Groupes de réflexions complexes

Corrigé

a) Si $\gamma_b = 1_{\mathrm{A}}$ pour tout $b \in \mathrm{B}$ et $\eta = 1_{\mathrm{B}}$, l'application θ est l'application $\mathrm{id}_{\mathrm{A}\times\mathrm{B}}$. Par ailleurs, si θ_1 est définie par

$$\theta_1 \colon \begin{cases} \mathrm{A}\times\mathrm{B} \longrightarrow \mathrm{A}\times\mathrm{B} \\ (a,b) \longmapsto (\delta_b(a), \mu(b)) \end{cases}$$

alors

$$\theta\circ\theta_1 \colon \begin{cases} \mathrm{A}\times\mathrm{B} \longrightarrow \mathrm{A}\times\mathrm{B} \\ (a,b) \longmapsto (\gamma_{\mu(b)}\delta_b(a), \eta\mu(b)) \end{cases}$$

est aussi de la forme souhaitée. Enfin, l'application

$$\widetilde{\theta} \colon \begin{cases} \mathrm{A}\times\mathrm{B} \longrightarrow \mathrm{A}\times\mathrm{B} \\ (a,b) \longmapsto (\gamma_{\eta^{-1}(b)}{}^{-1}(a), \eta^{-1}(b)) \end{cases}$$

vérifie $\theta\circ\widetilde{\theta} = \mathrm{id}_{\mathrm{A}\times\mathrm{B}}$ et $\widetilde{\theta}\circ\theta = \mathrm{id}_{\mathrm{A}\times\mathrm{B}}$ et est de la forme souhaitée. Ainsi $\mathrm{G}\wr\mathrm{H}$ est un sous-groupe de $\mathfrak{S}(\mathrm{A}\times\mathrm{B})$.

b) Considérons l'application

$$\varphi \colon \begin{cases} \mathrm{G}\wr\mathrm{H} \longrightarrow \mathrm{G}^{\mathrm{B}} \rtimes \mathrm{H} \\ \theta \longmapsto (\gamma\circ\eta^{-1}, \eta)\,. \end{cases}$$

Elle est bijective par définition du produit en couronne. De plus, pour la fonction θ_1 de la question **a**, on a $\theta\circ\theta_1(a,b) = (\gamma_{\mu(b)}\delta_b(a), \eta\mu(b))$ et donc

$$\varphi(\theta\circ\theta_1) = \big([(\gamma\circ\mu)\delta]\circ(\eta\mu)^{-1}, \eta\mu\big) = ((\gamma\circ\eta^{-1})[(\delta\circ\mu^{-1})\circ\eta^{-1}]), \eta\mu) = (\gamma\circ\eta^{-1}, \eta)\cdot_{\rtimes}(\delta\circ\mu^{-1}, \mu) = \varphi(\theta)\cdot_{\rtimes}\varphi(\theta_1)\,.$$

c) $\mathrm{G}\wr(\mathrm{H}\wr\mathrm{K})$ est l'ensemble des bijection de $\mathrm{A}\times\mathrm{B}\times\mathrm{C}$ de la forme

$$\theta \colon \begin{cases} \mathrm{A}\times\mathrm{B}\times\mathrm{C} \longrightarrow \mathrm{A}\times\mathrm{B}\times\mathrm{C} \\ (a,b,c) \longmapsto (\gamma_{b,c}(a), \mu((b,c))) \end{cases}$$

où $\mu \in \mathrm{H}\wr\mathrm{K}$ et $\gamma_{b,c} \in \mathrm{G}$. Ainsi θ est de la forme

$$\theta \colon \begin{cases} \mathrm{A}\times\mathrm{B}\times\mathrm{C} \longrightarrow \mathrm{A}\times\mathrm{B}\times\mathrm{C} \\ (a,b,c) \longmapsto (\gamma_{b,c}(a), \delta_c(b), \varepsilon(c)) \end{cases}$$

où $\gamma_{b,c} \in \mathrm{G}$, $\delta_c \in \mathrm{H}$ et $\varepsilon \in \mathrm{K}$.

Par ailleurs, $(\mathrm{G}\wr\mathrm{H})\wr\mathrm{K}$ est l'ensemble des bijection de $\mathrm{A}\times\mathrm{B}\times\mathrm{C}$ de la forme

$$\theta \colon \begin{cases} \mathrm{A}\times\mathrm{B}\times\mathrm{C} \longrightarrow \mathrm{A}\times\mathrm{B}\times\mathrm{C} \\ (a,b,c) \longmapsto (\gamma_c(a,b), \varepsilon(c)) \end{cases}$$

où $\gamma_c \in \mathrm{G}\wr\mathrm{H}$ et $\varepsilon \in \mathrm{K}$. Ainsi θ est de la forme

$$\theta \colon \begin{cases} \mathrm{A}\times\mathrm{B}\times\mathrm{C} \longrightarrow \mathrm{A}\times\mathrm{B}\times\mathrm{C} \\ (a,b,c) \longmapsto (\gamma_{b,c}(a), \delta_c(b), \varepsilon(c)) \end{cases}$$

où $\gamma_{b,c} \in \mathrm{G}$, $\delta_c \in \mathrm{H}$ et $\varepsilon \in \mathrm{K}$ ce qui montre l'égalité souhaité.

Corrigé

a) Pour $k \in \mathbb{N}$, notons u_k l'ensemble des multiples de p^k inférieur à n qui ne sont pas des multiples de p^{k+1} :

$$u_k = (p^k\mathbb{Z} \smallsetminus p^{k+1}\mathbb{Z}) \cap [\![1 \,,\, n]\!].$$

Chacun des éléments de u_k intervient pour la multiplicité de p pour exactement k et donc

$$\mathrm{M}_n = \sum_{k=1}^{+\infty} k|u_k| \,.$$

La somme précédente ne compte qu'un nombre fini de termes non nuls. Par ailleurs, $\mathrm{E}(n/p^k)$ représente le nombre de multiple non nul de p^k inférieur à n, ce qui donne

$$|u_k| = \mathrm{E}\left(\frac{n}{p^k}\right) - \mathrm{E}\left(\frac{n}{p^{k+1}}\right).$$

En remplaçant dans l'expression de M_n trouvée plus haut, on obtient la première égalité. Pour la deuxième égalité, il suffit de constater que

$$\mathrm{E}\left(\frac{n}{p^k}\right) = a_0 p^{u-k} + a_1 p^{u-k-1} + \cdots + a_{u-k}.$$

On obtient alors $\mathrm{M}_n = a_0(p^{u-1} + \cdots + 1) + a_1(p^{u-2} + \cdots + 1) + \cdots + a_{p-1}$. Enfin pour finir, il suffit de remarquer que

$$\mathrm{M}_{p^k} = \frac{p^k - 1}{p - 1}$$

ce qui est un simple conséquence de la deuxième égalité dans la cas $n = p^k$.

b) On crée une partition de l'ensemble $[\![1 \,,\, n]\!]$ formée de a_0 parties de cardinal p^u, a_1 parties de cardinal p^{u-1}, etc. Le sous-groupe des permutations de $[\![1 \,,\, n]\!]$ qui laisse stable toutes les parties de cette partition est alors isomorphe à $\mathfrak{S}_{p^u}{}^{a_0} \times \mathfrak{S}_{p^{u-1}}{}^{a_1} \times \cdots \times \mathfrak{S}_p{}^{a_{u-1}}$. Ainsi, si on note P_k un p-Sylow de $\mathfrak{S}_{p^k}$, alors $\mathrm{P}_u{}^{a_0} \times \mathrm{P}_{u-1}{}^{a_1} \times \cdots \times \mathrm{P}_1{}^{a_{u-1}}$ s'identifie un p-sous-groupe de $\mathfrak{S}_n$ de cardinal p^{M_n} (question **a**) c'est donc un p-Sylow de $\mathfrak{S}_n$.

c) On a
$$\mathrm{M}_{p^{r+1}} = \frac{p^{r+1} - 1}{p - 1} = \frac{p^{r+1} - p}{p - 1} + 1 = p\mathrm{M}_{p^r} + 1 \,.$$

d) Dans cette question, les indices sont pris modulo p. On pose

$$c = \prod_{j=1}^{p^{r-1}} (j, p^{r-1} + j, 2p^{r-1} + j, \ldots, (p-1)p^{r-1} + j)$$

Le produit précédent est défini sans équivoque puisque les cycles intervenant dans l'écriture sont à supports disjoints et donc commutent. On considère à présent la partition de l'ensemble $[\![1 \,,\, p^r]\!]$ en p parties $(\mathrm{X}_0, \ldots, \mathrm{X}_{p-1})$ de cardinal p^{r-1} donnée par

$$\forall\, i \in [\![0 \,,\, p-1]\!], \qquad \mathrm{X}_i = \left\{ip^{r-1} + 1, \ldots, ip^{r-1} + p^{r-1}\right\} = \left\{ip^{r-1} + 1, \ldots, (i+1)p^{r-1}\right\}.$$

Le sous-groupe des permutations de $[\![1 \,,\, p^r]\!]$ qui laissent stables toutes les parties de cette partition est alors isomorphe à $(\mathfrak{S}_{p^{r-1}})^p$. On note G un p-Sylow de $\mathfrak{S}(\mathrm{X}_1) = \mathfrak{S}_{p^{r-1}}$, G^p s'identifie alors à un sous-groupe de $(\mathfrak{S}_{p^{r-1}})^p \subset \mathfrak{S}_{p^r}$ et dans $\mathfrak{S}_{p^r}$ on a $c^{-j}(g_0, \ldots, g_{p-1})c^j = (g_j, \ldots, g_{p-1+j})$ et $\mathrm{G}^p \cap \langle c \rangle = \{1\}$. ce qui montre que $\langle \mathrm{G}^p, c \rangle$ est un produit semi-direct de G^p par $\langle c \rangle$ et a pour cardinal $p^{p\mathrm{M}_{p^{r-1}}} p = p^{\mathrm{M}_r}$. C'est donc un p-Sylow de $\mathfrak{S}_{p^r}$.

Par ailleurs, le groupe cyclique d'ordre p engendré par c agit de façon fidèle sur l'ensemble $\{\mathrm{X}_0, \ldots, \mathrm{X}_{p-1}\}$ via $c^j \cdot \mathrm{X}_i := c^j(\mathrm{X}_i) = \mathrm{X}_{i+j}$. Montrons que $\mathrm{G} \wr \langle c \rangle$ est isomorphe au p-Sylow de $\mathfrak{S}_{p^r}$ décrit plus haut. D'après la question **b** de l'exercice1, on dispose de l'isomorphisme $\mathrm{G} \wr \langle c \rangle \overset{\text{gr.}}{\simeq} \mathrm{G}^{\{\mathrm{X}_0, \ldots, \mathrm{X}_{p-1}\}} \rtimes \langle c \rangle \overset{\text{gr.}}{\simeq} \mathrm{G}^p \rtimes \langle c \rangle$ et dans ce produit semi-direct, on a $c^{-j}(g_0, \ldots, g_{p-1})c^j = (g_j, \ldots, g_{j-1+p})$ ce qui donne l'isomorphisme souhaité.

Corrigé

a) Le polynôme minimal de g est $\mathrm{P} = (\mathrm{X} - 1)(\mathrm{X} - \xi)$. Ainsi P est un polynôme annulateur de $f = g_{|\mathrm{F}}$. Le lemme des noyaux appliqué à f et P donne alors

$$\mathrm{F} = (\mathrm{W}_1 \cap \mathrm{F}) \oplus (\mathrm{W}_\xi \cap \mathrm{F}).$$

Si $W_\xi \not\subset F$, alors comme W_ξ est de dimension 1, $W_\xi \cap F = 0$ et donc $F = W_1 \cap F$ c'est-à-dire $F \subset W_1$.

Réciproquement, si F est contenu dans W_1 alors F est bien entendu stable par g. Si F contient W_ξ, alors pour $x \in F$, on a $g(x) \in F$. En effet, on considère $x = u + h$ la décomposition de x dans la somme directe $V = W_\xi \oplus W_1$ c'est-à-dire $u \in W_\xi$ et $h \in W_1$. Comme $W_\xi \subset F$, on a $h = x - u \in F$ et alors $g(x) = \xi u + h \in F$.

b) La décomposition de V est une décomposition de G-module, donc V_i est stable par g pour tout $i \in [\![1\,,\,\ell]\!]$. Ainsi, d'après la question **a**, $V_i \subset W_1$ ou $V_i \subset W_\xi$. Si $V_i \subset W_1$ pour tout $i \in [\![1\,,\,\ell]\!]$, alors comme $V^G \subset W_1$, on a $V = W_1$ et donc $g = \mathrm{id}$ ce qui est absurde. On en déduit qu'il existe $i \in [\![1\,,\,\ell]\!]$ tel que $W_\xi \subset V_i$. De plus, comme $V_j \cap V_i = \{0\}$ si $i \neq j$, on ne peut pas avoir $W_\xi \subset V_j$ si $i \neq j$ ce qui donne l'unicité et le fait que $V_j \subset W_1$ pour $j \neq i$.

c) Comme $V_i \cap V_j = \{0\}$, on a $R_i \cap R_j = \varnothing$. Par ailleurs, d'après la question **a**, on a $R = \amalg_{i=1}^{\ell} R_i$. De plus, pour tout $i \in [\![1\,,\,\ell]\!]$, on a $R_i \neq \varnothing$. En effet, sinon d'après la question **b**, on a $V_i \subset \mathrm{Ker}\,(g - \mathrm{id})$ pour tout $g \in R$. Comme G est engendré par R, on en déduit que $V_i \subset \mathrm{Ker}\,(g - \mathrm{id})$ pour tout $g \in G$ et donc $V_i \subset V^G$ ce qui est absurde.

d) Raisonnons par l'absurde et supposons que $\varphi : V_i \to V_j$ soit un isomorphisme de G-modules. D'après la question **c**, il existe $g \in R_i$. On note $v \in V_i$ un vecteur propre de g associé à la valeur propre $\xi \neq 1$. On a alors $g\varphi(v) = \varphi(gv) = \varphi(\xi v) = \xi\varphi(v)$. Ainsi $\varphi(v)$ est un vecteur propre de g associé à ξ et donc $\varphi(v) \in \mathbb{C}v \subset V_i$. Or, par hypothèse, φ est à valeurs dans V_j, donc $\varphi(v) = 0$ ce qui contredit l'injectivité de φ.

La décomposition $(*)$ est donc la décomposition en composantes isotypiques, ce qui montre l'unicité. On pose alors $G_i = \langle R_i \rangle$. D'après la question **b**, les éléments de G_i laissent fixes V_j pour $j \neq i$ et stabilisent V_i. Ainsi G_i s'identifie à un sous-groupe de réflexion de $\mathrm{GL}(V_i)$ et pour $g \in G_i$ et $h \in G_j$ avec $i \neq j$, les éléments g et h commutent. Comme R engendrent G, on en déduit que $G = G_1 \times \cdots \times G_\ell$. De plus, tout sous-espace stable de V_i stable par G_i est stable par G et donc G_i agit sur V_i de façon irréductible.

e) Soient $(s_1, \ldots, s_\ell)$ une système générateur de G formé de réflexions. On a alors

$$V^G = \bigcap_{i=1}^{\ell} \mathrm{Ker}\,(s_i - \mathrm{id})\,.$$

Comme les $\mathrm{Ker}\,(s_i - \mathrm{id})$ sont des hyperplans, on a $\dim V^G \geqslant \dim V - \ell$ c'est-à-dire $\ell \geqslant \dim V/V^G$. La deuxième partie est une conséquence élémentaire des questions **c** et **d**.

f) *Remarque.* Soient $g \in R_i$ et v un vecteur propre de g associé à la valeur propre $\xi \neq 1$. Alors

$$\mathrm{vect}\,(gv,\ g \in G) = \mathrm{vect}\,(gv,\ g \in G_i) = V_i.$$

En effet, $v \in V_i$ et V_i est G-stable donc $\mathrm{vect}\,(gv,\ g \in G_i) \subset \mathrm{vect}\,(gv,\ g \in G) \subset V_i$. De plus, $\mathrm{vect}\,(gv, g \in G_i)$ est un sous-G_i-module de V_i non réduit à 0 (car il contient v), donc par irréductibilité de V_i, on a les égalités souhaitées.

Centralisateur : première démonstration. Soit $\gamma \in \mathcal{C}$ et $i \in [\![1\,,\,\ell]\!]$. D'après la question **c**, il existe $g \in R_i$. On note v un vecteur propre de g associé à la valeur propre $\xi \neq 1$. Comme γ et g commutent, le sous-espace propre $\mathbb{C}v$ de g associé à la valeur propre ξ est stable par γ. Donc il existe $\mu \in \mathbb{C}$ tel que $\gamma v = \mu v$. De plus, comme γ est inversible, $\mu \in \mathbb{C}^\times$. Par ailleurs, $\gamma(g'v) = g'\gamma v = \mu g' v$ pour tout $g' \in G$. Ainsi, grâce à la remarque ci-dessus, γ agit comme une homothétie de rapport $\mu \in \mathbb{C}^\times$ sur V_i. Enfin, si $v \in V^G$, on a $g\gamma v = \gamma g v = \gamma v$ et donc $\gamma v \in V^G$. Le sous-espace V^G est donc stable par γ et comme G agit trivialement sur V^G, tout élément de $\mathrm{GL}(V^G)$ appartient à $\mathcal{C}$.

Centralisateur : deuxième démonstration. Tout élément de $\mathcal{C}$ est un automorphisme du G-module V et donc stabilise les composantes isotypiques c'est-à-dire la décomposition $(*)$. Comme G agit trivialement sur V^G, tout élément de $\mathrm{GL}(V^G)$ appartient à $\mathcal{C}$. De plus, pour $i \in [\![1\,,\,\ell]\!]$, γ induit un isomorphisme du G-module irréductible V_i c'est-à-dire une homothétie d'après le lemme de Schur.

Normalisateur. Soit $\gamma \in \mathcal{N}$, montrons que V^G et $V_1 \oplus \cdots \oplus V_\ell$ sont stables par γ. Si $v \in V^G$, on a $g\gamma v = \gamma g' v = \gamma v$ et donc $\gamma v \in V^G$. Si $g \in R_i$ et v est un vecteur propre pour g associé à la valeur propre $\xi \neq 1$ alors $\gamma g \gamma^{-1}$ est un pseudoréflexion de G dont γv est un vecteur propre pour la valeur propre $\xi \neq 1$. Ainsi, d'après la question **b**, il existe $j \in [\![1\,,\,\ell]\!]$ tel que $\gamma v \in V_j$. On a alors $\gamma g v = g'\gamma v \in g' V_j = V_j$ et donc d'après la remarque ci-dessus $\gamma V_i \subset V_j$ et donc $V_1 \oplus \cdots \oplus V_\ell$ est bien stable par γ. Pour finir, comme G agit trivialement sur V^G, tout élément de $\mathrm{GL}(V^G)$ appartient à $\mathcal{N}$.

g) Soit $\gamma \in \mathcal{N}$ un élément unipotent. D'après la question **f**, on peut écrire $\gamma = (x, y)$ avec $x \in \mathrm{GL}(V^G)$ unipotent et $y \in \mathrm{GL}(V_1 \oplus \cdots \oplus V_\ell)$ unipotent. Comme $\mathcal{N}/\mathcal{C}$ est fini puisque c'est un sous-groupe du groupe des automorphismes de G, on en déduit qu'il existe $n \in \mathbb{N}^*$ tel que $\gamma^n \in \mathcal{C}$. Or $\gamma^n = (x^n, y^n)$ avec x^n et y^n unipotents. La description des éléments de $\mathcal{C}$ donnée à la question **f** montre que $y^n = \mathrm{id}$. Or, si u est un

endomorphisme unipotent d'un espace vectoriel de dimension finie, on a $\mathrm{Ker}\,(u^k - \mathrm{id}) = \mathrm{Ker}\,(u - \mathrm{id})$ pour tout $k \in \mathbb{N}^*$. Ainsi $y = \mathrm{id}$ et $\gamma \in \mathrm{GL}(\mathrm{V}^{\mathrm{G}}) \subset \mathcal{N}$ est unipotent.

Corrigé

a) Dans cette question, les indices sont pris dans $\mathbb{Z}/n\mathbb{Z}$ et on note $\xi = \exp(2i\pi/n)$. Pour commencer, on remarque que $\mathrm{A}^n = a_1 a_2 \cdots a_n \mathrm{Id}_n$. On en déduit que A est diagonalisable et que les valeurs propres de A sont des racines n-ième de $a = a_1 \cdots a_n$. Par ailleurs, si

$$\mathrm{X} = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$$

est vecteur propre de A associé à la valeur propre α alors

$$\mathrm{Y} = \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix} = \begin{bmatrix} x_1 \\ \xi x_2 \\ \vdots \\ \xi^{n-1} x_n \end{bmatrix}$$

est vecteur propre de A associé à la valeur propre $\alpha\xi^{-1}$. En effet, l'égalité matricielle $\mathrm{AX} = \alpha\mathrm{X}$ se traduit par $x_i a_i = \alpha x_{i+1}$ pour $i \in \mathbb{Z}/n\mathbb{Z}$ ce qui donne $(\mathrm{AY})_{i+1} = a_i y_i = x_i \xi^{i-1} a_i = \alpha \xi^{i-1} x_{i+1} = \xi^{-1} \alpha y_{i+1}$ pour $i \in \mathbb{Z}/n\mathbb{Z}$. On obtient bien $\mathrm{AY} = \alpha\xi^{-1}\mathrm{Y}$. Toutes les racines n-ième de a sont donc valeurs propres de A. De plus, elles sont nécessairement simples. Enfin, la résolution du système $x_i a_i = \alpha x_{i+1}$ pour $i \in \mathbb{Z}/n\mathbb{Z}$ montre que l'on peut choisir comme vecteur propre associé à la valeur propre α le vecteur

$$\mathrm{X} = \begin{bmatrix} 1 \\ \dfrac{a_1}{\alpha} \\ \dfrac{a_1 a_2}{\alpha^2} \\ \vdots \\ \dfrac{a_1 \cdots a_{n-1}}{\alpha^{n-1}} \end{bmatrix}$$

b) On a $(\mathrm{P}_\sigma)_{ij} = \delta_{i\sigma(j)}$ et $(\mathrm{P}_\sigma{}^{-1})_{ij} = ({}^t\mathrm{P}_\sigma)_{ij} = \delta_{j\sigma(i)}$. On en déduit que $(\mathrm{P}_\sigma \mathrm{A} \mathrm{P}_\sigma{}^{-1})_{ij} = a_{\sigma^{-1}(i)\sigma^{-1}(j)}$.

c) Montrons que pour $r \geqslant 2$, on a $\mathrm{G}(de, e, r) \subset \mathrm{G}(d'e', e', r)$ si et seulement si $de \mid d'e'$ et $d \mid d'$.

On suppose que $\mathrm{G}(de, e, r) \subset \mathrm{G}(d'e', e', r)$. Soit ξ (resp. ζ) une racine d-ième (resp. de-ième) primitive de l'unité. Comme les éléments $g = \mathrm{diag}\,(\xi, 1, \ldots 1)$ et $h = \mathrm{diag}\,(\zeta, \zeta^{-1}, 1, \ldots, 1)$ sont dans $\mathrm{G}(de, e, r)$, on a $\xi^{d'} = 1$ et $\zeta^{d'e'} = 1$ c'est-à-dire $d \mid d'$ et $de \mid d'e'$.

Réciproquement, si $de \mid d'e'$ et $d \mid d'$ alors toute racine d-ième (resp. de-ième) de l'unité est une racine d'-ième (resp. $d'e'$-ième) de l'unité et donc $\mathrm{G}(de, e, r) \subset \mathrm{G}(d'e', e', r)$.

Pour $r = 1$, la définition de $\mathrm{G}(de, e, 1)$ montre que $\mathrm{G}(de, e, 1) = \mathrm{G}(d, 1, 1) = \mathbb{U}_d$. On en déduit que $\mathrm{G}(de, e, 1) \subset \mathrm{G}(d'e', e', 1)$ si et seulement si $d \mid d'$.

d) On commence par remarquer que $\mathfrak{S}_r$ et $\mathrm{D}(de, e, r)$ sont contenus dans $\mathrm{G}(de, e, r)$. Grâce aux opérations sur les lignes, on constate que $\mathrm{G}(de, e, r) = \mathrm{D}(de, e, r)\mathfrak{S}_r$, (de même, grâce aux opérations sur les colonnes, on constate que $\mathrm{G}(de, e, r) = \mathfrak{S}_r \mathrm{D}(de, e, r)$). Montrons à présent que $\mathrm{D}(de, e, r)$ est distingué dans $\mathrm{G}(de, e, r)$. Comme $\mathrm{G}(de, e, r) = \mathrm{D}(de, e, r)\mathfrak{S}_r$, il suffit de montrer que $\mathrm{P}_\sigma \mathrm{D} \mathrm{P}_\sigma{}^{-1} \in \mathrm{D}(de, e, r)$ pour tout $\mathrm{D} \in \mathrm{D}(de, e, r)$ et tout $\sigma \in \mathfrak{S}_r$. Or, pour $\mathrm{D} = \mathrm{diag}\,(\xi_1, \ldots, \xi_r) \in \mathrm{D}(de, e, r)$, la question **b** montre que

$$\mathrm{P}_\sigma \mathrm{D} \mathrm{P}_\sigma{}^{-1} = \mathrm{diag}\,(\xi_{\sigma^{-1}(1)}, \ldots, \xi_{\sigma^{-1}(r)}) \in \mathrm{D}(de, e, r).$$

Par ailleurs, on a $\mathrm{D}(de, e, r) \cap \mathfrak{S}_r = \{\mathrm{Id}_r\}$ ce qui montre bien que $\mathrm{G}(de, e, r)$ est un produit semi-direct de $\mathrm{G}(de, e, r)$ par $\mathfrak{S}_r$. On en déduit que $|\mathrm{G}(de, e, r)| = |\mathfrak{S}_r||\mathrm{D}(de, e, r)|$. Comme on dispose des isomorphismes de groupes réciproques l'un de l'autre

$$\varphi\colon \begin{cases} \mathrm{D}(de, e, r) & \longrightarrow \mathbb{U}_{de}{}^{r-1} \times \mathbb{U}_d \\ \mathrm{diag}\,(\xi_1, \ldots, \xi_r) & \longmapsto \begin{bmatrix} \xi_1 \\ \vdots \\ \xi_{r-1} \\ \xi_1 \cdots \xi_r \end{bmatrix} \end{cases} \quad \text{et} \quad \psi\colon \begin{cases} \mathbb{U}_{de}{}^{r-1} \times \mathbb{U}_d \longrightarrow \mathrm{D}(de, e, r) \\ \begin{bmatrix} \xi_1 \\ \cdots \\ \xi_{r-1} \\ y \end{bmatrix} \longmapsto \mathrm{diag}\,(\xi_1, \ldots, \xi_{r-1}, y/(\xi_1 \cdots \xi_{r-1})), \end{cases}$$

on obtient $|\mathrm{D}(de,e,r)| = (de)^{r-1}d$ et donc $|\mathrm{G}(de,e,r)| = r!(de)^{r-1}d$.

e) On note $\pi : \mathrm{G}(de,e,r) \to \mathfrak{S}_r$ la surjection associée à la structure de produit semi-direct. Soit $g \in \mathrm{G}(de,e,r)$ une réflexion. La décomposition de $\pi(g) \in \mathfrak{S}_r$ en cycles à support disjoint fournit une famille de sous-espaces de $\mathbb{C}^r$ stable par g sur lequel g agit comme une matrice du type de la question **a**. Autrement dit, g est conjuguée par une matrice de permutation à une matrice de la forme

$$\begin{bmatrix} \mathrm{A}_1 & & \\ & \ddots & \\ & & \mathrm{A}_d \end{bmatrix}$$

où A_i est comme dans la question **a**. Toujours d'après la question **a**, 1 est valeur propre de multiplicité au plus un de chacun des A_d donc au plus d de g. Comme g est une réflexion, 1 est valeur propre de multiplicité $r-1$. On en déduit que $r-1 \leqslant d$. On a donc $d = r$ ou $d = r-1$.

Si $d = r$ alors toutes les matrices A_i sont de taille 1. La conjuguée de g et donc g sont diagonales. Comme g est une réflexion, on a $g = \mathrm{diag}\,(1,\dots,1,\xi,1,\dots,1)$ avec $\xi^d = 1$ et $\xi \neq 1$. Le couple racine-coracine de g est alors $v = (e_i, (1-\xi)e_i^*)$ et l'ordre de g est celui de $\xi \in \mathbb{U}_d \smallsetminus \{1\}$ c'est-à-dire un diviseur de d différent de 1.

Si $d = r-1$ alors les matrices A_i sont de taille 1 et égal à Id_1 sauf une qui est de taille 2 et possède 1 comme valeur propre. D'après la question **a**, on en déduit que le produit des coefficients non nuls de cette matrice de taille 2 est 1. Elle est donc de la forme

$$\begin{bmatrix} & \xi^{-1} \\ \xi & \end{bmatrix}$$

avec $\xi \in \mathbb{U}_{de}$. On en déduit que $g = \mathrm{diag}\,(1,\dots,1,\xi^{-1},1,\dots,1,\xi,1,\dots,1)\mathrm{P}_{\tau_{ij}}$ où $\xi \in \mathbb{U}_{de}$, τ_{ij} est la transposition qui échange i et j et ξ^{-1} est en place i et ξ en place j sur la diagonale. L'ordre de g est 2 et un couple racine-coracine est $(e_i - \xi e_j, e_i^* - \xi^{-1}e_j^*)$. Remarquez que le cas $\xi = 1$ correspond aux matrices de transposition.

f) Si $r = 1$ alors $\mathrm{G}(de,e,1)$ est bien sûr irréductible.

On suppose $r > 1$. Soit V un sous-$\mathrm{G}(de,e,r)$-module de $\mathbb{C}^r$ avec $\mathrm{V} \neq \{0\}$ et $\mathrm{V} \neq \mathbb{C}^r$. L'espace V est en particulier stable par les matrices de permutation. L'exercice11 et l'exemple13 de la feuille de TD 3. montre que $\mathrm{V} = \mathbb{C}(1,\dots,1)$ ou V est l'hyperplan H des vecteurs dont la somme des coordonnées est nulle. De plus, comme tout sous-espace stable par $\mathrm{G}(de,e,r)$ admet un supplémentaire stable par $\mathrm{G}(de,e,r)$, on en déduit que $\mathbb{C}(1,\dots,1)$ est stable par $\mathrm{G}(de,e,r)$ si et seulement si H l'est. Il suffit donc d'étudier $\mathbb{C}(1,\dots,1)$.

On suppose $r \geqslant 3$. Si $de \neq 1$, on considère $g = \mathrm{diag}\,(\xi,\xi^{-1},1,\dots,1)$ où ξ est une racine de-ième primitive de l'unité. On a alors $g((1,\dots,1)) = (\xi,\xi^{-1},1,\dots,1) \notin \mathbb{C}(1,\dots,1)$ puisque $\xi \neq 1$. Si $de = 1$ alors $\mathrm{G}(1,1,r) = \mathfrak{S}_r$ n'est pas irréductible.

On suppose que $r = 2$ et on considère $g = \mathrm{diag}\,(\xi,\xi^{-1})$ où ξ est une racine de-ième primitive de l'unité. On a alors $g((1,1)) = (\xi,\xi^{-1})$ et donc $g((1,1)) \in \mathbb{C}(1,1)$ si et seulement si $\xi = \xi^{-1}$ c'est-à-dire si et seulement si $\xi^2 = 1$ ou encore si et seulement si $de \mid 2$.

Si $\mathbb{C}(1,1)$ est stable par $\mathrm{G}(de,e,2)$ alors $de \mid 2$ c'est-à-dire

(i) soit $d = e = 1$;
(ii) soit $d = 2$ et $e = 1$;
(iii) soit $d = 1$ et $e = 2$.

Dans le cas (ii), on a $\mathrm{diag}\,(-1,1) \in \mathrm{G}(2,1,2)$ et $g((1,1)) = (-1,1) \notin \mathbb{C}(1,1)$. Dans le cas (i) et (iii), $\mathrm{G}(de,e,2)$ a respectivement 2 et 4 éléments et donc est commutatif. Une représentation de dimension 2 ne peut donc être irréductible.

Finalement $\mathrm{G}(de,e,r)$ est irréductible sauf si $d = e = 1$ et $r \geqslant 2$ ou $e = r = 2$ et $d = 1$.

g) Comme $\mathfrak{S}_r \subset \mathrm{G}(de,e,r)$, on a $(\mathbb{C}^r)^{\mathrm{G}(de,e,r)} \subset (\mathbb{C}^r)^{\mathfrak{S}_r}$. Or pour $\sigma \in \mathfrak{S}_r$ et $\mathrm{X} = (x_1,\dots,x_r)$, on a

$$\sigma \cdot \mathrm{X} = \mathrm{P}_\sigma \mathrm{X} = \begin{bmatrix} x_{\sigma^{-1}(1)} \\ \vdots \\ x_{\sigma^{-1}(n)} \end{bmatrix}.$$

Comme σ agit transitivement sur $[\![1\,,\, n]\!]$, on en déduit que $(\mathbb{C}^r)^{\mathfrak{S}_r} = \mathbb{C}(1,\dots,1)$ (voir aussi l'exercice 6 de la feuille de TD 3).

Si $r = 1$ alors $\mathrm{G}(de,e,1) = \mathbb{U}_d$ est le groupe cyclique d'ordre d des racines d-ième de l'unité. Si $d > 1$ alors $\mathbb{C}^{\mathbb{U}_d} = \{0\}$. D'après la question **e** de l'exercice3, il faut au moins une réflexion pour engendré $\mathrm{G}(de,e,1)$.

De plus, une racine d-ième primitive de l'unité engendré $\mathbb{U}_d$ et agit sur $\mathbb{C}$ comme une réflexion. Finalement pour $d > 1$, le groupe $\mathrm{G}(de, e, 1)$ est bien engendré et contient donc un sous-groupe bien engendré. Si $d = 1$ alors $\mathrm{G}(e, e, 1) = \{1\}$ et $\mathbb{C}^{\{1\}} = \mathbb{C}$. Comme l'ensemble $\varnothing$ est un système générateur de $\mathrm{G}(e, e, 1)$ formé de 0 réflexions et que $\dim \mathbb{C}/\mathbb{C}^{\{1\}} = 0$. Ainsi $\mathrm{G}(e, e, 1)$ est bien engendré et contient donc un sous-groupe bien engendré.

Si $r \geqslant 2$ alors $\mathrm{G}(de, e, r)$ contient l'élément $g = \mathrm{diag}\,(\xi, \xi^{-1}, 1, \ldots, 1)$ où ξ est une racine de-ième primitive de l'unité. On a alors $g((1, \ldots, 1)) = (\xi, \xi^{-1}, 1, \ldots, 1)$. Si $de \neq 1$ alors $\xi \neq 1$ et $(1, \ldots, 1) \notin (\mathbb{C}^r)^{\mathrm{G}(de,e,r)}$. On en déduit que $(\mathbb{C}^r)^{\mathrm{G}(de,e,r)} = \{0\}$ et grâce à la question **e** de l'exercice3 qu'il faut au moins r réflexions pour engendrer $\mathrm{G}(de, e, r)$. Si $de = 1$ c'est-à-dire $d = e = 1$ alors $\mathrm{G}(1, 1, r) = \mathfrak{S}_r$ et $(\mathbb{C}^r)^{\mathfrak{S}_r} = \mathbb{C}(1, \ldots, 1)$. La question **e** de l'exercice3 montre qu'il faut au moins $r-1$ réflexions pour engendrer $\mathfrak{S}_r$. Mais les transpositions $(i, i+1)$ pour $1 \leqslant i \leqslant r-1$ forment un ensemble de $r-1$ réflexions (voir la question **d**) qui engendrent $\mathfrak{S}_r$. Ainsi $\mathrm{G}(1, 1, r)$ est bien engendré et donc contient un groupe de réflexion bien engendré.

On note

(i) τ_i la transposition qui échange i et $i+1$ pour $1 \leqslant i \leqslant r-1$;
(ii) $g_d = \mathrm{diag}\,(\xi, 1, \ldots, 1)$ pour ξ une racine d-ième primitive de l'unité ;
(iii) $h_{de} = \mathrm{diag}\,(\zeta, \zeta^{-1}, 1, \ldots, 1)\tau_1$ pour ζ une racine de-ième primitive de l'unité.

D'après la question **d**, l'ensemble $\mathrm{F} = \{h_{de}, g_d, \tau_i, 1 \leqslant i \leqslant r-1\}$ est un sous-ensemble de $\mathrm{G}(de, e, r)$ formé de l'identité ou de réflexions. Montrons que c'est un système générateur de $\mathrm{G}(de, e, r)$. On note $\mathrm{G} = \langle \mathrm{F} \rangle$. On a bien sûr $\mathfrak{S}_r \subset \mathrm{G}$ et $f_{de} = \mathrm{diag}\,(\zeta, \zeta^{-1}, 1, \ldots, 1) \in \mathrm{G}$. En conjugant par des matrices de permutations, on en déduit que $\mathrm{D}(de, de, r) \subset \mathrm{G}$. En effet, considérons $g \in \mathrm{D}(de, de, r)$ c'est-à-dire $g = \mathrm{diag}\,(\zeta_1, \ldots, \zeta_r)$ avec $\zeta_i \in \mathbb{U}_{de}$ et $\zeta_1 \ldots \zeta_r = 1$. Comme ζ engendre $\mathbb{U}_{de}$, il existe une famille d'entier $n_i \in \mathbb{N}$ tel que $\zeta_i = \zeta^{n_i}$. On pose $\sigma_i = (1, i)(2, i+1) \in \mathfrak{S}_r \subset \mathrm{G}$. On a alors

$$g = {f_{de}}^{n_1} \left(\sigma_2 {f_{de}}^{n_1+n_2} {\sigma_2}^{-1}\right) \cdots \left(\sigma_{r-1} {f_{de}}^{n_1+\cdots+n_{r-1}} {\sigma_{r-1}}^{-1}\right) \in \mathrm{G}.$$

De plus, si $g = \mathrm{diag}\,(\xi_1, \ldots, \xi_r) \in \mathrm{D}(de, e, r)$, on peut écrire $g = hh'$ avec

$$h = \mathrm{diag}\,((\xi_2 \cdots \xi_r)^{-1}, \xi_2, \ldots, \xi_r) \in \mathrm{D}(de, de, r) \subset \mathrm{G} \qquad \text{et} \qquad h' = \mathrm{diag}\,(\xi_1 \cdots \xi_r, 1, \ldots, 1)$$

où $(\xi_1 \cdots \xi_r)^d = 1$. On en déduit qu'il existe $n \in \mathbb{N}$ tel que $h' = {g_d}^n \in \mathrm{G}$. Ainsi $g \in \mathrm{G}$ et donc $\mathrm{D}(de, e, r) \subset \mathrm{G}$. On en déduit que $\mathrm{G}(de, e, r) = \mathrm{D}(de, e, r)\mathfrak{S}_r = \mathrm{G}$.

Finalement, si $de \neq 1$, le cardinal minimal d'une famille génératrice formée de réflexions est donc r ou $r+1$. De plus, si $d = e = 1$ alors $g_d = \mathrm{id}$ et $h_{de} = \tau_1$ et on dispose d'une famille génératrice formée de $r-1$ réflexions. Le groupe $\mathrm{G}(1, 1, r) = \mathfrak{S}_r$ est bien engendré (Ce cas a déjà été traité). Si $d = 1$ et $e \neq 1$ alors $g_d = \mathrm{id}$ et on dispose d'une famille génératrice formé de réflexions de cardinal r. Le groupe $\mathrm{G}(e, e, r)$ est donc bien engendré. De même, si $e = 1$ alors $h_{de} = g_d \tau_1 {g_d}^{-1}$ et donc on dispose d'une famille génératrice formé de réflexions de cardinal r. Le groupe $\mathrm{G}(d, 1, r)$ est donc bien engendré.

Finalement $\mathrm{G}(de, e, r)$ est bien engendré si et seulement si $d = 1$ ou $e = 1$ ou $r = 1$. Et d'après la question **c**, $\mathrm{G}(de, e, r)$ contient le sous-groupe bien engendré $\mathrm{G}(de, de, r)$. De plus, d'après la question **f**, $\mathrm{G}(de, de, r)$ est irréductible sauf si $de = 1$ et $r \geqslant 2$ ou $e = r = 2$ et $d = 1$. Dans le premier cas, on a $d = e = 1$ et donc $\mathfrak{S}_r = \mathrm{G}(de, e, r)$ n'est pas irréductible. Dans le deuxième cas, on a $\mathrm{G}(de, de, r) = \mathrm{G}(2, 2, 2)$ et donc $\mathrm{G}(de, e, r) = \mathrm{G}(2, 1, 2)$ qui est irréductible et bien engendré ou $\mathrm{G}(de, e, r) = \mathrm{G}(2, 2, 2)$ qui est n'est pas irréductible.

h) D'après la question **b**, $\mathrm{A} = (a_{ij})_{i,j}$ commute avec toutes les matrices de permutation si et seulement si $a_{\sigma(i)\sigma(j)} = a_{ij}$ pour tout σ et tout (i, j). Comme $\mathfrak{S}_r$ est transitif sur $[\![1\,,\, r]\!]$ et doublement transitif sur $[\![1\,,\, r]\!]$ si $r \geqslant 2$, on en déduit que A est de la forme

$$\mathrm{A}(a, b) = \begin{bmatrix} a & b & \cdots & b \\ b & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & b \\ b & \cdots & b & a \end{bmatrix} \qquad \text{avec} \quad a, b \in \mathbb{C}\,.$$

Première démonstration. Soit $g \in \mathrm{ZG}(de, e, r)$. En particulier, g commute avec toutes les matrices de permutation et donc $g = \mathrm{A}(a, b)$ pour $a, b \in \mathbb{C}$. Si $a \neq 0$ alors comme le nombre de coefficients non nuls dans la matrice g est r, on en déduit que g est scalaire. Si $a = 0$ alors nécessairement $b \neq 0$ puisque g est inversible mais le nombre de coefficient non nuls de g est $r(r-1)$. On a donc $r(r-1) = r$ c'est-à-dire $r = 2$.

Ainsi, si $r \neq 2$ le centre de $\mathrm{G}(de, e, r)$ est formé de matrices scalaires. On a donc $g = \zeta\mathrm{id}$ avec $\zeta \in \mathbb{U}_{de}$ et $\zeta^{rd} = 1$ ce qui est équivalent à $g = \zeta\mathrm{id}$ avec $\zeta^{d\mathrm{pgcd}\,(e,r)} = 1$. Ainsi, le centre est $\mathbb{U}_{d\mathrm{pgcd}\,(e,r)}\mathrm{id}$ et a pour cardinal $d\mathrm{pgcd}\,(e, r)$.

Si $r = 2$ alors soit g est scalaire et donc comme ci-dessus $g = \zeta\mathrm{id}$ avec $\zeta \in \mathbb{U}_{d\mathrm{pgcd}\,(2,e)}$. Soit

$$g = \begin{bmatrix} 0 & \xi \\ \xi & 0 \end{bmatrix}$$

avec $\xi \in \mathbb{U}_{de}$ et $\xi^{2d} = 1$. Comme g commute avec $\mathrm{diag}\,(\zeta, \zeta^{-1}) \in \mathrm{G}(de, e, r)$ avec ζ racine de-ième primitive de l'unité, on en déduit que $\xi\zeta = \xi\zeta^{-1}$ et donc $\zeta^2 = 1$ ce qui signifie que $de \mid 2$.

Si $de = 1$ alors $d = e = 1$ et $\mathrm{G}(1, 1, 2) = \mathfrak{S}_2$ est commutatif et donc égal à son centre. Si $de = 2$ alors soit $d = 2$ et $e = 1$ soit $d = 1$ et $e = 2$. Dans le premier cas, g commute avec $\mathrm{diag}\,(-1, 1)$ ce qui donne $-\xi = \xi$ ce qui est absurde donc g est scalaire. Dans le deuxième cas, on a

$$\mathrm{G}(2, 2, 2) = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} \right\}.$$

Il est donc de cardinal 4 et isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$ puisque tous ses éléments sont d'ordre 2.

Finalement, $\mathrm{ZG}(de, e, r) = \mathbb{U}_{d\mathrm{pgcd}\,(e,r)}\mathrm{id}$ sauf si $d = e = 1$ et $r = 2$ auquel cas $\mathrm{ZG}(1, 1, 2) = \mathrm{G}(1, 1, 2) = \mathfrak{S}_2$ et si $d = 1$ et $e = r = 2$ auquel cas $\mathrm{ZG}(2, 2, 2) = \mathrm{G}(2, 2, 2) \overset{\mathrm{gr.}}{\simeq} (\mathbb{Z}/2\mathbb{Z})^2$.

Deuxième démonstration. Si $\mathrm{G}(de, e, r)$ est irréductible alors d'après le lemme de Schur tout élément $g \in \mathrm{ZG}(de, e, r)$ est une matrice scalaire. On a donc $g = \zeta\mathrm{id}$ avec $\zeta \in \mathbb{U}_{de}$ et $\zeta^{rd} = 1$ ce qui est équivalent à $g = \zeta\mathrm{id}$ avec $\zeta^{d\mathrm{pgcd}\,(e,r)} = 1$. Ainsi, le centre est $\mathbb{U}_{d\mathrm{pgcd}\,(e,r)}\mathrm{id}$ et a pour cardinal $d\mathrm{pgcd}\,(e, r)$.

D'après la question **f**, il reste à traiter les cas $de = 1$ et $r \geqslant 2$ et $e = r = 2$ et $d = 1$. Dans le premier cas, on a $\mathrm{G}(1, 1, r) = \mathfrak{S}_r$ qui a un centre trivial sauf si $r = 2$. Si $r \neq 2$, on a bien $\mathrm{ZG}(de, e, r) = \mathbb{U}_{d\mathrm{pgcd}\,(e,r)}\mathrm{id}$. Si $r = 2$, on a $\mathrm{ZG}(1, 1, 2) = \mathrm{G}(1, 1, 2)$. Dans le deuxième cas, $\mathrm{G}(2, 2, 2)$ est commutatif et donc $\mathrm{ZG}(2, 2, 2) = \mathrm{G}(2, 2, 2)$.

i) Le groupe $\mathrm{G}(de, e, r)$ est abélien si et seulement si $\mathrm{ZG}(de, e, r) = \mathrm{G}(de, e, r)$. Pour $r = 1$, $\mathrm{G}(de, e, 1)$ est bien sûr commutatif. Si $r \neq 1$ alors $\mathrm{G}(de, e, r)$ n'est pas contenu dans le groupe des matrices scalaires. Donc $\mathrm{G}(de, e, r) \neq \mathrm{ZG}(de, e, r)$ sauf si le centre n'est pas constitué uniquement de matrices scalaires c'est-à-dire si $d = e = 1$ et $r = 2$ ou $d = 1$ et $e = r = 2$. Dans le premier cas, on a $\mathrm{ZG}(1, 1, 2) = \mathrm{G}(1, 1, 2) = \mathfrak{S}_2$ est commutatif ; dans le deuxième cas on a $\mathrm{ZG}(2, 2, 2) = \mathrm{G}(2, 2, 2)$ est commutatif.

Ainsi $\mathrm{G}(de, e, r)$ est commutatif si et seulement si $r = 1$ ou ($d = e = 1$ et $r = 2$) ou ($d = 1$ et $e = r = 2$).

j)

k) D'après la question **d**, $\mathrm{G}(d, 1, r)$ est un produit semi-direct de ${\mathbb{U}_d}^r$ par $\mathfrak{S}_r$. Le morphisme de $\mathfrak{S}_r$ dans $\mathrm{Aut}({\mathbb{U}_d}^r)$ associé est :

$$\Psi : \begin{cases} \mathfrak{S}_r \longrightarrow \mathrm{Aut}({\mathbb{U}_d}^r) \\ \sigma \longmapsto ((\xi_1, \ldots, \xi_r) \mapsto (\xi_{\sigma^{-1}(1)}, \ldots, \xi_{\sigma^{-1}(r)})) \,. \end{cases}$$

Passons au cas du produit en couronne $\mathrm{C}_d \wr \mathfrak{S}_r$. On considère $\mathrm{C}_d = \mathbb{U}_d$ comme groupe de permutation de lui-même via l'action naturelle et $\mathfrak{S}_r$ agissant par permutation sur $[\![1 , r]\!]$. D'après la question **b** de l'exercice 1, $\mathrm{C}_d \wr \mathfrak{S}_r$ est isomorphe à ${\mathrm{C}_d}^r \rtimes \mathfrak{S}_r$ et le morphisme de $\mathfrak{S}_r$ dans $\mathrm{Aut}({\mathbb{U}_d}^r)$ associé est :

$$\Psi_1 : \begin{cases} \mathfrak{S}_r \longrightarrow \mathrm{Aut}({\mathbb{U}_d}^r) \\ \sigma \longmapsto ((\xi_1, \ldots, \xi_r) \mapsto (\xi_{\sigma^{-1}(1)}, \ldots, \xi_{\sigma^{-1}(r)})) \,. \end{cases}$$

Les deux produits semi-directs sont donc les mêmes et $\mathrm{G}(d, 1, r) \overset{\mathrm{gr.}}{\simeq} \mathrm{C}_d \wr \mathfrak{S}_r$.

l)

m) La famille $\left\{ (\mathrm{X}_1 \cdots \mathrm{X}_r)^d,\ \Sigma_k({\mathrm{X}_1}^{de}, \ldots, {\mathrm{X}_r}^{de}), \quad 1 \leqslant k \leqslant r-1 \right\}$ est une famille d'invariants algébriquement indépendants dont le produit des degrés est $|\mathrm{G}(de, e, r)|$. C'est donc une famille d'invariants fondamentaux pour le groupe $\mathrm{G}(de, e, r)$. Les degrés de $\mathrm{G}(de, e, r)$ sont donc $de, 2de, \ldots, (r-1)de, rd$.

n) $\mathrm{G}(de, e, r)$ est un groupe de Coxeter si et seulement si l'un de ses degrés est 2 (voir l'exercice12 de la feuille de TD 3).

Si $r = 1$, le degré de $\mathrm{G}(de, e, r)$ est d et donc $\mathrm{G}(de, e, 1)$ est de Coxeter si et seulement si $d = 2$.

Si $r = 2$ les degrés sont de et $2d$ et donc $\mathrm{G}(de, e, r)$ est de Coxeter si et seulement si $de = 2$ ou $d = 1$ c'est-à-dire si et seulement si ($d = 2$ et $e = 1$) ou $d = 1$.

Si $r \geqslant 3$ alors $rd \geqslant 3$ et donc $\mathrm{G}(de, e, r)$ est de Coxeter si et seulement si $de = 1$ ou $de = 2$.

Finalement $\mathrm{G}(de, e, r)$ est de Coxeter si et seulement si ($d = e = 1$ et $r \geqslant 2$ (groupe A_{r-1})) ou ($d = 2$ et $e = 1$ (groupe B_n)) ou ($d = 1$, $e = 2$ et $r \geqslant 2$ (groupe D_n)) ou ($r = 2$ et $d = 1$ (groupe $\mathrm{I}_2(e)$)) ou ($r = 1$ et $d = 2$ (groupe A_1)).

Corrigé

a) G_1 a pour cardinal $(2^3-1)(2^3-2)(2^3-2^2) = 168 = 7\times 3\times 2^3$. En effet, le cardinal de G_1 est celui de l'ensemble des bases de ${\mathbb{F}_2}^3$: il s'agit donc de choisir un vecteur non nul puis un vecteur qui n'est pas dans la droite engendré par le précédent et enfin un vecteur qui n'est pas dans le plan engendré par les deux premiers.

Soient u un élément d'ordre 2, π_u son polynôme minimal et χ_u son polynôme caractéristique. Comme u est d'ordre 2, on a $u^2 - \mathrm{id} = 0$ et donc π_u un diviseur de $X^2 - 1 = (X-1)^2$. Si $\pi_u = X - 1$ alors $u = \mathrm{id}$ n'est pas d'ordre 2. On en déduit que $\pi_u = (X-1)^2$ et donc $\chi_u = (X-1)^3$ puisque le polynôme caractéristique et le polynôme minimal de u ont les mêmes facteurs irréductibles. En dimension 3, les classes de conjugaison sont caractérisées par le polynôme minimal et le polynôme caractéristique. L'ensemble des éléments de G d'ordre 2 forme donc une classe de conjugaison dont un représentant est

$$u = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

On cherche alors les éléments v de G_1 qui commutent avec u. Un tel v laisse fixe $\mathrm{Im}\,(u - \mathrm{id}) = e_1$ et $\mathrm{Ker}\,(u - \mathrm{id}) = \mathrm{vect}\,(e_1, e_3)$. Il est donc de la forme

$$v = \begin{bmatrix} a & b & c \\ 0 & d & 0 \\ 0 & e & f \end{bmatrix}.$$

Le calcul $uv = vu$ donne $a = d$. Comme v doit être inversible, on obtient $a = d = 1$ sinon la première colonne est nulle. De plus, en développant le déterminant de v par rapport à la première colonne, on obtient $0 \neq \det v = f$ et donc $f = 1$. Finalement,

$$v = \begin{bmatrix} 1 & b & c \\ 0 & 1 & 0 \\ 0 & e & 1 \end{bmatrix}.$$

Il y a donc 8 éléments de G_1 qui commutent avec u et la classe de conjugaison de u a $168/8 = 21$ éléments.

b) Le sous-groupe $[H, H]$ de H est un sous-groupe distingué donc $[H, H] = H$ puisque H n'est pas commutatif. On a alors $\rho(H) = [\rho(H), \rho(H)] \subset [GL(V), GL(V)] \subset SL(V)$.

c) Raisonnons par l'absurde et considérons $\rho : H \to GL(V)$ une représentation irréductible sur $\mathbb{C}$ de dimension 2. Comme la dimension d'une représentation irréductible divise l'ordre du groupe, H a un élément g d'ordre 2. Par ailleurs, le noyau de ρ est un sous-groupe distingué de H. Comme H est simple, on a $\mathrm{Ker}\,\rho = \{1_H\}$ ou $\mathrm{Ker}\,\rho = H$. Dans le deuxième cas, H agit trivialement sur V et donc la représentation n'est pas irréductible puisque $\dim V = 2 > 1$. On en déduit que ρ est injective. En particulier, $\rho(g)$ est d'ordre 2 et donc son polynôme minimal π_g divise $X^2 - 1 = (X-1)(X+1)$. On a donc les possibilités suivantes.

(*i*) $\pi_g = X - 1$ et donc $\rho(g) = \mathrm{id}$ ce qui contredit le fait que $\rho(g)$ est d'ordre 2.
(*ii*) $\pi_g = X + 1$ et donc $\rho(g) = -\mathrm{id} \in Z\rho(H)$. Comme ρ est un isomorphisme de H sur $\rho(H)$, on obtient $g \in ZH$. Comme $g \neq 1_H$, cela contredit la simplicité de H.
(*iii*) $\pi_g = (X-1)(X+1)$. Comme π_g divise le polynôme caractéristique χ_g de $\rho(g)$ qui est de degré 2, on a $\chi_g = X^2 - 1$ et donc $\det \rho(g) = -1$ ce qui contredit la question **b**.

Les trois cas sont impossibles et on aboutit bien à une contradiction.

d) On utilise les résultats suivants :

(*i*) les dimensions des représentations irréductibles divisent l'ordre du groupe ;
(*ii*) la question **c**
(*iii*) le nombre ℓ de représentations irréductibles est égal au nombre de classe de conjugaison de G_1.
(*iv*) $|G_1| = {n_1}^2 + \cdots + {n_\ell}^2$ où les n_i sont les dimensions des représentations irréductibles de G_1.

Commençons par déterminer le nombre de classes de conjugaison de G_1. On est en dimension 3, donc une classe de conjugaison est déterminée par son polynôme minimal et son polynôme caractéristique. Pour $u \in G_1$, on note π_u son polynôme minimal et χ_u son polynôme caractéristique. Le polynôme χ_u est alors unitaire de degré 3 et son terme constant n'est pas nul puisque u est inversible. On a donc les possibilités suivantes pour χ_u

(*i*) $\chi_u = X^3 + X^2 + 1$;

(*ii*) $\chi_u = \mathrm{X}^3 + \mathrm{X} + 1$;
(*iii*) $\chi_u = \mathrm{X}^3 + \mathrm{X}^2 + \mathrm{X} + 1 = (\mathrm{X}-1)^3$;
(*iv*) $\chi_u = \mathrm{X}^3 + 1 = (\mathrm{X}-1)(\mathrm{X}^2 + \mathrm{X} + 1)$.

Dans les cas (*i*) et (*ii*), χ_u est irréductible sur $\mathbb{F}_2$ puisqu'il est de degré 3 et n'a pas de racines dans $\mathbb{F}_2$. Comme $\pi_u \mid \chi_u$, on en déduit que $\pi_u = \chi_u$ et chacun des deux polynômes détermine une classe de conjugaison.

Dans le cas (*iii*), on a $\pi_u = \chi_u$. En effet, $\mathrm{X}^2 + \mathrm{X} + 1$ est irréductible sur $\mathbb{F}_2$ car il est de degré 3 et n'a pas de racines dans $\mathbb{F}_2$. Comme le polynôme minimal et le polynôme caractéristique font intervenir les mêmes facteurs irréductibles, on a l'égalité voulue et donc une nouvelle classe de conjugaison.

Dans le cas (*iv*), on a $\pi_u = (\mathrm{X}-1)$ ou $\pi_u = (\mathrm{X}-1)^2$ ou $\pi_u = (\mathrm{X}-1)^3$ ce qui donne trois nouvelles classes de conjugaison.

On obtient ainsi 6 classes de conjugaison et donc 6 représentations irréductibles.

On suppose que $n_1 \leqslant \cdots \leqslant n_6$. Comme $13^2 = 169 > |\mathrm{G}_1| = 168$, on obtient $n_i < 13$. De plus, n_i divise $|\mathrm{G}_1|$ donc $n_i \in \{1,2,3,4,6,7,8,12\}$. La question **c** montre alors que $n_i \in \{1,3,4,6,7,8,12\}$. Enfin, comme G_1 est simple, la seule représentation irréductible de dimension 1 de G est la représentation triviale. On en déduit que $n_i \in \{3,4,6,7,8,12\}$ pour $i \geqslant 2$.

Montrons que $n_6 = 8$. Si $n_6 = 12$ alors $36 = 4 \cdot 3^2 \leqslant {n_2}^2 + {n_3}^2 + {n_4}^2 + {n_5}^2 = 168 - 1 - 144 = 23$. Si $n_6 \leqslant 4$ alors ${n_2}^2 + {n_3}^2 + {n_4}^2 + {n_5}^2 + {n_6}^2 = 167 \leqslant 5 \cdot 4^2 = 80$. Si $n_6 = 6$ alors par raison de parité $n_2 = 3$ et on a ${n_3}^2 + {n_4}^2 + {n_5}^2 = 122 \leqslant 3 \cdot 6^2 = 108$. Ces trois inégalités étant absurdes, on en déduit que $n_6 \in \{7,8\}$. Il reste donc à écarter le cas $n_6 = 7$. Si $n_6 = 7$ alors ${n_2}^2 + {n_3}^2 + {n_4}^2 + {n_5}^2 = 118$. On ne peut avoir $n_4 = 7$, sinon on aurait $n_5 = 7$ et ${n_2}^2 + {n_3}^2 = 20$. Cela imposerait alors $n_2, n_3 \in \{3,4\}$ et $20 = {n_2}^2 + {n_3}^2 \in \{18,25,32\}$ ce qui est absurde. Ainsi, si $n_6 = 7$ alors $n_4 \in \{3,4,6\}$. Si $n_5 = 7$ alors ${n_2}^2 + {n_3}^2 + {n_4}^2 = 69$ et $n_2, n_3, n_4 \in \{3,4,6\}$. Par raison de parité, on a nécessairement $n_2 = 3$ et donc ${n_3}^2 + {n_4}^2 = 60$. Mais ${n_3}^2 + {n_4}^2 \in \{18,25,32,45,52,72\}$ et donc $n_5 \in \{3,4,6\}$. Si $n_2 = 3$ alors par raison de parité, on a aussi $n_3 = 3$ et donc ${n_4}^2 + {n_5}^2 = 100 \leqslant 6^2 + 6^2 = 72$. On en déduit que $n_2 \in \{4,6\}$. On a alors $n_i \in \{4,6\}$ pour $2 \leqslant i \leqslant 5$ et donc $118 = {n_2}^2 + {n_3}^2 + {n_4}^2 + {n_5}^2 \in \{64,84,104,124,144\}$. Finalement $n_6 \neq 7$ et donc $n_6 = 8$.

Montrons à présent que $n_5 = 7$. Comme $n_6 = 7$, il reste ${n_2}^2 + {n_3}^2 + {n_4}^2 + {n_5}^2 = 103$. Si $n_5 = 8$ alors ${n_2}^2 + {n_3}^2 + {n_4}^2 = 39 < 49$ donc $n_4 \leqslant 6$. Par parité, on a alors $n_2 = 3$ et donc ${n_3}^2 + {n_4}^2 = 30$. On en déduit que $n_4 \leqslant 4$. Ainsi $30 = {n_3}^2 + {n_4}^2 \in \{18,25,32\}$ et donc $n_5 \neq 8$. Si $n_5 = 6$ alors par parité, on a $n_2 = 3$ et donc ${n_3}^2 + {n_4}^2 = 58 \in \{18,25,32,45,52,72\}$ ce qui donne $n_5 \neq 6$. Si $n_5 \leqslant 4$ alors $103 = {n_2}^2 + {n_3}^2 + {n_4}^2 + {n_5}^2 \leqslant 4 \cdot 4^2 = 64$. Finalement $n_5 = 7$ et ${n_2}^2 + {n_3}^2 + {n_4}^2 = 54$.

Montrons que $n_4 = 6$. Si $n_4 \leqslant 4$ alors $54 = {n_2}^2 + {n_3}^2 + {n_4}^2 \leqslant 3 \cdot 4^2 = 48$. On en déduit que $n_4 \in \{6,7\}$. Si $n_4 = 7$ alors ${n_2}^2 + {n_3}^2 = 5$ ce qui est absurde puisque $n_2 \geqslant 3$. On obtient bien $n_4 = 6$.

On a alors ${n_2}^2 + {n_3}^2 = 18$ et donc $n_2 = n_3 = 3$. Finalement, les dimensions des représentations irréductibles de G_1 sont $1, 3, 3, 6, 7$ et 8.

e) On a vu dans la question **c** que ρ est injectif. L'élément $\rho(y)$ est donc d'ordre 2 c'est-à-dire une symétrie. D'après la question **b**, $\rho(y)$ de déterminant 1. On en déduit qu'il existe une base dans laquelle la matrice de $\rho(y)$ est $\mathrm{diag}\,(-1,-1,1)$. On a donc bien $\mathrm{tr}\,(\rho(y)) = -1$ et $-\rho(y)$ est une réflexion.

f) On a bien sûr $\mathrm{G} \subset \pm\rho(\mathrm{G}_1)$. De plus, d'après la question **b**, $\rho(\mathrm{G}_1) \subset \mathrm{SL}_3(\mathbb{C})$, d'où $-\mathrm{id} \notin \rho(\mathrm{G}_1)$. On en déduit que $\pm\rho(\mathrm{G}_1) = \mathrm{G}_1 \times \{-1,1\}$. Par ailleurs, on considère dans G_1 les éléments d'ordre 2

$$u = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}, \qquad v = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \qquad \text{et} \qquad w = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}.$$

Ils vérifient $uvw = \mathrm{Id}_3$. On obtient ainsi $(-\rho(u))(-\rho(v))(-\rho(w)) = -\mathrm{id} \in \mathrm{G}$. De plus, $\mathrm{G}_1 = \mathrm{SL}_3(\mathbb{F}_2)$ est engendré par les transvections qui sont d'ordre 2 puisqu'on travaille sur $\mathbb{F}_2$. On en déduit que $\rho(\mathrm{G}_1)$ est engendré par les $\rho(y)$ pour y d'ordre 2. Comme $\rho(y) = (-\rho(y))(-\mathrm{id}) \in \mathrm{G}$ pour y d'ordre 2, on en déduit que $\rho(\mathrm{G}_1) \subset \mathrm{G}$. Finalement comme $-\mathrm{id} \in \mathrm{G}$, on a aussi $-\rho(\mathrm{G}_1) \subset \mathrm{G}$ et donc $\mathrm{G} = \pm\rho(\mathrm{G}_1) = \rho(\mathrm{G}_1) \times \{-1,1\}$.

On a alors $\det \mathrm{G} \subset \{-1,1\}$. Les réflexions de G sont donc nécessairement d'ordre 2 et contenu dans $-\mathrm{G}_1$. Il s'agit donc de l'ensemble $\{-\rho(y), y \text{ d'ordre } 2\}$ qui est de cardinal 21 puisque ρ est injectif (question **a**).

g) On note $d_1 \leqslant d_2 \leqslant d_3$ les invariants caractéristiques de G. On a alors

$$d_1 d_2 d_3 = 2 \cdot 168 = 336 \qquad \text{et} \qquad d_1 + d_2 + d_3 = 24.$$

De plus, G agit de façon irréductible sur $\mathbb{C}^3$ puisque c'est déjà le cas pour G_1. On en déduit que $d_i \geqslant 2$ et donc $d_i \leqslant 20$. On a aussi $d_3 > 8$ puisque $24 = d_1 + d_2 + d_3 \leqslant 3d_3$ et si $d_3 = 8$ alors $d_1 = d_2 = d_3 = 8$

et $336 = 8^3 = 2^9$ ce qui est absurde. Comme d_3 est un diviseur de 336, on a $d_3 \in \{12, 14, 16\}$. Si $d_3 = 12$ alors $d_1 + d_2 = 12$ et $d_1 d_2 = 28$ mais le polynôme $\mathrm{X}^2 - 12\mathrm{X} + 28$ n'a pas de racines entières. Si $d_3 = 16$ alors $d_1 + d_2 = 8$ et $d_1 d_2 = 21$ mais le polynôme $\mathrm{X}^2 - 8\mathrm{X} + 21$ n'a pas de racines entières. Donc $d_3 = 14$ et $d_1 + d_2 = 10$ et $d_1 d_2 = 24$. Ainsi d_1 et d_2 sont racines de $\mathrm{X}^2 - 10\mathrm{X} + 24$ ce qui donne $d_1 = 4$ et $d_2 = 6$ et $d_3 = 14$. Le groupe G n'est donc pas un groupe de Coxeter puisque $d_i \neq 2$ pour tout i.

h) On suppose que G est imprimitif. Comme G agit sur un espace de dimension 3, on obtient une décomposition de $\mathbb{C}^3$ de la forme $\mathbb{C}^3 = \mathrm{V}_1 \oplus \mathrm{V}_2$ avec $\dim \mathrm{V}_i = i$ ou de la forme $\mathbb{C}^3 = \mathrm{V}_1 \oplus \mathrm{V}_2 \oplus \mathrm{V}_3$ avec $\dim \mathrm{V}_i = 1$. Dans le premier type de décomposition, les sous-espaces V_i sont stables par G par raison de dimension. Comme G agit de façon irréductible sur $\mathbb{C}^3$, la première situation est impossible. On en déduit qu'il existe un morphisme $\delta : \mathrm{G} \to \mathfrak{S}_3$. De plus, $\delta(\mathrm{G})$ est un sous-groupe transitif sur $\{1, 2, 3\}$ car G agit de façon irréductible. Ainsi $\delta(\mathrm{G}) = \mathfrak{S}_3$ ou $\delta(\mathrm{G}) = \mathfrak{A}_3 = \mathbb{Z}/3\mathbb{Z}$. Comme la suite de Jordan-Hölder de $\mathfrak{S}_3$ est $(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z})$, on en déduit que G a un terme $\mathbb{Z}/3\mathbb{Z}$ dans sa suite de Jordan-Hölder. Mais, comme G_1 est simple, la suite de Jordan-Hölder de G est $(\mathbb{Z}/2\mathbb{Z}, \mathrm{G}_1)$ ce qui donne une contradiction. Le groupe G est donc primitif. On regarde alors la classification de Shephard et Todd et grâce aux d_i, on trouve G_{24}.