{v}_{i_1} \quad \overline{v}_{i_m} \end{array} \longrightarrow \begin{array}{c} R\ 2R \\ \overline{v_{i_1} + \quad + v_i} \end{array}$$

est bien définie, est surjective. Elle est linéaire : on a en effet

$$\Psi(\ \overline{v}_{i_1} \quad \overline{v}_{i_m} + \overline{v}_{j_1} \quad \overline{v}_{j_t}\ ) = \overline{v_{i_1} + \quad + v_{i_m}} + \overline{v_{j_1} + \quad + v_{j_t}}$$

puisque les éléments qui disparaissent de la somme $\overline{v}_{i_1} \quad \overline{v}_{i_m} + \overline{v}_{j_1} \quad \overline{v}_{j_t}$ sont ceux qui appartiennent à la fois à $\overline{v}_{i_1} \quad \overline{v}_{i_m}$ et à $\overline{v}_{j_1} \quad \overline{v}_{j_t}$, et que les classes $\overline{v}$ correspondnat à ces éléments sont alors comptés 2 fois dans le membre de droite, et disparaissent de la somme puisque $\overline{v} + \overline{v} = \overline{0}$. On constate aussi

$$\begin{cases} \Psi\left(\overline{0} \quad \overline{v}_{i_1} \quad \overline{v}_{i_m}\ \right) = \Psi(\ ) = \overline{0} = \overline{0}\ \Psi(\ \overline{v}_{i_1} \quad \overline{v}_{i_m}\ ) \\ \Psi\left(\overline{1} \quad \overline{v}_{i_1} \quad \overline{v}_{i_m}\ \right) = \Psi(\ \overline{v}_{i_1} \quad \overline{v}_{i_m}\ ) = \overline{v_{i_1} + \quad + v_i} = \overline{1}\ \Psi(\ \overline{v}_{i_1} \quad \overline{v}_{i_m}\ ) \end{cases}$$

Ψ est injective car sont noyau est réduit à $\quad$ (c'est le vecteur nul de $\mathcal{P}(\Omega)$).
Les systèmes $(\ \overline{v}_1 \quad \overline{v}\ )$ et $(\overline{v}_1 \quad \overline{v}\ )$ sont des bases respectives de $\mathcal{P}(\Omega)$ et de $R\ 2R$, de sorte que montrer que α et β, bilinéaires, se correspondent via Ψ revient à montrer qu'elles se correspondent sur chacun des couples de vecteurs de la base $(\ \overline{v}_1 \quad \overline{v}\ )$. C'est évident puisque :

$$\alpha(\ \overline{v}_i \quad \overline{v}_j\ ) = \overline{\overline{v}_i \ \setminus \ \overline{v}_j} = \begin{cases} \overline{0} \text{ si } i = j \\ \overline{1} \text{ sinon.} \end{cases}$$

et

$$\beta(\Psi(\ \overline{v}_i\ )\ \ \Psi(\ \overline{v}_j\ )) = \overline{\overline{2v_i}\ v_j} = \begin{cases} \overline{0} \text{ si } i = j \\ \overline{1} \text{ sinon.} \end{cases}$$

III.B.4.a. On a

$$R \quad \overset{\pi}{\longrightarrow} \quad \begin{array}{c} R\ 2R \\ \overline{v_{i_1} + \quad + v_{i_m}} \end{array} \quad \overset{\Psi}{\underset{\sim}{\longrightarrow}} \quad \begin{array}{c} \mathcal{P}(\Omega) \\ \overline{v}_{i_1} \quad \overline{v}_{i_m} \end{array}$$

et plusieurs façons d'écrire $L(\mathcal{C})$:

$$L(\mathcal{C}) = \pi^{-1}(\mathcal{C}) = \quad v \quad R \quad x = \overline{v}_{i_1} \quad \overline{v}_{i_m} \quad \mathcal{P}(\Omega) \quad \overline{v} = \overline{v_{i_1} + \quad + v_{i_m}}$$

$$= \quad v \quad R \quad x = \overline{v}_{i_1} \quad \overline{v}_{i_m} \quad \mathcal{P}(\Omega) \quad \mu_i \quad \mathbb{Z} \quad v - (v_{i_1} + \quad + v_{i_m}) = \sum_{i=1} 2\mu_i v_i \quad (1)$$

$$= \quad v \quad R \quad x = \overline{v}_{i_1} \quad \overline{v}_{i_m} \quad \mathcal{P}(\Omega) \quad \mu_i \quad \mathbb{Z} \quad v - (v_{i_1} + \quad + v_{i_m}) \quad 2R$$

$$= \quad v \quad R \quad x = \overline{v}_{i_1} \quad \overline{v}_{i_m} \quad \mathcal{P}(\Omega)\ v = \sum_{i=1} \lambda_i v_i \text{ et } \lambda_i \text{ impair ssi } i \quad i_1 \quad i_m \quad (2)$$

En prenant $x =$ dans (2), on constate que $2R \subset L(\mathcal{C}) \subset R$. L'ensemble $L(\mathcal{C})$ est un sous-groupe de R comme image réciproque du groupe additif $\mathcal{C}$ par π. L'écriture (1) montre, par ailleurs, que le groupe $L(\mathcal{C})$ est engendré par la famille $2v_1 \quad 2v \quad v_{i_1} + \quad + v_{i_m} \quad i_1 \quad i_m \subset \mathbb{N}$. La question **III.A.3** prouve alors que $L(\mathcal{C})$ est un réseau.

III.B.4.b. ▶ Pour montrer l'égalité $(2R)^0 = R$ on peut supposer, sans restreindre la généralité, que $(v_1 \quad v\ )$ est choisie comme en **III.B.1**. Alors

$$\begin{aligned}(2R)^0 = \ & v \quad \mathbb{Q} \quad w \quad 2R \quad v\ w \quad \mathbb{Z} \\ = \ & v = \sum_{i=1} \lambda_i v_i \quad \mathbb{Q} \quad w = \sum_{i=1} 2\mu_i v_i \quad 2R \quad \sum_{i=1} \lambda_i \mu_i \quad \mathbb{Z} \\ = \ & v = \sum_{i=1} \lambda_i v_i \quad \mathbb{Q} \quad \lambda_i \quad \mathbb{Z} \quad = R\end{aligned}$$

▶ L'inclusion $2R \subset L(\mathcal{C})$ entraîne $L(\mathcal{C})^0 \subset (2R)^0 = R$. Donc

$$\begin{aligned}L(\mathcal{C})^0 = \ & v \quad R \quad w \quad L(\mathcal{C}) \quad v\ w \quad \mathbb{Z} \\ = \ & v \quad R \quad w \quad L(\mathcal{C}) \quad 2(v\ w) \quad 2\mathbb{Z} \\ = \ & \left\{v \quad R \quad \overline{w} \quad \mathcal{C} \quad \beta(\overline{v}\ \overline{w}) = \overline{2v\ w} = \overline{0}\right\} = L\left(\mathcal{C}^0\right)\end{aligned}$$

III.B.4.c. Comme $\pi : R \quad R$ $2R$ est surjective, $\pi(L(\mathcal{C})) = \pi\left(\pi^{-1}(\mathcal{C})\right) = \mathcal{C}$ et l'image $(\overline{u}_1 \quad \overline{u}\ )$ de $(u_1 \quad u\ )$ engendrera l'espace vectoriel $\mathcal{C}$. Si $j \geq d+1$ alors $\overline{u}_j$ sera combinaison linéaire de $\overline{u}_1 \quad \overline{u}_d$, disons $\overline{u}_j = \sum_{i=1}^{d} {}_i\overline{u}_i$, donc

$$u_j - \sum_{i=1}^{d} {}_i u_i \quad 2R$$

Il suffit de poser $x_j = \sum_{i=1}^{d} {}_i u_i \quad X$ pour obtenir $u_j = u_j - x_j \quad 2R$.

III.B.4.d. ▶ Le système $\left(u_1 \quad u_d\ u_{d+1} \quad u\ \right)$ est une base de $\mathbb{Q}$ et engendre $L(\mathcal{C})$ (puisque $(u_1 \quad u\ )$ une $\mathbb{Z}$-base de $L(\mathcal{C})$), donc est une $\mathbb{Z}$-base de $L(\mathcal{C})$.

▶ On a vu que $2R \subset L(\mathcal{C})$ en **III.B.4.b** , de sorte que tout $v \quad 2R$ s'écrive sous la forme

$$v = \sum_{i=1}^{d} \lambda_i u_i + \sum_{i=d+1} \lambda_i u_i$$

Cela entraîne $\overline{0} = \sum_{i=1}^{d} \overline{\lambda}_i \overline{u}_i$, donc $\overline{\lambda}_1 = \quad = \overline{\lambda}_d = 0$ (puisque $(\overline{u}_1 \quad \overline{u}_d)$ est une base). Par conséquent v s'écrira

$$v = \sum_{i=1}^{d} \mu_i (2u_i) + \sum_{i=d+1} \lambda_i u_i \text{ avec } \mu_i\ \lambda_i \quad \mathbb{Z}$$

et cela prouve que le système $\left(2u_1 \quad 2u_d \ u_{d+1} \quad u \ \right)$ engendre le groupe $2R$. Comme ce système est clairement une base de $\mathbb{Q}$, on peut affirmer que c'est une $\mathbb{Z}$-base de $2R$.

▶ Si e désigne la base canonique de $\mathbb{Q}$, ce qui précède entraîne par définition :

$$\begin{aligned}\mathrm{Vol}\,(2R) &= \left|\det_e\left(2u_1 \quad 2u_d \ u_{d+1} \quad u \ \right)\right| \\ &= 2^d\left|\det_e\left(u_1 \quad u_d \ u_{d+1} \quad u \ \right)\right| = 2^d\,\mathrm{Vol}\,(R) \qquad (*)\end{aligned}$$

Mais $\mathrm{Vol}\,(2R) = 2 \ \mathrm{Vol}\,(R)$, et **III.B.2.b** donne $\mathrm{Vol}\,(R) = 2^{-\overline{2}}$. En reportant dans $(*)$, on obtient bien

$$\mathrm{Vol}\,(L\,(\mathcal{C})) = 2^{\overline{2}-\dim(\mathcal{C})}$$

III.B.5.a. Posons $z = a + ib$ où $b > 0$. Alors

$$\left|e^{i2\pi\left(k+\frac{1}{2}\right)^2 z}\right| = e^{-b2\pi\left(k+\frac{1}{2}\right)^2} = o\left(\frac{1}{k^2}\right) \text{ et } \left|e^{i2\pi k^2 z}\right| = e^{-b2\pi k^2} = o\left(\frac{1}{k^2}\right)$$

prouve que les deux séries $\overset{+}{\underset{k=0}{}} e^{i2\pi\left(k+\frac{1}{2}\right)^2 z}$ et $\overset{+}{\underset{k=0}{}} e^{i2\pi k^2 z}$ sont absolument convergentes lorsque z est fixé tel que $\mathrm{Im}\,(z) > 0$.

III.B.5.b. On a

$$P_{\mathcal{C}}\left(\ {}_2(z) \quad {}_3(z)\right) = \underset{x \ \mathcal{C}}{} \left(\ {}_2(z)\right)^{x} \left(\ {}_3(z)\right)^{-x}$$

$$= \underset{x \ \mathcal{C}}{} \underset{\substack{m \text{ impair} \\ m \ \mathbb{Z}}}{} e^{i\pi\frac{m^2}{2}z}{}^{x} \underset{\substack{m \text{ pair} \\ m \ \mathbb{Z}}}{} e^{i\pi\frac{m^2}{2}z}{}^{-x} = \overset{+}{\underset{h=0}{}} v_h e^{i\pi\frac{h}{2}z}$$

où

$$v_h = \underset{x \ \mathcal{C}}{} \left|\left\{\left(m_1 \quad m_{\ x} \ n_1 \quad n_{\ -x}\right) \quad \mathbb{Z} \quad \left\{\begin{array}{l} m_j \text{ impair et } n_j \text{ pair,} \\ m_1^2 + \quad + m_{\ x}^2 + n_1^2 + \quad + n_{\ -x}^2 = h \end{array}\right\}\right|$$

III.B.5.c. On a bien

$$\theta_{L(\mathcal{C})}\,(z) = \underset{v \ L(\mathcal{C})}{} e^{i\pi(v\ v)z} = \overset{+}{\underset{h=0}{}} d_h e^{i\pi\frac{h}{2}z} \text{ où } d_h = \left|\left\{v \quad L\,(\mathcal{C}) \quad v\ v = \frac{h}{2}\right\}\right|$$

III.B.5.d. Comme $L\,(\mathcal{C}) \subset R$ tout $v \quad L\,(\mathcal{C})$ s'écrit $v = \underset{j=1}{} \lambda_j v_j \quad \mathbb{Z}$. Posons $x = \ \overline{v}_{i_1} \quad \overline{v}_{i_m}$ identifié à $\overline{v_{i_1} + \quad + v_{i_m}}$ par l'isomorphisme $\Psi : R \ 2R \quad \mathcal{P}\,(\Omega)$. On a

	$v = \underset{j=1}{} \lambda_j v_j$	$v = \underset{j=1}{} \lambda_j v_j$
$v \quad \Lambda_{h\,x}$	$\overline{v} = \underset{j=1}{} \overline{\lambda}_j \overline{v}_j = x = \overline{v_{i_1} + \quad + v_{i_m}}$	λ_j est $\left\{\begin{array}{l} \text{impair si } j \quad i_1 \quad i_m \\ \text{pair sinon.} \end{array}\right.$
	$v\ v = \frac{1}{2} \underset{j=1}{} \lambda_j^2 = \frac{h}{2}$	$\underset{j=1}{} \lambda_j^2 = h$

donc

$$\Lambda_{h\,x} = \left| \quad (\lambda_1 \qquad \lambda \ ) \quad \mathbb{Z} \quad \lambda_j \text{ est } \begin{cases} \text{impair si } j & i_1 \qquad i_m \\ \text{pair sinon.} \end{cases} \text{, et } \sum_{j=1} \lambda_j^2 = h \quad \right|$$

$$= v_h$$

En conclusion

$$d_h = \Lambda_h = \sum_{x \ \mathcal{C}} \Lambda_{h\,x} = v_h \quad \text{et} \quad P_{\mathcal{C}}\left(\ {}_2(z) \quad {}_3(z)\right) = \theta_{L(\mathcal{C})}(z)$$