

Problème d'agrégation de 1978 : Codes, polynôme des poids, identité de Mac Williams et réseaux.

Dany-Jack Mercier

IUFM de Guadeloupe, Morne Ferret,
BP399, Pointe-à-Pitre cedex 97159, France
dany-jack.mercier@univ-ag.fr

5 janvier 2002

Je voudrais ici partager un travail que j'ai effectué sur la composition de Mathématiques Générales de l'agrégation externe 1978. La Section 1 présente l'énoncé d'un problème très voisin de celui qui a été effectivement donné en 1978 puisque seulement les deux questions originelles III.B.5 et III.B.6 de la dernière partie, que je considère comme purement techniques et assez gratuites, ont été supprimées. J'ai aussi fractionné et détaillé un certain nombre d'autres questions, jugées trop abruptes, dans le but de rendre le problème plus abordable et formateur. La solution proposée à la Section 2 est personnelle.

1 Énoncé du problème

Dans tout le problème, n désigne un entier pair strictement positif, Ω représente un ensemble de cardinal n , et $\mathcal{P}(\Omega)$ représente l'ensemble des parties de Ω . Le cardinal d'un ensemble fini E est noté $|E|$, et la classe d'un entier n modulo 2 est noté \bar{n} . La notation $\mathbb{Z}[X, Y]$ représente l'anneau des polynômes à deux indéterminées et à coefficients dans \mathbb{Z} . Si $m \in \mathbb{N}^*$, la notation \mathbb{N}_m représente l'ensemble $\{1, 2, \dots, m\}$.

Les notations et certains résultats de la partie I seront utilisés dans les parties II.B et III.B. Les parties II et III sont indépendantes l'une de l'autre.

Partie I

I.A. Généralités

I.A.1. Vérifier que $\mathcal{P}(\Omega)$ muni de la loi "différence symétrique" définie par

$$(x \ominus y) = x + y = (x \cup y) \setminus (x \cap y)$$

est un groupe abélien.

⁰[ucod0005] v1.02 <http://perso.wanadoo.fr/megamaths>
© 2002, D.-J. Mercier. Vous pouvez faire une copie de ces notes pour votre usage personnel.

I.A.2. Démontrer que $\mathcal{P}(\Omega)$ peut être muni d'une structure d'espace vectoriel sur le corps à deux éléments $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z} = \{\bar{0}, \bar{1}\}$ pour la loi $+$ définie en **I.A.1**. Grâce à quelle propriété particulière de cette loi de groupe cela est-il possible ?

I.A.3. Quelle est la dimension de $\mathcal{P}(\Omega)$? Donner une base de cet espace.

I.A.4. Vérifier que l'application α de $\mathcal{P}(\Omega) \times \mathcal{P}(\Omega)$ dans \mathbb{F}_2 définie par

$$\alpha(x, y) = \overline{x \setminus y}$$

est une forme bilinéaire symétrique non dégénérée sur $\mathcal{P}(\Omega)$. Cette forme bilinéaire sera appelée "forme bilinéaire naturelle sur $\mathcal{P}(\Omega)$ ".

I.A.5. Soient $\mathcal{D}(\Omega)$ la droite vectorielle de $\mathcal{P}(\Omega)$ engendrée par Ω , et $\mathcal{H}(\Omega) = \mathcal{D}(\Omega)^\perp$ l'orthogonal de $\mathcal{D}(\Omega)$ pour la forme bilinéaire α . Décrire $\mathcal{H}(\Omega)$, et retrouver ainsi la formule

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

Quel est le noyau de la restriction de la forme bilinéaire naturelle à $\mathcal{H}(\Omega)$?

I.B. Codes et Polynômes des Poids

Les sous-espaces vectoriels de $\mathcal{P}(\Omega)$ sont appelés les codes de $\mathcal{P}(\Omega)$. Si \mathcal{C} est un code de $\mathcal{P}(\Omega)$, on désigne par \mathcal{C}^\perp son orthogonal. Pour toute permutation s de Ω , on désigne par \bar{s} l'endomorphisme de $\mathcal{P}(\Omega)$ définie par

$$\bar{s}(x) = s(x)$$

On dit que deux codes \mathcal{C} et \mathcal{C}' de $\mathcal{P}(\Omega)$ sont isomorphes s'il existe une permutation s de Ω telle que $\bar{s}(\mathcal{C}) = \mathcal{C}'$.

I.B.1. Un code \mathcal{C} est dit auto-orthogonal si $\mathcal{C} = \mathcal{C}^\perp$. Quelle est la dimension d'un code auto-orthogonal ? Démontrer que si \mathcal{C} est auto-orthogonal on a $\mathcal{D}(\Omega) \subset \mathcal{C} \subset \mathcal{H}(\Omega)$.

Soit \mathcal{C} un code de $\mathcal{P}(\Omega)$. On appelle polynôme des poids de \mathcal{C} et on note $P_{\mathcal{C}}(X, Y)$ l'élément de $\mathbb{Z}[X, Y]$ défini par

$$P_{\mathcal{C}}(X, Y) = \sum_{x \in \mathcal{C}} X^{|x|} Y^{|\Omega| - |x|}$$

I.B.2. On pose $n = 2m$ et $\Omega = \{t_1, t_2, \dots, t_m, u_1, u_2, \dots, u_m\}$. Construire un code auto-orthogonal dont le polynôme des poids est $P(X, Y) = (X^2 + Y^2)^m$. Soit $\Gamma(\Omega)$ l'ensemble des codes auto-orthogonaux dont le polynôme des poids est $P(X, Y)$. Démontrer que deux éléments quelconques de $\Gamma(\Omega)$ sont isomorphes.

I.B.3. Dans cette question, on suppose que $n = 2m$ est un multiple de 4 et l'on note toujours

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

On définit le code \mathcal{B} engendré par

$$t_1 t_2 \dots t_m \quad u_1 u_2 \dots u_m \quad \text{et} \quad t_h t_j u_h u_j \quad \text{avec} \quad h = j \quad \text{et} \quad (h, j) \in \mathbb{N}_m^2$$

I.B.3.a. On pose $x = t_1 t_2 \dots t_m$ et pour tout $2 \leq h \leq m$, $y_h = t_1 t_h u_1 u_h$. Démontrer que la famille $(x, y_h)_{1 \leq h \leq m}$ est libre, puis que \mathcal{B} est un code auto-orthogonal. En déduire que $(x, y_h)_{1 \leq h \leq m}$ est une base de \mathcal{B} .

I.B.3.b. Si μ est une partie non vide de \mathbb{N}_m , on pose

$$\begin{cases} x_\mu = \prod_{h \in \mu} t_h & y_\mu = \prod_{h \in \mu} u_h \\ y_\mu = \prod_{h \in \mu} t_h & x_\mu = \prod_{h \in \mu} u_h \end{cases}$$

On pose aussi $x = y = 1$. On note \mathcal{B} la partie de $\mathcal{P}(\Omega)$ définie par

$$\mathcal{B} = \{x_\mu \mid \mu \subset \mathbb{N}_m \text{ et } |\mu| \text{ pair}\} \cup \{y_\mu \mid \mu \subset \mathbb{N}_m \text{ et } |\mu| \text{ pair}\}$$

On admet les relations suivantes

$$x_\mu = \prod_{h=1}^m t_h \quad \text{et} \quad y_\mu = \prod_{h=1}^m u_h + x_{\mathbb{N}_m \setminus \mu}$$

qui prouvent l'inclusion $\mathcal{B} \subset \mathcal{B}$. Démontrer que si $\mu \subset \mathbb{N}_m$ et $\nu \subset \mathbb{N}_m$, alors $\overline{\mu + \nu} = \overline{\mu} + \overline{\nu}$ et $\overline{\mu + \nu} = \overline{\mu} + \overline{\nu}$. Démontrer ensuite que \mathcal{B} est un sous-espace vectoriel de $\mathcal{P}(\Omega)$, puis déduire l'égalité $\mathcal{B} = \mathcal{B}$.

I.B.3.c. Déduire des questions précédentes que le polynôme des poids de \mathcal{B} est

$$Q(X, Y) = \frac{1}{2} \left((X^2 + Y^2)^m + (X^2 - Y^2)^m + (2XY)^m \right)$$

I.B.3.d. On dit qu'un code auto-orthogonal est pair si les cardinaux de tous ses éléments sont multiples de 4. Vérifier que le code \mathcal{B} défini ci-dessus est pair dès que m est multiple de 8.

I.B.3.e. Si $m = 16$, on se propose de construire un code \mathcal{B}_{16} non isomorphe à \mathcal{B}_{16} et dont le polynôme des poids est $Q_{16}(X, Y)$. On remarque que $(Q_8(X, Y))^2 = Q_{16}(X, Y)$. Si

$$\Omega = t_1 t_2 \dots t_8 u_1 u_2 \dots u_8$$

on note $\Omega = t_1 t_2 t_3 t_4 u_1 u_2 u_3 u_4$ et $\Omega = t_5 t_6 t_7 t_8 u_5 u_6 u_7 u_8$. Soit \mathcal{C} (resp. \mathcal{C}) un code de Ω (resp. Ω) du même type que \mathcal{B}_8 . On construit le code

$$\mathcal{B}_{16} = \mathcal{C} + \mathcal{C} = \{x + x \mid x \in \mathcal{C} \text{ et } x \in \mathcal{C}\}$$

de $\mathcal{P}(\Omega)$. Calculer le polynôme des poids Q_{16} de \mathcal{B}_{16} . On pose

$$\begin{aligned} x &= t_1 t_2 t_3 t_4 \\ \mathcal{E} &= \{y \in \mathcal{B}_{16} \mid |y| = 4 \text{ et } |x \setminus y| = 2\} \\ \mathcal{E} &= \{y \in \mathcal{B}_{16} \mid |y| = 4 \text{ et } |x \setminus y| = 2\} \end{aligned}$$

Montrer que $\sum_{y \in \mathcal{E}} y = \Omega$, puis que $\sum_{y \in \mathcal{E}} y = \Omega$. On admettra que ces égalités sont encore vraies si l'on remplace $x = t_1 t_2 t_3 t_4$ par n'importe quelle partie x de cardinal 4 de Ω et si l'on prend soin de conclure à $\sum_{y \in \mathcal{E}} y = \Omega$ ou à $\sum_{y \in \mathcal{E}} y = \Omega$ cette fois-ci. Expliquer brièvement pourquoi \mathcal{B}_{16} et \mathcal{B}'_{16} ne sont pas isomorphes.

I.B.4. Soit \mathcal{C} un code de $\mathcal{P}(\Omega)$. On se propose de démontrer l'identité de Mac Williams (1963) :

$$2^{\dim \mathcal{C}} \times P_{\mathcal{C}}(X, Y) = P_{\mathcal{C}}(Y - X, X + Y) \quad (\text{MW})$$

I.B.4.a. Soit $f : \mathcal{P}(\Omega) \rightarrow M$ une application à valeurs dans un groupe abélien M dont la loi est notée additivement. On pose $(-1)^{\overline{0}} = 1$ et $(-1)^{\overline{1}} = -1$, et l'on note $f : \mathcal{P}(\Omega) \rightarrow M$ la fonction définie par

$$f(x) = \sum_{y \in \mathcal{P}(\Omega)} (-1)^{\alpha(x, y)} f(y)$$

Démontrer que pour tout code \mathcal{C} de $\mathcal{P}(\Omega)$, on a

$$\sum_{x \in \mathcal{C}} f(x) = 2^{\dim \mathcal{C}} \sum_{y \in \mathcal{C}} f(y)$$

I.B.4.b. Ecrire la formule de la question précédente avec $M = \mathbb{Z}[X, Y]$ et

$$f : \mathcal{P}(\Omega) \rightarrow \mathbb{Z}[X, Y] \\ x \mapsto X^x Y^{-x}$$

Montrer ensuite que l'identité de Mac Williams sera bien démontrée si l'on prouve que

$$f(x) = (Y - X)^x (X + Y)^{-x}$$

pour tout $x \in \mathcal{C}$. Démontrer cette dernière formule (Indication : Dans l'expression sommatoire donnant f , on pourra écrire toute partie y de $\mathcal{P}(\Omega)$ sous la forme $y = y_1 + y_2$ avec $y_1 \subset x$ et $y_2 \subset \Omega \setminus x$).

Partie II

II.A. Invariants d'un groupe fini

Soit V un espace vectoriel de dimension finie $n \geq 1$ sur le corps des complexes \mathbb{C} . Si g est un endomorphisme de V , on note $\text{Tr}(g)$ sa trace. On note Id l'endomorphisme identité sur V , $\text{Aut}(V)$ le groupe des automorphismes de V , et G un sous-groupe fini de $\text{Aut}(V)$.

II.A.1. Soit V^G le sous-espace vectoriel de V formé des vecteurs v tels que $g(v) = v$ pour tout $g \in G$. Soit p_G l'endomorphisme de V défini par

$$p_G = \frac{1}{|G|} \sum_{g \in G} g$$

II.A.1.a. Montrer que $\text{Im}(p_G) = V^G$ et que p_G est un projecteur de V .

II.A.1.b. En déduire la formule

$$\dim(V^G) = \frac{1}{|G|} \sum_{g \in G} \text{Tr}(g)$$

II.A.1.c. Si G est un groupe fini quelconque et si $\rho : G \rightarrow \text{Aut}(V)$ est un morphisme de groupes, on pose

$$V^G = \{v \in V \mid \rho(g)(v) = v \text{ pour tout } g \in G\}$$

Démontrer la formule plus générale

$$\dim(V^G) = \frac{1}{|G|} \sum_{g \in G} \text{Tr}(\rho(g))$$

II.A.2. On choisit une base $e = (e_1, \dots, e_n)$ de V , et l'on note A l'algèbre $\mathbb{C}[X_1, \dots, X_n]$ des polynômes d'indéterminées X_1, \dots, X_n et à coefficients dans \mathbb{C} . À tout élément g de $\text{Aut}(V)$ on associe l'application $\sigma_g : A \rightarrow A$ définie de la manière suivante :

Si $g(e_h) = \sum_{j=1}^n \gamma_{jh} e_j$ pour tout $h \in \{1, \dots, n\}$, et si $P(X_1, \dots, X_n) \in A$, alors

$$\sigma_g(P)(X_1, \dots, X_n) = P\left(\sum_{j=1}^n \gamma_{j1} X_j, \dots, \sum_{j=1}^n \gamma_{jn} X_j\right)$$

II.A.2.a. Montrer que σ_g est un automorphisme de l'algèbre A , et que l'application

$$\Psi : \text{Aut}(A) \rightarrow \text{Aut}(A)$$

$$g \mapsto \sigma_g$$

est un homomorphisme de groupes.

II.A.2.b. Soit A_k ($k \in \mathbb{N}$) le sous-espace vectoriel de A formé des polynômes homogènes de degré k . Quelle est la dimension a_k de A_k ? Vérifier que $\sigma_g(A_k) = A_k$ pour tout g appartenant à $\text{Aut}(A)$.

On notera $g_k = \sigma_g|_{A_k}$ la restriction de σ_g à A_k , et l'on dira que g_k est l'automorphisme de A_k définie par g .

II.A.3. On pose $A_k^G = \sum_{g \in G} \sigma_g(P) = P$ et $a_k(G) = \dim(A_k^G)$. Démontrer que les séries entières $\sum_{k=0}^{\infty} a_k z^k$ et $\sum_{k=0}^{\infty} a_k(G) z^k$ ont des rayons de convergence strictement positifs.

II.A.4. Soit $g \in G$. On pose

$$\Phi_G(z) = \sum_{k=0}^{\infty} a_k(G) z^k \quad \text{et} \quad \frac{1}{\det(\text{Id} - zg)} = \sum_{k=0}^{\infty} r_k z^k.$$

II.A.4.a. Montrer que la série $\sum_{k=0}^{\infty} r_k z^k$ possède un rayon de convergence ≥ 1 .

II.A.4.b. On suppose que la matrice de g dans la base e est diagonale et on la note $\text{diag}(\alpha_1 \dots \alpha_n)$. Exprimer r_k en fonction des complexes $\alpha_1 \dots \alpha_n$ et de l'entier k . En déduire l'égalité $\text{Tr}(g_k) = r_k$.

II.A.4.c. On se place maintenant dans le cas général où $g \in G$. Montrer que g est diagonalisable, et en déduire l'égalité $\text{Tr}(g_k) = r_k$.

II.A.4.d. Utiliser les questions **II.A.1.c.** et **II.A.4.c.** pour montrer l'égalité

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

pour tout z tel que $|z| < 1$.

II.B. Algèbre associée aux polynômes des poids

On utilise les notations, définitions et résultats des parties I.A, I.B et II.A. On note G le groupe des matrices engendrées par

$$\mu = \frac{1}{2} \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix} \quad \text{et} \quad \rho = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

Si $P(X, Y) \in \mathbb{C}[X, Y]$ et si $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$, on rappelle que (cf. II.A) :

$$\sigma_g(P)(X, Y) = P(aX + cY, bX + dY)$$

II.B.1. Soit \mathcal{C} un code auto-orthogonal de $\mathcal{P}(\Omega)$. On rappelle qu'alors $\dim \mathcal{C} = \frac{n}{2}$ et que tous les mots de \mathcal{C} sont de cardinal pair. En utilisant la formule de Mac Williams (**MW**), démontrer que $P_{\mathcal{C}}(X, Y)$ est invariant par les transformations lorsque $g \in G$.

II.B.2. Quelle est la nature géométrique de l'endomorphisme μ ? et celle de ρ ? En déduire la nature de la composée $\rho\mu$ puis l'ordre du groupe monogène H engendré par $\rho\mu$. Montrer que H est un sous-groupe distingué de G . Expliciter le quotient G/H , puis en déduire le cardinal de G .

On pose $A = \mathbb{C}[X, Y]$ et on utilise les notations de II.A pour $n = 2$.

II.B.3.a. Décomposer la fraction rationnelle $\frac{1}{(1-X^2)(1-X^8)}$ en éléments simples dans $\mathbb{R}(X)$.

II.B.3.b. Calculer le déterminant $\det(\text{Id} - zg)$ lorsque g est une réflexion ou une rotation de l'espace euclidien \mathbb{R}^2 . En utilisant **II.A.4.d.**, en déduire que

$$\Phi_G(z) = \frac{1}{(1-z^2)(1-z^8)}$$

pour tout complexe z tel que $|z| < 1$.

II.B.4. Si r est un réel, on note $[r]$ sa partie entière. En utilisant les questions **II.A.4.** et **II.B.3.b**, montrer que la dimension $a_k(G)$ de l'espace A_k^G des polynômes homogènes à deux variables de degré k invariants par G est

$$a_k(G) = \begin{cases} \left[\frac{k}{8}\right] + 1 & \text{si } k \text{ est pair,} \\ 0 & \text{si } k \text{ est impair.} \end{cases}$$

II.B.5. On considère l'algèbre

$$A = \mathbb{C}[P_2(X, Y), Q_8(X, Y)] = \mathbb{C}\langle P_2(X, Y), Q_8(X, Y) \rangle \cong \mathbb{C}[X, Y]$$

engendrée par les polynômes

$$P_2(X, Y) = X^2 + Y^2 \text{ et } Q_8(X, Y) = \frac{1}{2} \left((X^2 + Y^2)^4 + (X^2 - Y^2)^4 + (2XY)^4 \right)$$

On note A_k la composante homogène de A de degré k . En remarquant que les polynômes P_2 et Q_8 ont déjà été introduits en **I.B.2** et **I.B.3**, démontrer les inclusions $A \subset A^G$ et $A_k \subset A_k^G$. Comme P_2 et Q_8 sont homogènes de degré 2 et 8, la composante homogène A_k sera engendrée par la famille

$$P_2^i Q_8^j \quad (i, j) \in \mathbb{N} \times \mathbb{N} \text{ et } 2i + 8j = k$$

Démontrer que cette famille est libre, et en déduire l'égalité $A = A^G$.

II.B.6. On pose $\Delta(X, Y) = X^2 Y^2 (X^2 - Y^2)^2$ et l'on remarque que

$$Q_8 = P_2^4 - 4\Delta$$

Démontrer que si \mathcal{C} est un code auto-orthogonal de $\mathcal{P}(\Omega)$, le polynôme $P_{\mathcal{C}}(X, Y)$ appartient à l'algèbre

$$\mathbb{Z}[P_2(X, Y), \Delta(X, Y)] = \mathbb{Z}\langle P_2(X, Y), \Delta(X, Y) \rangle \cong \mathbb{Z}[X, Y]$$

Partie III

Dans cette partie on considère l'espace vectoriel \mathbb{Q}^n muni du produit scalaire canonique défini par

$$(v, w) = v_1 w_1 + \dots + v_n w_n \quad \forall v, w \in \mathbb{Q}^n$$

lorsque $v = (v_1, \dots, v_n)$ et $w = (w_1, \dots, w_n)$. On dit qu'un sous-groupe additif L de \mathbb{Q}^n est un réseau de \mathbb{Q}^n s'il existe une base $e = (e_1, \dots, e_n)$ de \mathbb{Q}^n pour laquelle L est l'ensemble de toutes les combinaisons linéaires à coefficients entiers relatifs des vecteurs e_1, \dots, e_n . Dans ce cas, on note $L = \mathbb{Z}e_1 + \dots + \mathbb{Z}e_n$ et l'on dit que e est une \mathbb{Z} -base de L .

III.A. Généralités sur les réseaux

III.A.1. Soit L un réseau de \mathbb{Q} . On appelle dual de L , et on note L^0 , l'ensemble des vecteurs $v \in \mathbb{Q}$ tels que $v \cdot w \in \mathbb{Z}$ pour tout $w \in L$. Démontrer que le dual d'un réseau est un réseau.

III.A.2. Soit L un réseau de \mathbb{Q} et $e = (e_1 \dots e_n)$ une \mathbb{Z} -base de L . On considère une famille $e = (e_1 \dots e_n)$ de n vecteurs dans L , et l'on note P_e^e la matrice carrée de taille n dont les colonnes sont formées des coordonnées des vecteurs e_j dans la base e .

III.A.2.a. Montrer que e est une \mathbb{Z} -base de L si et seulement si $\det(P_e^e) = \pm 1$.

III.A.2.b. En déduire que la valeur absolue du déterminant d'une \mathbb{Z} -base de L par rapport à une base orthonormale de \mathbb{Q}^n ne dépend que de L . Cette valeur est appelée volume de L et notée $\text{Vol}(L)$.

III.A.2.c. Démontrer que $\text{Vol}(L) \text{Vol}(L^0) = 1$.

III.A.3. Dans cette question, M désigne un sous-groupe additif de \mathbb{Q} engendré par un nombre fini d'éléments e_1, \dots, e_s de \mathbb{Q} .

III.A.3.a. Montrer l'existence d'au moins un réseau L qui contient M .

III.A.3.b. Soit $(e_1 \dots e_n)$ une \mathbb{Z} -base de L . Pour tout $k \in \mathbb{N}$ on appelle L_k le sous-groupe additif engendré par $e_1 \dots e_k$. Démontrer par récurrence sur k que $M \setminus L_k$ est engendré par k vecteurs de \mathbb{Q} . En déduire que le groupe M est engendré par n vecteurs.

III.A.3.c. Déduire de la question précédente que, si M contient un réseau de \mathbb{Q} , alors M est lui-même un réseau de \mathbb{Q} .

III.A.4. On suppose que n est un multiple de 4. Soit $(w_1 \dots w_n)$ une base orthogonale de \mathbb{Q}^n telle que pour tout $j = 1, \dots, n$ on a $w_i \cdot w_j = \frac{1}{4}$. Soit Λ l'ensemble des vecteurs $v = \sum_{1 \leq j \leq n} \lambda_j w_j$ tels que

- (a) les λ_j sont entiers et tous de même parité,
- (b) $\sum_{1 \leq j \leq n} \lambda_j$ est multiple de 4.

Démontrer que Λ est un réseau de \mathbb{Q}^n , et que $\Lambda^0 = \Lambda$.

III.A.5. Soit L un réseau de \mathbb{Q}^n . Démontrer qu'il existe un entier $d \geq 1$ tel que $L \subset \frac{1}{d}\mathbb{Z}^n$, puis que l'on peut définir l'entier $d_L = \min_{m \in \mathbb{N}^*} \min_{v \in L} |v|^2 \in \mathbb{N}$. Pour tout entier naturel k , on note $c_k(L)$ le nombre de vecteurs de L de carré scalaire $\frac{k}{d_L}$. Démontrer l'inégalité

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

puis en déduire que la série $\sum_{k=0}^{+\infty} c_k(L) e^{ik\pi z}$ est absolument convergente lorsque z appartient au demi-plan supérieur ouvert du plan de Cauchy.

On pose

$$\theta_L(z) = \sum_{k=0}^{+\infty} c_k(L) e^{ik\pi z} d_L$$

Comme la série est commutativement et associativement convergente, on peut aussi écrire

$$\theta_L(z) = \sum_{v \in L} e^{i(v,v)\pi z}$$

III.B. Codes et réseaux

III.B.1. Démontrer qu'il existe une base orthogonale (v_1, \dots, v_n) de \mathbb{Q}^n telle que l'on ait $(v_i, v_i) = \frac{1}{2}$ pour tout $j = 1, \dots, n$. Dans la suite du problème, on choisit une telle base et on désigne par R le réseau qu'elle engendre.

III.B.2. Dans cette question, on se propose de montrer que les \mathbb{Z} -bases orthogonales de R ont toutes le même ensemble image par la surjection canonique de R sur $R/2R$.

III.B.2.a. Soit $v = (v_1, \dots, v_n)$ une base orthogonale de \mathbb{Q}^n . On note P_e^v la matrice de passage de la base canonique e vers la base v . Calculer la matrice ${}^t(P_e^v)P_e^v$ et en déduire la formule

$$\left(\det P_e^v\right)^2 = \prod_{j=1}^n (v_j, v_j).$$

III.B.2.b. Calculer $(\text{Vol}(R))^2$. En déduire que, si $v = (v_1, \dots, v_n)$ désigne une \mathbb{Z} -base orthogonale de R , alors

$$\prod_{j=1}^n (v_j, v_j) = \frac{1}{2^n}$$

Utiliser cette dernière relation pour montrer qu'il existe des entiers ϵ_j ($1 \leq j \leq n$), valant ± 1 et tels que $v_1, \dots, v_n = \epsilon_1 v_1, \dots, \epsilon_n v_n$. Conclure.

III.B.3. On note Ω l'ensemble image d'une \mathbb{Z} -base orthogonale de R dans $R/2R$. On désigne par \bar{v} l'image de v dans $R/2R$. Le groupe-quotient $R/2R$ est muni d'une structure naturelle d'espace vectoriel sur le corps à deux éléments $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$. On munit cet espace de la forme bilinéaire symétrique β définie par $\beta(\bar{v}, \bar{w}) = \overline{2(v, w)}$.

Vérifier que l'espace vectoriel $R/2R$ muni de la forme bilinéaire β est canoniquement isomorphe à $\mathcal{P}(\Omega)$ muni de la forme bilinéaire naturelle α . On identifiera dorénavant $R/2R$ et $\mathcal{P}(\Omega)$.

III.B.4. Soit \mathcal{C} un code de $\mathcal{P}(\Omega)$. On note $L(\mathcal{C})$ l'image réciproque de \mathcal{C} par la surjection canonique de R sur $R/2R = \mathcal{P}(\Omega)$.

III.B.4.a. Montrer que $2R \subset L(\mathcal{C}) \subset R$. Utiliser la question **III.A.3** pour démontrer que $L(\mathcal{C})$ est un réseau.

III.B.4.b. Montrer que $(2R)^0 = R$. En déduire $L(\mathcal{C})^0 \subset R$ puis $L(\mathcal{C})^0 = L(\mathcal{C}^0)$.

III.B.4.c. Soit $(u_1 \dots u_d)$ une \mathbb{Z} -base de $L(\mathcal{C})$. Expliquer pourquoi $(\bar{u}_1 \dots \bar{u}_d)$ engendre l'espace vectoriel \mathcal{C} . On pose $d = \dim \mathcal{C}$, et l'on suppose que $(\bar{u}_1 \dots \bar{u}_d)$ est une base de \mathcal{C} quitte à modifier l'ordre des vecteurs. Soit X le sous-groupe engendré par les vecteurs $u_1 \dots u_d$. Montrer que pour tout $j \geq d+1$ il existe $x_j \in X$ tel que $u_j = x_j + 2R$.

III.B.4.d. On conserve les notations de la question précédente. Démontrer que

$$(u_1 \dots u_d \ u_{d+1} \dots u_n)$$

est une \mathbb{Z} -base de $L(\mathcal{C})$, puis que $(2u_1 \dots 2u_d \ u_{d+1} \dots u_n)$ est une \mathbb{Z} -base de $2R$. En utilisant la question **III.B.2.b**, déduire alors l'égalité

$$\text{Vol}(L(\mathcal{C})) = 2^{\frac{n}{2} - \dim(\mathcal{C})}$$

III.B.5. Dans cette question on démontre la formule $P_{\mathcal{C}}(\theta_2(z) \theta_3(z)) = \theta_{L(\mathcal{C})}(z)$

III.B.5.a. Montrer que les séries

$$\sum_{k=0}^{+\infty} e^{i2\pi(k+\frac{1}{2})^2 z} \text{ et } \sum_{k=0}^{+\infty} e^{i2\pi k^2 z}$$

convergent pour tout z appartenant au demi-plan ouvert supérieur du plan de Cauchy.

III.B.5.b. En notant que l'on peut écrire

$$\theta_2(z) = \sum_{\substack{m \text{ impair} \\ m \in \mathbb{Z}}} e^{i\pi \frac{m^2}{2} z} \text{ et } \theta_3(z) = \sum_{\substack{m \text{ pair} \\ m \in \mathbb{Z}}} e^{i\pi \frac{m^2}{2} z}$$

montrer que

$$P_{\mathcal{C}}(\theta_2(z) \theta_3(z)) = \sum_{h=0}^{+\infty} v_h e^{i\pi \frac{h}{2} z}$$

où

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

III.B.5.c. Montrer que $\theta_{L(\mathcal{C})}(z) = \sum_{h=0}^{+\infty} d_h e^{i\pi \frac{h}{2} z}$ où $\Lambda_h := \{v \in L(\mathcal{C}) \mid v \cdot v = \frac{h}{2}\}$ et $d_h = \#\Lambda_h$

III.B.5.d. En écrivant l'ensemble Λ_h comme la réunion disjointe

$$\Lambda_h = \sum_{x \in \mathcal{C}} \Lambda_{h-x} \text{ où } \Lambda_{h-x} := \left\{ v \in L(\mathcal{C}) \mid \bar{v} = x \text{ et } v \cdot v = \frac{h}{2} \right\},$$

montrer que $d_h = v_h$. Conclure.

2 Solution proposée

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

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

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 0 car $x + 0 = x$. Enfin le symétrique de x est \overline{x} puisque $x + \overline{x} = 0$.

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 $0 \times x = 0$ et $1 \times x = x$ vérifie bien les quatre axiomes d'un espace vectoriel :

- a) $1 \times x = x$ (trivial)
- b) $(\lambda + \mu) \times x = (\lambda \times x) + (\mu \times x)$. En effet

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

La propriété particulière de la loi de groupe $+$ nous permettant de vérifier ce deuxième axiome est $x + x = 0$ vérifiée pour toute partie x .

- c) $\lambda \times (x + y) = (\lambda \times x) + (\lambda \times y)$ (trivial)
- d) $\lambda \times (\mu \times x) = (\lambda\mu) \times x$ (trivial)

Remarque : On aurait pu utiliser la bijection

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

qui à une partie x de Ω associe la fonction caractéristique χ_x , pour transporter la structure d'espace vectoriel de \mathbb{F}_2^Ω 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^Ω sur $\mathcal{P}(\Omega)$, la multiplication interne étant alors égale à la loi intersection \setminus .

I.A.3. On sait que $\mathcal{P}(\Omega) = 2^n$ et que $\mathcal{P}(\Omega)$ est un \mathbb{F}_2 -espace vectoriel. Nécessairement $\dim_{\mathbb{F}_2}(\mathcal{P}(\Omega)) = n$. On retrouve ce résultat en exhibant une base de $\mathcal{P}(\Omega)$. Si $\Omega = \{t_1, \dots, t_n\}$, et si l'on note x_i le singleton $\{t_i\}$, alors toute partie $x = \{t_{i_1}, \dots, t_{i_k}\}$ de Ω s'écrit

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

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

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

$$\left(\lambda_1 X_1\right) + \dots + \left(\lambda_n X_n\right) = \emptyset \iff \lambda_1 = \dots = \lambda_n = 0$$

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

$$\begin{aligned} \alpha(x + x \setminus y) &= \overline{(x+x) \setminus y} \stackrel{(1)}{=} \overline{(x \setminus y) + (x \setminus y)} \stackrel{(2)}{=} \overline{x \setminus y + x \setminus y - 2x \setminus x \setminus y} \\ &= \overline{x \setminus y} + \overline{x \setminus y} = \alpha(x \setminus y) + \alpha(x \setminus y) \end{aligned}$$

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

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

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

$$y \in \text{Ker } \alpha(x \setminus y) = \overline{x \setminus y} = 0 \iff x = \emptyset$$

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 élément t dans x , et l'on aurait $\overline{x \setminus y} = 1$ pour $y = \{t\}$.

I.A.5. On a $\mathcal{D}(\Omega) = \{x \in \mathcal{P}(\Omega) \mid \overline{x \setminus \Omega} = 0\}$. Comme α est non dégénérée, on a

$$\dim \mathcal{H}(\Omega) + \dim \mathcal{D}(\Omega) = \dim \mathcal{P}(\Omega) = 2^n \text{ donc } \dim \mathcal{H}(\Omega) = 2^n - 1$$

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

$$x \in \mathcal{H}(\Omega) \iff \alpha(x \setminus \Omega) = 0 \iff \overline{x \setminus \Omega} = 0 \iff |x| \text{ pair.}$$

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

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

On a

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

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

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

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

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

Remarque : On a $\mathcal{D}(\Omega) = \Omega \subset \mathcal{H}(\Omega) = \mathcal{D}(\Omega)$ ce qui prouve que $\mathcal{D}(\Omega) \setminus \mathcal{D}(\Omega) = \mathcal{D}(\Omega) = \Omega$, 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 $\dim \mathcal{C} + \dim \mathcal{C} = \dim \mathcal{P}(\Omega) = 2^m$ entraîne $\dim \mathcal{C} = 2^{m/2}$. Ainsi $\mathcal{C} = 2^{m/2}$ 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

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

et

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

où $N(k) = \#\{x \in \mathcal{C} \mid x = k\}$. 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

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

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

$$\begin{cases} N(2k) = C_m^k \\ N(2k+1) = 0 \end{cases}$$

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 $t_{i_1} \setminus t_{i_k}$ de $t_1 \setminus t_m$ telle que $x = t_{i_1} \setminus t_{i_k} \setminus u_{i_1} \setminus u_{i_k}$. 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

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

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 $t_1 \setminus u_1 \setminus t_m \setminus u_m$ est

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

► Montrons que deux éléments \mathcal{C} et $\overline{\mathcal{C}}$ de $\Gamma(\Omega)$ sont isomorphes.

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

$$t_1 u_1, \dots, t_m u_m$$

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

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

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

Le même raisonnement appliqué à $\overline{\mathcal{C}}$ donne

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

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

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

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

$$x = \prod_{s \subset \{1, \dots, m\}} t_{i_s} u_{i_s}$$

et admettra pour image le mot

$$\overline{s(x)} = \prod_{s \subset \{1, \dots, m\}} \{t_{i_s} u_{i_s}\}$$

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

$$\lambda_h = \sum_{h=1}^m \lambda_h = \sum_{k \geq 2} \lambda_k = \alpha \left(\prod_{h=1}^m u_k \right) \lambda_h = \overline{0}$$

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.

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

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

$$\begin{aligned}\bar{\mu} + \bar{\mu} &= (\bar{\mu} \quad \bar{\mu}) \quad (\bar{\mu} \setminus \bar{\mu}) = (\bar{\mu} \quad \bar{\mu}) \setminus \overline{(\bar{\mu} \setminus \bar{\mu})} = (\bar{\mu} \quad \bar{\mu}) \setminus (\mu \quad \mu) \\ \mu + \mu &= (\mu \quad \mu) \quad (\mu \setminus \mu) = (\mu \quad \mu) \setminus (\mu \setminus \mu) = (\mu \quad \mu) \setminus (\bar{\mu} \quad \bar{\mu})\end{aligned}$$

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

$$\begin{aligned}\mu + \bar{\mu} &= (\mu \quad \bar{\mu}) \setminus \overline{(\mu \setminus \bar{\mu})} = (\mu \quad \bar{\mu}) \setminus (\bar{\mu} \quad \mu) = (\bar{\mu} \setminus \bar{\mu}) \quad (\mu \setminus \mu) \\ \bar{\mu} + \mu &= (\bar{\mu} \quad \mu) \setminus (\bar{\mu} \setminus \mu) = (\bar{\mu} \quad \mu) \quad (\mu \setminus \mu) = (\bar{\mu} \setminus \bar{\mu}) \quad (\mu \setminus \mu)\end{aligned}$$

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

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

a)

$$\begin{aligned}x_\mu + x_\mu &= t_h \quad h \quad \mu + \{t_h \quad h \quad \mu\} + u_h \quad h \quad \mu + \{u_h \quad h \quad \mu\} \\ &= \{t_h \quad h \quad \mu + \mu\} + \{u_h \quad h \quad \mu + \mu\} \\ &= x_{\mu+\mu} \quad \mathcal{B}\end{aligned}$$

b)

$$\begin{aligned}y_\mu + y_\mu &= t_h \quad h \quad \mu + \{t_h \quad h \quad \mu\} + u_h \quad h \quad \mathbb{N}_m \mu + \{u_h \quad h \quad \mathbb{N}_m \mu\} \\ &= \{t_h \quad h \quad \mu + \mu\} + \{u_h \quad h \quad \bar{\mu} + \bar{\mu}\} \\ &= \{t_h \quad h \quad \mu + \mu\} + \{u_h \quad h \quad \mu + \mu\} \quad (\text{puisque } \bar{\mu} + \bar{\mu} = \mu + \mu) \\ &= x_{\mu+\mu} \quad \mathcal{B}\end{aligned}$$

c)

$$\begin{aligned}x_\mu + y_\mu &= t_h \quad h \quad \mu + \{t_h \quad h \quad \mu\} + u_h \quad h \quad \mu + \{u_h \quad h \quad \bar{\mu}\} \\ &= \{t_h \quad h \quad \mu + \mu\} + \{u_h \quad h \quad \mu + \bar{\mu}\} \\ &= \{t_h \quad h \quad \mu + \mu\} + \{u_h \quad h \quad \overline{\mu + \bar{\mu}}\} \quad (\text{puisque } \mu + \bar{\mu} = \overline{\mu + \bar{\mu}}) \\ &= y_{\mu+\mu} \quad \mathcal{B}\end{aligned}$$

► 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 $(h)_{1 \leq h \leq m}$ de \mathcal{B} puisque :

$$\begin{cases} 1 = t_1 \quad t_2 \quad t_m = y_\Omega \\ h \quad 2 \quad m \quad h = t_1 \quad t_h \quad u_1 \quad u_h = x_{1 \quad h} \end{cases}$$

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 $x_\mu = 2|\mu|$, $y_\mu = m$,

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

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

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

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 $|\mu|$ pair, et $y_\mu = m$. Ainsi \mathcal{B} sera pair si et seulement si $m \in 4\mathbb{Z}$, i.e. $8\mathbb{Z}$.

I.B.3.e. ► On a

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

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

$$\Omega = \{t_h, t_j, u_h, u_j\} \subset y \subset \Omega.$$

► Montrons que $y \in \Omega$. On a

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

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

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

On a ainsi $y \supset t_i t_j$ et $y \in \mathcal{B}_{16}$ donc $y = x + x$ avec $x \in \mathcal{C}$ et $x \in \mathcal{C}$. 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

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

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

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

I.B.4.a. On a

$$\begin{aligned} f(x) &= \sum_{x \in \mathcal{C}} \sum_{y \in \mathcal{P}(\Omega)} (-1)^{\alpha(x, y)} f(y) = \sum_{y \in \mathcal{P}(\Omega)} \left(\sum_{x \in \mathcal{C}} (-1)^{\alpha(x, y)} \right) f(y) \\ &= \sum_{y \in \mathcal{C}} \left(\sum_{x \in \mathcal{C}} (-1)^{\bar{0}} \right) f(y) + \sum_{y \in \mathcal{C}} \left(\sum_{x \in \mathcal{C}} (-1)^{\alpha(x, y)} \right) f(y) \\ &= 2^{\dim \mathcal{C}} \sum_{y \in \mathcal{C}} f(y) + \sum_{y \in \mathcal{C}} \left(\sum_{x \in \mathcal{C}} (-1)^{\alpha(x, y)} \right) f(y) \end{aligned}$$

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

$$H := \{x \in \mathcal{C} \mid \alpha(x, y) = \bar{1}\} = \{x \in \mathcal{C} \mid \alpha(x - x, y) = \bar{0}\}$$

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

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

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

Donc

$$\begin{aligned}
 \text{(MW)} \quad & 2^{\dim \mathcal{C}} \binom{x}{x} \binom{x}{\mathcal{C}} X^x Y^{-x} = \binom{x}{x} \binom{x}{\mathcal{C}} (Y - X)^x (X + Y)^{-x} \\
 & f(x) = \binom{x}{x} \binom{x}{\mathcal{C}} (Y - X)^x (X + Y)^{-x}
 \end{aligned}$$

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

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

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

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

où

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

Le nombre de parties de x à k éléments est $\binom{x}{k}$ donc

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

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

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

L'égalité (*) s'en déduit.

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

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

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

► Si $v \in V$ alors $p_G(v) \in V^G$ 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

$$\text{Tr}(p_G) = \frac{1}{G} \text{Tr}(g)$$

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

$$\text{Mat}(p_G; v) = \begin{pmatrix} 1 & & 0 & 0 & 0 \\ & \ddots & & & \\ 0 & & 1 & 0 & 0 \\ 0 & & 0 & 0 & 0 \\ & & & & \ddots & \\ 0 & & 0 & 0 & & 0 \end{pmatrix}$$

d'où $\text{Tr}(p_G) = k = \dim(V^G)$.

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

$$\dim(V^G) = \dim(V^G) = \frac{1}{G} \text{Tr}(g) \quad (*)$$

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

$$\{g \in G \mid (g) = g\} = \{g \in G \mid (g g^{-1}) = Id\} = g \text{ (Ker)}$$

donc

$$|\{g \in G \mid (g) = g\}| = |g \text{ (Ker)}| = \text{Ker} = \frac{G}{G}$$

En remplaçant dans (*) :

$$\dim(V^G) = \dim(V^G) = \frac{1}{G} \frac{1}{\text{Ker}} \text{Tr}((g)) = \frac{1}{G} \text{Tr}((g))$$

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 $M = \text{Mat}(g; e)$, on a

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

ce que l'on notera plus simplement

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

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

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

donc

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

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. ► $X_1^{\alpha_1} X_2^{\alpha_2} \dots X_n^{\alpha_n}$ est une base de A_k , et le nombre de n -uplets d'entiers $(\alpha_1, \dots, \alpha_n)$ tels que $\alpha_1 + \dots + \alpha_n = k$ 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

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

dès que $\alpha_1 + \dots + \alpha_n = k$. Comme chacun des polynômes $\prod_{j=1}^n \gamma_{ji} X_j^{\alpha_j}$ est homogène de degré α_m , le polynôme

$$\sigma_g(X_1^{\alpha_1} X_2^{\alpha_2} \dots X_n^{\alpha_n}) = \prod_{j=1}^n \gamma_{j1} X_j^{\alpha_1} \prod_{j=1}^n \gamma_{jn} X_j^{\alpha_n}$$

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 $\sum_{k=0}^+ a_k z^k$ entraînera 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 $\lim_{k \rightarrow +\infty} \frac{a_{k+1}}{a_k} = 1$ 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 $|\frac{1}{z}| = 1$. En particulier la fonction $z \mapsto \frac{1}{\det(Id-zg)}$ 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 $\sum_{k=0}^{\infty} r_k z^k$ sera ≥ 1 .

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

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

avec

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

Par ailleurs $M = \text{Mat}(g; e) = \text{diag}(\alpha_1, \dots, \alpha_n)$ entraîne

$$\begin{aligned} g_k \begin{pmatrix} X_1^{k_1} & X_2^{k_2} & \cdots & X_n^{k_n} \end{pmatrix} &= \sigma_g \begin{pmatrix} X_1^{k_1} & X_2^{k_2} & \cdots & X_n^{k_n} \end{pmatrix} = (\alpha_1 X_1)^{k_1} \cdots (\alpha_n X_n)^{k_n} \\ &= \begin{pmatrix} \alpha_1^{k_1} & & & \\ & \alpha_2^{k_2} & & \\ & & \ddots & \\ & & & \alpha_n^{k_n} \end{pmatrix} \begin{pmatrix} X_1^{k_1} & & & \\ & X_2^{k_2} & & \\ & & \ddots & \\ & & & X_n^{k_n} \end{pmatrix} \end{aligned}$$

d'où

$$\text{Tr}(g_k) = \sum_{\alpha_1 + \dots + \alpha_n = k} \alpha_1^{k_1} \cdots \alpha_n^{k_n} = r_k$$

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

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

Alors

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

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

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

$$a_k(G) = \dim(A_k^G) = \frac{1}{G} \sum_{g \in G} \text{Tr}(g_k)$$

Alors, pour $z < 1$,

$$\Phi_G(z) = \sum_{k=0}^{+\infty} a_k(G) z^k = \sum_{k=0}^{+\infty} \frac{1}{G} \operatorname{Tr}(g_k) z^k = \frac{1}{G} \sum_{k=0}^{+\infty} \operatorname{Tr}(g_k) z^k$$

soit

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

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 $\dim \mathcal{C} = \frac{x}{2}$ et $\mathcal{C} = \mathcal{C}^x$. La formule de Mac Williams donne

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

d'où

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

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

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

puisque 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 :

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

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

$$\rho(\rho\mu)^k \rho^{-1} \in H \quad (1)$$

$$\rho(\rho\mu)^k \mu^{-1} \in H \quad (2)$$

$$\mu(\rho\mu)^k \mu^{-1} \in H \quad (3)$$

$$\mu(\rho\mu)^k \rho^{-1} \in H \quad (4)$$

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

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

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

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

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

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

$$G/H = \{\overline{Id}, \overline{\rho}\} \text{ et } |G/H| = 2$$

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

$$G = Id \quad \rho\mu \quad (\rho\mu)^2 \quad (\rho\mu)^3 \quad \rho \quad (\rho\mu)\rho \quad (\rho\mu)^2\rho \quad (\rho\mu)^3\rho$$

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

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

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

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

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

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

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

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

d'où

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

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

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

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

$$e = \frac{A\left(e^{i\frac{\pi}{4}}\right)}{B\left(e^{i\frac{\pi}{4}}\right)} = \frac{1}{8i\sqrt{2}}$$

$$f = \frac{A(i)}{B(i)} = \frac{1}{16i}$$

$$g = \frac{A\left(e^{i\frac{3\pi}{4}}\right)}{B\left(e^{i\frac{3\pi}{4}}\right)} = \frac{1}{8i\sqrt{2}}$$

Enfin on calcule

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

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

et

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

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

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

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

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

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

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

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

$$\begin{aligned}\Phi_G(z) &= \frac{1}{G} \frac{1}{\det(Id - zg)} = \frac{1}{16} \frac{8}{1 - z^2} + \frac{1}{z^2 - 2 \cos \frac{k\pi}{4} z + 1} \\ &= \frac{1}{16} \frac{8}{1 - z^2} + \frac{1}{(z - e^{i\frac{k\pi}{4}})(z - e^{-i\frac{k\pi}{4}})}\end{aligned}$$

d'où

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

Finalement

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

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

$$a_k(G) = \sum_{(i, j) \in \mathbb{N} \times \mathbb{N}, 2i + 8j = k} 1$$

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 $\lfloor \frac{k}{8} \rfloor + 1$ 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

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

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

$$\lambda_{i,j} P_2^i Q_8^j = 0$$

$$\begin{matrix} (i,j) \in \mathbb{N} \times \mathbb{N} \\ 2i+8j=k \end{matrix}$$

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 $T \in \mathbb{C}[X,Y]$ tel que

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

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

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

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

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

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

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

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

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

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 $\lambda_{i,j_0} \notin \mathbb{Z}$. Cet indice i est alors unique puisque vérifie $2i + 8j_0 = k$ (où k est pair par hypothèse). Notons i_0 l'indice tel que $\lambda_{i_0,j_0} \notin \mathbb{Z}$. On a

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

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 $H_1(X, Y) \in \mathbb{Z}[X, Y]$. On aura

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

soit

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

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

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

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

III.A.1. L'ensemble

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

est clairement un sous-groupe additif de \mathbb{Q} . Soit $e = (e_1, \dots, e_n)$ une \mathbb{Z} -base de L . Soit $e^* = (e_1^*, \dots, e_n^*)$ 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 $l_v : x \mapsto v \cdot x$. Soit e_i l'unique vecteur tel que $e_i^* = l_{e_i}$. Alors (e_1, \dots, e_n) est une base de \mathbb{Q} et si $w = \sum_{i=1}^n w_i e_i$,

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

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

$$v \in L^0 \iff \exists (v \cdot e_i) \in \mathbb{Z} \quad v = \sum_{i=1}^n (v \cdot e_i) e_i \in \mathbb{Z} e_1 \oplus \dots \oplus \mathbb{Z} e_n$$

III.A.2.a. Notons d'abord que si e est une \mathbb{Z} -base de L , ou bien si $\det(P_e^e) = \pm 1$, 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 $X = {}^t(x_1, \dots, x_n)$ le vecteur-colonne des coordonnées de x dans e , et $X = {}^t(x_1, \dots, x_n)$ 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

$$X = {}^t(x_1 \quad \dots \quad x_n) \in \mathbb{Z}^n \quad X = P^{-1}X \in \mathbb{Z}^n$$

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

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

entraîne $\det P = \pm 1$.

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

$$P^{-1} = \frac{1}{\det P} {}^t \text{com}(P) \in \mathcal{M}_n(\mathbb{Z})$$

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

$$L \subset \mathbb{Z}e_1 + \dots + \mathbb{Z}e_n$$

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

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

$$P_v^e \times P_e^{e'} \times P_{e'}^{v'} = P_{v'}^{v'}$$

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

$$\det(P_v^e) \times \det(P_e^{e'}) = \pm 1$$

d'où

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

Finalement $\det(P_v^e) = \left| \det(P_{e'}^{v'}) \right|$.

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

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

et

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

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

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

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

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

donc

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

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

III.A.3.b. $M \setminus L_1$ est un sous-groupe du groupe monogène $L_1 = \text{Gr}(e_1)$. 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, \dots, u_k de \mathbb{Q} , la projection

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

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

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

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

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

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

Au rang s on aura

$$M = M \setminus L = \mathbb{Z}u_1 + \dots + \mathbb{Z}u_s$$

de sorte que M soit bien engendré par n vecteurs.

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

$$\mathbb{Z}e_1 \oplus \dots \oplus \mathbb{Z}e_n \subset M = \mathbb{Z}u_1 + \dots + \mathbb{Z}u_n$$

d'où

$$n = \dim \text{Vect}(e_1, \dots, e_n) \leq \dim \text{Vect}(u_1, \dots, u_n)$$

Nécessairement le système (u_1, \dots, u_n) sera libre dans \mathbb{Q} , et l'on aura

$$M = \mathbb{Z}u_1 \oplus \dots \oplus \mathbb{Z}u_n$$

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 $v = \sum_{1 \leq j \leq n} \lambda_j w_j$ et $v' = \sum_{1 \leq j \leq n} \lambda'_j w_j$ vérifient (a) et (b), alors $v - v' = \sum_{1 \leq j \leq n} (\lambda_j - \lambda'_j) w_j$, les $\lambda_j - \lambda'_j$ sont tous de même parité, et

$$\sum_{1 \leq j \leq n} (\lambda_j - \lambda'_j) \equiv \sum_{1 \leq j \leq n} \lambda_j - \sum_{1 \leq j \leq n} \lambda'_j \equiv 0 \pmod{2} \quad (4)$$

Donc $v - v' \in \Lambda$. 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

$$v = \sum_{1 \leq j \leq n} \lambda_j w_j = \sum_{1 \leq j \leq n} \mu_j (4w_j) \in \Lambda$$

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

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

$$\begin{aligned} (v \in \Lambda^0) \iff v \in \Lambda \iff v - v' \in \Lambda \iff \sum_{1 \leq j \leq n} (\lambda_j - \lambda'_j) w_j \in \Lambda \iff \sum_{1 \leq j \leq n} (\lambda_j - \lambda'_j) \lambda_j \in 4\mathbb{Z} \\ \iff \sum_{1 \leq j \leq n} (\lambda_j - \lambda'_j) \lambda_j \equiv 0 \pmod{4} \iff \sum_{1 \leq j \leq n} \lambda_j \lambda'_j \equiv 0 \pmod{4} \end{aligned} \quad (*)$$

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

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

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

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

$$\prod_{1 \leq j \leq} \lambda_j \lambda_j = \prod_{1 \leq j \leq} (2\mu_j) (2\mu_j + 1) \equiv \prod_{1 \leq j \leq} (2\mu_j) \equiv \prod_{1 \leq j \leq} \lambda_j \equiv 0 \pmod{4}$$

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

$$\begin{aligned} \prod_{1 \leq j \leq} \lambda_j \lambda_j &= \prod_{1 \leq j \leq} (2\mu_j + 1) (2\mu_j + 1) \equiv \prod_{1 \leq j \leq} (2\mu_j + 2\mu_j + 1) \\ &\equiv \prod_{1 \leq j \leq} (\lambda_j + \lambda_j) \equiv 0 \pmod{4} \end{aligned}$$

puisque (λ_j) et (λ_j) vérifient (a) et (b), et puisque $\prod_{1 \leq j \leq} \lambda_j \lambda_j$ 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 $L \subset \frac{1}{d}\mathbb{Z}^n$. Pour tout $v \in L$ on a donc $d^2 \|v\|^2 = (dv) \cdot (dv) \in \mathbb{Z}$, d'où $d^2 \|v\|^2 \in \mathbb{N}$. L'ensemble $\{m \in \mathbb{N}^* \mid m \|v\|^2 \in \mathbb{N}\}$ inclus dans \mathbb{N} n'est donc pas vide et possède un plus petit élément d_L .

Si $v \in L$ et $\|v\|^2 = \frac{k}{d_L}$, écrivons $v = \frac{1}{d} (n_1 \dots n_n)$ dans la base canonique. On a

$$\frac{n_i^2}{d^2} = \frac{k}{d_L} \quad n_i \leq d \sqrt{\frac{k}{d_L}} \quad n_i \leq d \sqrt{\frac{k}{d_L}}$$

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

$$c_k(L) \leq \left(2d \sqrt{\frac{k}{d_L}} + 1 \right)^n$$

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

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

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

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

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

$$(\alpha \sqrt{k} + 1) e^{-bk\pi} \sim \alpha \sqrt{k} e^{-bk\pi}$$

et $\lim_{k \rightarrow +\infty} (\alpha \sqrt{k} e^{-bk\pi}) = 0$. la série à termes positifs $\sum_{k=0}^{+\infty} (\alpha \sqrt{k} + 1) e^{-bk\pi}$ convergera donc, et cela entraîne la convergence de $\sum_{k=0}^{+\infty} c_k(L) e^{ik\pi z}$ par comparaison.

III.B.1. Si $e = (e_1 \dots e_n)$ 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 orthogonale qui satisfait $v_i \cdot v_i = \frac{1}{2}$

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

$${}^t(P_e^v) P_e^v = \text{Diag}(v_1 \cdot v_1 \quad \dots \quad v_n \cdot v_n) \quad \text{et} \quad (\det P_e^v)^2 = \prod_{j=1}^n (v_j \cdot v_j).$$

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

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

d'où

$$\prod_{j=1}^n (v_j \cdot v_j) = \frac{1}{2^n} \quad (1)$$

Si l'on pose $v_j = \sum_{k=1}^n a_{kj} v_k$ où $a_{kj} \in \mathbb{Z}$, alors

$$v_j \cdot v_j = \frac{1}{2} \sum_{k=1}^n a_{kj}^2 \geq \frac{1}{2} \quad (2)$$

(1) et (2) impliquent $v_j \cdot v_j = \frac{1}{2}$ pour tout j , donc $\sum_{k=1}^n a_{kj}^2 = 1$ 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 ϵ_j ($1 \leq j \leq n$), valant ± 1 tels que

$$\{v_1 \quad \dots \quad v_n\} = \epsilon_1 v_1 \quad \dots \quad v_n$$

Par conséquent l'image de l'ensemble $v_1 \dots v_m$ par la surjection canonique de R sur $R/2R$ sera égale à celle de $\bar{v}_1 \dots \bar{v}_m$.

III.B.3. On a $\Omega = \bar{v}_1 \dots \bar{v}_m \subset R/2R$. L'application

$$\Psi : \mathcal{P}(\Omega) \rightarrow \frac{R/2R}{v_{i_1} + \dots + v_{i_m}}$$

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

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

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

$$\begin{cases} \Psi(\bar{0} \bar{v}_{i_1} \dots \bar{v}_{i_m}) = \Psi(\bar{0}) = \bar{0} = \bar{0} \Psi(\bar{v}_{i_1} \dots \bar{v}_{i_m}) \\ \Psi(\bar{1} \bar{v}_{i_1} \dots \bar{v}_{i_m}) = \Psi(\bar{v}_{i_1} \dots \bar{v}_{i_m}) = \overline{v_{i_1} + \dots + v_{i_m}} = \bar{1} \Psi(\bar{v}_{i_1} \dots \bar{v}_{i_m}) \end{cases}$$

Ψ est injective car son noyau est réduit à $\bar{0}$ (c'est le vecteur nul de $\mathcal{P}(\Omega)$).

Les systèmes $(\bar{v}_1 \dots \bar{v}_m)$ et $(\bar{v}_1 \dots \bar{v}_m)$ 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 $(\bar{v}_1 \dots \bar{v}_m)$. C'est évident puisque :

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

et

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

III.B.4.a. On a

$$R \xrightarrow{\pi} \frac{R/2R}{v_{i_1} + \dots + v_{i_m}} \xrightarrow{\Psi} \mathcal{P}(\Omega)$$

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

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

$$= \{v \in R \mid x = \bar{v}_{i_1} \dots \bar{v}_{i_m} \in \mathcal{P}(\Omega), \mu_i \in \mathbb{Z}, v - (v_{i_1} + \dots + v_{i_m}) = \sum_{i=1}^m 2\mu_i v_i\} \quad (1)$$

$$= \{v \in R \mid x = \bar{v}_{i_1} \dots \bar{v}_{i_m} \in \mathcal{P}(\Omega), \mu_i \in \mathbb{Z}, v - (v_{i_1} + \dots + v_{i_m}) \in 2R\}$$

$$= \{v \in R \mid x = \bar{v}_{i_1} \dots \bar{v}_{i_m} \in \mathcal{P}(\Omega), v = \sum_{i=1}^m \lambda_i v_i \text{ et } \lambda_i \text{ impair ssi } i = i_1, \dots, i_m\} \quad (2)$$

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 $2v_1 \dots 2v_m$ $v_{i_1} + \dots + v_{i_m} \quad i_1 \dots i_m \subset \mathbb{N}$. 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 $(v_1 \dots v_m)$ est choisie comme en **III.B.1**. Alors

$$\begin{aligned} (2R)^0 &= \left\{ v = \sum_{i=1}^m \lambda_i v_i \mid \lambda_i \in \mathbb{Q}, w = \sum_{i=1}^m 2\mu_i v_i \mid \mu_i \in \mathbb{Z} \right\} \\ &= \left\{ v = \sum_{i=1}^m \lambda_i v_i \mid \lambda_i \in \mathbb{Q} \right\} = R \end{aligned}$$

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

$$\begin{aligned} L(\mathcal{C})^0 &= \left\{ v \in R \mid \exists w \in L(\mathcal{C}) \text{ tel que } v = 2w \right\} \\ &= \left\{ v \in R \mid \exists w \in L(\mathcal{C}) \text{ tel que } v = 2w \right\} \\ &= \left\{ v \in R \mid \exists \bar{w} \in \mathcal{C} \text{ tel que } \beta(\bar{v} \bar{w}) = \overline{2v \bar{w}} = \bar{0} \right\} = L(\mathcal{C}^0) \end{aligned}$$

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

$$u_j - \sum_{i=1}^d \lambda_i u_i \in 2R$$

Il suffit de poser $x_j = \sum_{i=1}^d \lambda_i u_i \in X$ pour obtenir $u_j = x_j + 2r_j \in 2R$.

III.B.4.d. ► Le système $(u_1 \dots u_d, u_{d+1} \dots u_m)$ est une base de \mathbb{Q} et engendrent $L(\mathcal{C})$ (puisque $(u_1 \dots u_m)$ 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 $v \in 2R$ s'écrit sous la forme

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

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

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

et cela prouve que le système $(2u_1 \quad 2u_d \quad u_{d+1} \quad u)$ 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 :

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

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

$$\text{Vol}(L(\mathcal{C})) = 2^{-\bar{2} - \dim(\mathcal{C})}$$

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

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

prouve que les deux séries $\sum_{k=0}^{+\infty} e^{i2\pi(k+\frac{1}{2})^2 z}$ et $\sum_{k=0}^{+\infty} e^{i2\pi k^2 z}$ sont absolument convergentes lorsque z est fixé tel que $\text{Im}(z) > 0$.

III.B.5.b. On a

$$\begin{aligned} P_{\mathcal{C}}(z) &= \sum_{x \in \mathcal{C}} (z)^x (z)^{-x} \\ &= \sum_{x \in \mathcal{C}} e^{i\pi \frac{m^2}{2} z} + \sum_{\substack{m \text{ pair} \\ m \in \mathbb{Z}}} e^{i\pi \frac{m^2}{2} z} = \sum_{h=0}^{+\infty} v_h e^{i\pi \frac{h}{2} z} \end{aligned}$$

où

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

III.B.5.c. On a bien

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

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

$$\begin{aligned} v &= \sum_{j=1}^m \lambda_j v_j & v &= \sum_{j=1}^m \lambda_j v_j \\ \overline{v} &= \sum_{j=1}^m \overline{\lambda_j} \overline{v_j} = x = \overline{v_{i_1} + \dots + v_{i_m}} & \lambda_j &\text{ est } \begin{cases} \text{impair si } j = i_1 \quad \dots \quad i_m \\ \text{pair sinon.} \end{cases} \\ v(v) &= \frac{1}{2} \sum_{j=1}^m \lambda_j^2 = \frac{h}{2} & \lambda_j^2 &= h \end{aligned}$$

donc

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

$$= v_h$$

En conclusion

$$d_h = \Lambda_h = \prod_{x \in \mathcal{C}} \Lambda_{h,x} = v_h \quad \text{et} \quad PC(\varphi_2(z), \varphi_3(z)) = \theta_{L(\mathcal{C})}(z)$$