Dualité de Pontrjagin pour les groupes finis

On note $\mathbb{U} \subset \mathbb{C}$ l'ensemble des complexes de module 1. Soit G un groupe abélien fini, et $\pi : G \to GL(V)$ une représentation de G sur un espace vectoriel complexe de dimension finie. On munit V d'un produit scalaire hermitien quelconque $\langle \cdot , \cdot \rangle$.

1. On munit V d'un nouveau produit scalaire en posant

$$(\zeta|\xi) = \frac{1}{|G|} \sum_{g \in G} \langle \pi(g)\zeta, \pi(g)\xi \rangle.$$

   On note $U(V)$ le groupe unitaire de V relativement à ce produit scalaire.

   (a) Vérifier que la formule ci-dessus définit bien un produit scalaire sur V.

   (b) Vérifier que $\pi(g) \in U(V)$ pour tout $g \in G$.

2. (a) Soit $g \in G$. Dire pourquoi $\pi(g)$ est diagonalisable. Justifier l'existence d'une base (e_i) de V formée de vecteurs propres communs à tous les $\pi(g)$.

   (b) Montrer qu'il existe des représentations de G de dimension 1, $\alpha_1, \cdots, \alpha_n$, telles que π soit équivalente à $\alpha_1 \oplus \cdots \oplus \alpha_n$.

   Comme les représentations de dimension 1 sont évidemment irréductibles, cela montre que toutes les représentations de G se décomposent en sommes de représentations irréductibles. Cela est encore vrai pour les groupes finis, ou compacts, non nécessairement abéliens, mais les dimensions irréductibles ne sont plus nécessairement de dimension 1. On a vu en cours que cela est également vrai pour les (coreprésentations des) algèbres de Hopf admettant une forme invariante unifère.

3. On note $\hat{G} = \mathrm{Mor}(G, \mathbb{U})$ l'ensemble des morphismes de groupes $\alpha : G \to \mathbb{U}$. Les éléments de $\hat{G}$ s'appellent les caractères de G.

   (a) Montrer que $\hat{G}$ est un groupe pour le produit des fonctions.
   Monter que $\hat{G}$ coïncide avec $\mathrm{Mor}(G, \mathbb{C}^*)$, en utilisant la question 1.

   (b) On définit une application $\phi : G \mapsto \mathrm{Mor}(\hat{G}, \mathbb{U})$ en posant $\phi(g)(\alpha) = \alpha(g)$.
   Montrer que ϕ est un morphisme de groupes.

4. On considère la représentation régulière droite λ de G sur le $\mathbb{C}$-espace vectoriel $V = \mathbb{C}^G$ définie par la formule $\rho(g)(f) = (h \mapsto f(hg))$.

   (a) Vérifier que ρ est une représentation de g.

   (b) Montrer que $f \in \mathbb{C}^G$ est vecteur propre commun aux $\rho(g)$ **ssi** f est multiple non nul d'un élément de $\hat{G}$.

5. (a) En utilisant la question précédente, montrer que les éléments de $\hat{G}$ forment une famille génératrice dans V. En déduire que ϕ est injective.

   (b) Montrer que les éléments de $\hat{G}$ sont des « group-like » dans l'algèbre de Hopf des fonctions sur G. En déduire qu'ils forment une famille libre dans V.

   (c) Montrer que $\mathrm{Card}\,\hat{G} = \mathrm{Card}\,G$ et que ϕ est un isomorphisme.

   C'est le théorème de bidualité de Pontrjagin, dans le cas particulièrement simple des groupes finis. Il s'étend au cas des groupes abéliens localement compacts, en considérant les caractères continus, et en munissant $\hat{G}$ d'une topologie localement compacte naturelle. On a vu en cours que la dualité des algèbres de Hopf de dimension finie permet d'étendre la dualité de Pontrjagin au cas des groupes finis non nécessairement abéliens.

6. On considère le cas $G = \mathbb{Z}/n\mathbb{Z}$. Montrer que $\hat{G} \simeq \mathbb{Z}/n\mathbb{Z}$.

   Il résulte de la classification des groupes abéliens finis que $G \simeq \hat{G}$ pour tout G abélien fini, mais cet isomorphisme est non canonique, au contraire de l'isomorphisme ϕ entre G et son bidual. Dans le cas localement compact, ou dans le cas des algèbres de Hopf, G et $\hat{G}$ ne sont plus isomorphes.

Quelques représentations de $SU(2)$

On note $\mathbb{U} \subset \mathbb{C}$ l'ensemble des complexes de module 1. On note $SU(2) \in M_2(\mathbb{C})$ le groupe des matrices unitaires de déterminant 1. On note $V_n \subset \mathbb{C}[X, Y]$ l'espace des polynômes de deux variables homogènes de degré n.

1. Vérifier que $(X^k Y^{n-k})_k$ est une base de V_n. Quelle est la dimension de V_n ?
   On définit une représentation π_n de $SU(2)$ sur V_n en posant
   $$\pi_n(g)(P) = P(aX + cY, bX + dY) \quad \text{pour} \quad g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$
   Vérifier que π_n est bien une représentation.
2. Pour tout $z \in \mathbb{U}$ on note $d_z = \begin{pmatrix} z & 0 \\ 0 & \bar{z} \end{pmatrix}$. Soit $P = \sum_0^n a_k X^k Y^{n-k}$ un élément de V_n.
   (a) Montrer que $W_P = \mathrm{Vect}\{\pi_n(d_z)(P) \mid z \in \mathbb{U}\} \subset V_n$ est stable par $\pi_n(d_z)$ pour tout z.
   (b) Calculer $z^{n-2i}\pi_n(d_z)(P)$ pour tout $i \in \{0, \ldots, n\}$.
   (c) Montrer que $a_i X^i Y^{n-i} \in W_P$ pour tout i.
3. Soit $W \subset V_n$ un sous-espace non nul invariant par π_n.
   (a) Montrer que W contient un monôme $X^i Y^{n-i}$.
   (b) Trouver un élément $g \in SU(2)$ tels que le coeff. de X^n dans $\pi_n(g)(X^i Y^{n-i})$ soit non nul. Trouver un élément $h \in SU(2)$ tels que tous les coefficents de $\pi_n(h)(X^n)$ soient non nuls.
   (c) Montrer que $W = V_n$. Ainsi π_n est irréductible.
4. On fixe m, $n \geq 1$ et on considère les applications $\phi : V_{m-1} \otimes V_{n-1} \to V_m \otimes V_n$, $P \otimes Q \mapsto (X \otimes Y - Y \otimes X)(P \otimes Q)$, et $\psi : V_n \otimes V_m \to V_{n+m}$, $P \otimes Q \mapsto PQ$.
   (a) Montrer que $X \otimes Y - Y \otimes X$ est un vecteur fixe de $V_1 \otimes V_1$. Vérifier que ϕ et ψ entrelacent les représentations de $SU(2)$.
   (b) Montrer que la suite $0 \to V_{m-1} \otimes V_{n-1} \to V_m \otimes V_n \to V_{n+m} \to 0$ est exacte, c'est-à-dire : ϕ est injective, ψ est surjective, et $\mathrm{Ker}\, \psi = \mathrm{Im}\, \phi$.
   (c) En déduire qu'on a $\pi_n \otimes \pi_m \simeq \pi_{|n-m|} \oplus \pi_{|n-m|+2} \oplus \cdots \oplus \pi_{n+m}$.

   On peut en fait montrer que toute représentation irréductible de $SU(2)$ est équivalente à l'une des représentations π_n. On peut aussi réaliser ces représentations d'une autre manière :
5. Soit $E_1 = \mathbb{C}^2$, $E_n = E_1^{\otimes n}$. On définit une représentation σ_n de $\mathfrak{S}_n$ sur E_n en posant
   $$\sigma_n(\tau)(\zeta_1 \otimes \cdots \otimes \zeta_n) = \zeta_{\tau^{-1}(1)} \otimes \cdots \otimes \zeta_{\tau^{-1}(n)}.$$
   Soit $F_n \subset E_n$ l'espace des vecteurs fixes pour σ_n.
   (a) Montrer que $S = \frac{1}{n!} \sum_{\tau \in \mathfrak{S}_n} \sigma_n(\tau)$ est une projection d'image F_n.
   (b) Soit (e_1, e_2) la base canonique de $\mathbb{C}^2$. On pose
   $$f_k = S(e_1 \otimes \cdots \otimes e_1 \otimes e_2 \otimes \cdots \otimes e_2),$$
   où e_1 apparaît k fois. Montrer que (f_k) est une base de F_n.
6. Soit ρ_1 la représentation canonique de $SU(2)$ sur $\mathbb{C}^2 = E_1$, et
   $$\rho_n(g) = \rho_1(g) \otimes \cdots \otimes \rho_1(g) \in GL(E_n).$$
   (a) Montrer que $\rho_n(g)\sigma_n(\tau) = \sigma_n(\tau)\rho_n(g)$ pour tous $g \in SU(2)$, $\tau \in \mathfrak{S}_n$. En déduire que F_n est stable pour ρ_n.
   (b) Montrer que la restriction de ρ_n à F_n est équivalente à π_n.

Algèbres de Taft et q-nombres

Le corps de base est $\mathbb{C}$. Les algèbres et morphismes d'algèbres considérés sont unifères.

1. On fixe $q \in \mathbb{C}^*$. On pose $(n)_q = 1 + q + \cdots + q^{n-1}$ pour tout $n \in \mathbb{N}^*$, et $(0)_q = 0$: ce sont les « q-nombres ». On introduit les q-factorielles et les q-coefficients binômiaux comme suit :

$$(0)!_q = 1, \qquad (n)!_q = (n)_q(n-1)_q \cdots (1)_q, \qquad \binom{k}{l}_q = \frac{(k)!_q}{(l)!_q(k-l)!_q}.$$

   (a) Montrer que les q-coefficients binômiaux sont bien définis pour tous entiers $0 \leq l \leq k$ si q n'est pas une racine de l'unité. Quelles restrictions faut-il imposer à k, l si q est une racine primitive n^{e} de l'unité ?

   (b) Démontrer la q-identité de Pascal pour $1 \leq l \leq k$:

$$\binom{k-1}{l-1}_q + q^l \binom{k-1}{l}_q = \binom{k}{l}_q.$$

   Lorsque q est une racine n^e de l'unité, on peut utiliser la q-identité de Pascal pour définir les q-coefficients binômiaux, par récurrence.

   (c) Soit a, b deux éléments d'une algèbre tels que $ba = qab$. Démontrer la q-formule du binôme, pour tout $k \in \mathbb{N}^*$:

$$(a+b)^k = \sum_{l=0}^{k} \binom{k}{l}_q a^l b^{k-l}.$$

   Qu'obtient-on pour $k = n$, si q est une racine primitive n^{e} de l'unité ?

2. On fixe une un entier $n \geq 2$ et une racine primitive n^{e} de l'unité q. On considère l'algèbre $T_n(q)$ définie par générateurs et relations :

$$T_n(q) = \langle x, g \mid g^n = 1,\ x^n = 0,\ xg = qgx \rangle_{\text{alg}}.$$

   (a) On note $(e_i)_{i=0}^{n-1}$ la base canonique de $\mathbb{C}^n$ et on considère les endomorphismes σ, τ de $E = \mathbb{C}^n \otimes \mathbb{C}^n$ définis comme suit :

$$\sigma(e_i \otimes e_j) = e_{i+1} \otimes e_j, \quad \sigma(e_{n-1} \otimes e_j) = e_1 \otimes e_j,$$
$$\tau(e_i \otimes e_j) = q^i e_i \otimes e_{j+1}, \quad \tau(e_i \otimes e_{n-1}) = 0.$$

   Montrer qu'il existe un unique morphisme d'algèbres $\phi : T_n(q) \to L(E)$ tel que $\phi(g) = \sigma$ et $\phi(x) = \tau$. Calculer $\sigma^k \tau^l (e_0 \otimes e_0)$ pour tous $0 \leq k, l \leq n-1$.

   (b) Montrer que $(g^k x^l)_{0 \leq k,l \leq n-1}$ est une base de $T_n(q)$.

3. On considère les éléments suivants de $T_n(q) \otimes T_n(q)$ et $T_n(q)$:

$$G = g \otimes g, \quad X = 1 \otimes x + x \otimes g, \quad \tilde{g} = g^{-1}, \quad \tilde{x} = -xg^{-1}.$$

   (a) Montrer qu'il existe un unique morphisme d'algèbre $\Delta : T_n(q) \to T_n(q) \otimes T_n(q)$ tel que $\Delta(g) = G$ et $\Delta(x) = X$.
   Procéder de même avec $\epsilon : T_n(q) \to \mathbb{C}$ vérifiant $\epsilon(g) = 1$, $\epsilon(x) = 0$.

   (b) Démontrer les identités $(\Delta \otimes \text{id})\Delta = (\text{id} \otimes \Delta)\Delta$ et $(\epsilon \otimes \text{id})\Delta = (\text{id} \otimes \epsilon)\Delta = \text{id}$.

   (c) Montrer qu'il existe un unique morphisme d'algèbre $S : T_n(q) \to T_n(q)^{\text{op}}$ tel que $S(g) = \tilde{g}$ et $S(x) = \tilde{x}$. Démontrer que $m(\text{id} \otimes S)\Delta(a) = m(S \otimes \text{id})\Delta(a) = \epsilon(a)1$ pour tout $a \in T_n(q)$. *On pourra commencer par $a = g$, $a = x$, puis montrer que l'identité est vérifiée pour $a = bc$ si elle l'est pour b et c.*

   (d) Vérifier que S est bijective et calculer son ordre.

4. Déterminer l'espace des formes ϕ invariantes à droite sur $T_n(q)$. *On pourra chercher des conditions nécessaires sur ϕ en calculant $(\phi \otimes \text{id})\Delta(g^k x^l)$, qui doit être proportionnel à 1.*

Les « algèbres de Taft » $T_n(q)$ jouent un rôle non négligeable dans la classifications des algèbres de Hopf de dimension finie sur $\mathbb{C}$. Plus précisément on peut montrer qu'une algèbre de Hopf sur $\mathbb{C}$ de dimension p^2 avec p premier est nécessairement de la forme $\mathbb{C}[\mathbb{Z}/p^2\mathbb{Z}]$, $\mathbb{C}[\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}]$ ou $T_p(q)$.

Dualité de Pontrjagin pour les groupes finis (corrigé)

1a) La formule définit clairement une forme sesquilinéaire hermitienne. De plus pour $\zeta \in V$, $\zeta \neq 0$ on a $\pi(g)\zeta \neq 0$ car $\pi(g)$ est inversible, donc $\langle \pi(g)\zeta, \pi(g)\zeta \rangle > 0$ pour tout g, donc $(\zeta|\zeta) > 0$.

1b) On remarque que si h est un élément fixé de G et g parcourt G, alors gh parcourt également G. Ainsi $\pi(h)$ ne modifie pas le produit scalaire :

$$(\pi(h)\zeta|\pi(h)\xi) = \sum_{g \in G} \langle \pi(gh)\zeta, \pi(gh)\xi \rangle = (\zeta|\xi).$$

2a) Les endomorphismes $\pi(g)$ sont diagonalisables car unitaires. De plus ils sont codiagonalisables car ils commutent deux-à-deux : on a $\pi(g)\pi(h) = \pi(gh) = \pi(hg) = \pi(h)\pi(g)$ car G est abélien. Remarque : on peut aussi montrer que les $\pi(g)$ sont diagonalisables sans utiliser la première question, en remarquant que si n est l'ordre de g dans G alors $X^n - 1$ est un polynôme annulateur à racines simples de $\pi(g)$.

2b) Par construction de la base de vecteurs propres (e_i) il existe pour tout i et pour tout g un scalaire $\alpha_i(g)$ tel que $\pi(g)(e_i) = \alpha_i(g)e_i$. Ce scalaire est non nul car $\pi(g)$ est inversible, et il vaut 1 quand g est l'élément neutre de G car $\pi(g) = \mathrm{id}$. En fait $\alpha_i : G \to \mathbb{C}^*$ est un morphisme de groupes :

$$\alpha_i(g)\alpha_i(h)e_i = \alpha_i(g)\pi(h)(e_i) = \pi(h)(\alpha_i(g)e_i) = \pi(h)\pi(g)(e_i) = \pi(hg)(e_i) = \alpha_i(hg)e_i,$$

donc $\alpha_i(hg) = \alpha_i(g)\alpha_i(h) = \alpha_i(h)\alpha_i(g)$.

Modulo l'identification $\mathbb{C}^* \simeq GL(\mathbb{C})$, les α_i définissent donc des représentations de G sur $\mathbb{C}$, et $\alpha = \alpha_1 \oplus \cdots \oplus \alpha_n$ est une représentation de G sur $\mathbb{C}^n$. Soit $u \in L(\mathbb{C}^n, V)$ l'isomorphisme définit par $u(\lambda_1, \ldots, \lambda_n) = \lambda_1 e_1 + \cdots + \lambda_n e_n$. Cet isomorphisme établit une équivalence entre les représentations α et π car

$$\begin{aligned} u \circ \alpha(g)(\lambda_1, \ldots, \lambda_n) &= u(\alpha_1(g)\lambda_1, \ldots, \alpha_n(g)\lambda_n) = \alpha_1(g)\lambda_1 e_1 + \cdots + \alpha_n(g)\lambda_n e_n \\ &= \pi(g)(\lambda_1 e_1) + \cdots + \pi(g)(\lambda_n e_n) = \pi(g) \circ u(\lambda_1, \ldots, \lambda_n). \end{aligned}$$

3a) L'ensemble des fonctions de G dans $\mathbb{U}$ est un groupe car c'est le cas de $\mathbb{U}$. Il faut donc vérifier que $\mathrm{Mor}(G, \mathbb{U})$ en est un sous-groupe. La fonction constante 1 est clairement un morphisme de groupes donc appartient à $\mathrm{Mor}(G, \mathbb{U})$. Par ailleurs si f, $g \in \mathrm{Mor}(G, \mathbb{U})$ on a

$$(fg)(hk) = f(hk)g(hk) = f(h)f(k)g(h)g(k) = f(h)g(h)f(k)g(k) = (fg)(h)(fg)(k)$$

et $(fg)(1) = f(1)g(1) = 1$ donc $fg \in \mathrm{Mor}(G, \mathbb{U})$. De même $f^{-1} = (h \mapsto f(h)^{-1}) \in \mathrm{Mor}(G, \mathbb{U})$.

Par ailleurs, si $f \in \mathrm{Mor}(G, \mathbb{C}^*)$ la question 1 montre l'existence d'une constante $c = (1|1)$ telle que $|f(g)|^2 = (f(g)1|f(g)1) = c$ pour tout g. Mais comme $f(e) = 1$ on doit avoir $c = 1$, donc f prend ses valeurs dans $\mathbb{U}$. On peut aussi invoquer l'argument suivant : comme G est fini, pour tout $g \in G$ il existe $n \in \mathbb{N}^*$ tel que $g^n = e$, on a alors $f(g)^n = 1$ donc $f(g) \in \mathbb{U}$.

3b) Pour tous $\alpha \in \mathrm{Mor}(G, \mathbb{U})$, g, $h \in G$ on a, par définition du produit de $\mathrm{Mor}(\hat{G}, \mathbb{U})$, l'égalité suivante qui montre que ϕ est multiplicative :

$$\phi(gh)(\alpha) = \alpha(gh) = \alpha(g)\alpha(h) = \phi(g)(\alpha)\phi(h)(\alpha) = (\phi(g)\phi(h))(\alpha).$$

Par ailleurs $\phi(e)(\alpha) = \alpha(e) = 1$, or la fonction constante 1 est l'élément neutre de $\mathrm{Mor}(\hat{G}, \mathbb{U})$.

4a) Il est clair que $\rho(e) = \mathrm{id}$. De plus

$$\rho(gh)(f) = (k \mapsto f(kgh)) = \rho(g)(k \mapsto f(kh)) = \rho(g)\rho(h)(f).$$

4b) Si $f \in \mathrm{Mor}(G, \mathbb{U})$ on a $\rho(g)(f) = (h \mapsto f(hg)) = (h \mapsto f(h)f(g)) = f(g)f$ donc f est bien vecteur propre de tous les $\rho(g)$. Inversement, si f est un tel vecteur propre, il existe pour tout g un scalaire $\alpha(g)$ tel que $f(hg) = \alpha(g)f(h)$ pour tout h, et comme à la question 2b) on voit que α est un morphisme de G dans $\mathbb{C}^*$, donc un élément de $\mathrm{Mor}(G, \mathbb{U})$ d'après 3a). De plus en prenant $h = e$ dans l'identité précédente on obtient $f = f(e)\alpha$.

5a) D'après la question 2a), il existe une base de V formée de vecteurs propres communs aux $\rho(g)$, donc également une base formée d'éléments de $\hat{G}$ d'après 4b). En particulier $\hat{G}$ est une famille génératrice de V. Prenons maintenant un élément $g \in G$ tel que $\phi(g) = 1$: autrement dit on a $\alpha(g) = 1 = \alpha(e)$ pour tout $\alpha \in \hat{G}$. Par linéarité on a alors $f(g) = f(e)$ pour toute fonction $f \in V$, ce qui implique que $g = e$: ϕ est injective.

5b) Pour $\alpha \in \hat{G}$ on a $\Delta(\alpha)(g, h) = \alpha(gh) = \alpha(g)\alpha(h) = (\alpha \otimes \alpha)(g, h)$ en identifiant $V \otimes V$ aux fonctions de deux variables sur G. Ainsi les éléments de $\hat{G}$ sont des group-like de V, donc ils forment une famille libre d'après le cours.

5c) Les deux questions précédentes montrent que $\hat{G}$ est une base de V, donc $\operatorname{Card} \hat{G} = \dim V = \operatorname{Card} G$. En particulier ϕ est une application injective entre deux ensembles de même cardinal, donc elle est bijective, donc c'est un isomorphisme.

6) On note additivement la loi de $\mathbb{Z}/n\mathbb{Z}$. L'application $\psi : \hat{G} \to \mathbb{C}^*$, $\alpha \mapsto \alpha(\bar{1})$ est clairement un morphisme de groupes. Montrons qu'elle est injective et que son image est l'ensemble $\mathbb{U}_n$ des racines n^{es} de l'unité. L'injectivité résulte de l'identité $\alpha(\bar{k}) = \alpha(\bar{1})^k$ pour tout k. Par ailleurs $\alpha(\bar{1})^n = \alpha(\bar{n}) = \alpha(\bar{0}) = 1$ donc $\alpha(\bar{1}) \in \mathbb{U}_n$ pour tout α. Enfin si $\omega \in \mathbb{U}_n$ on définit un antécédent de ω par ψ en posant $\alpha(\bar{k}) = \omega^k$ pour tout k.

Quelques représentations de $SU(2)$ (corrigé)

1) Il est clair que $(X^k Y^{n-k})$ est une base de V_n, qui est donc de dimension $n+1$. Pour tout $g \in SU(2)$ on vérifie que $\pi_n(g)$ est linéaire :

$$\begin{aligned}\pi_n(g)(P + \lambda Q) &= (P + \lambda Q)(aX + cY, bX + dY) \\ &= P(aX + cY, bX + dY) + \lambda Q(aX + cY, bX + dY) = \pi_n(g)(P) + \lambda \pi_n(g)(Q).\end{aligned}$$

Par ailleurs on a clairement $\pi_n(e) = \mathrm{id}$, et le calcul suivant montre que π_n est à valeurs dans $GL(V_n)$ et un morphisme de groupes :

$$\begin{aligned}\pi_n(g)\pi_n(g')(P) &= \pi_n(g)P(a'X + c'Y, b'X + d'Y) \\ &= P(a'(aX + cY) + c'(bX + dY), b'(aX + cY) + d'(bX + dY)) \\ &= P((aa' + bc')X + (ca' + dc')Y, (ab' + bd')X + (cb' + dd')Y),\end{aligned}$$

or $aa' + bc'$, $ca' + dc'$, $ab' + bd'$ et $cb' + dd'$ sont les coefficients de la matrice gg'.

Remarque : on voit que π_n définit en fait une représentation de $GL(2)$ sur V_n.

2a) On a $\pi_n(d_z)\pi_n(d_{z'})(P) = \pi_n(d_z d_{z'})(P) = \pi_n(d_{zz'})(P)$ pour tout $z' \in \mathbb{U}$, donc W_p est stable par $\pi_n(d_z)$ si $z \in \mathbb{U}$.

2b) Un calcul immédiat donne

$$z^{n-2i}\pi_n(d_z)(P) = \textstyle\sum_{k=0}^n a_k z^{2(k-i)} X^k Y^{n-k}. \tag{1}$$

2c) L'idée est de sommer l'identité précédente sur un certain ensemble de racines de l'unité. En effet si z est une racine pq^{e} de l'unité, alors z^p est une racine q^{e} de l'unité, et si $p \neq 0$, $q \geq 2$ on a

$$\textstyle\sum_{z \in \mathbb{U}_{pq}} z^p = p \sum_{z \in \mathbb{U}_q} z = 0.$$

Posons alors $N = 2 \operatorname{ppcm}\{2(k-i) \mid 0 \leq k \leq n,\ k \neq i\}$ et sommons (1) en faisant varier z dans $\mathbb{U}_N$. Le membre de gauche est clairement dans W_P. Dans le membre de droite, tous les termes avec $k \neq i$ s'annulent d'après la remarque précédente. On obtient $N a_i X^i Y^{n-i} \in W_p$, donc $a_i X^i Y^{n-i} \in W_p$.

3a) Comme W est non nul, il existe $P = \sum_0^n a_i X^i Y^{n-i} \in W$ et i tels que $a_i \neq 0$. D'après la question précédente, $X^i Y^{n-i} \in W_P$. Mais comme W est invariant et $P \in W$ on a $W_P \subset W$.

3b) On peut prendre dans les deux cas la matrice

$$g = h = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}.$$

En effet on a alors $\pi_n(g)(X^i Y^{n-i}) = 2^{-n/2}(X - Y)^i (X + Y)^{n-i}$ et $\pi_n(h)(X^n) = 2^{-n/2}(X - Y)^n$.

3c) Comme en 3a), on applique la question 2 à $\pi_n(g)(X^i Y^{n-i})$, qui est dans W par stabilité de W et d'après 3a). On obtient $X^n \in W$. Puis on recommence avec $\pi_n(h)(X^n)$ et on voit que tous les monômes $X^k Y^{n-k}$ sont dans W, donc $W = V_n$.

4a) Calculons l'action d'un élément de $SU(2)$ sur $X\otimes Y - Y\otimes X$:

$$\begin{aligned}(\pi_1\otimes\pi_1)(g)(X\otimes Y - Y\otimes X) &= \pi_1(g)(X)\otimes\pi_1(g)(Y) - \pi_1(g)(Y)\otimes\pi_1(g)(X)\\ &= (aX+cY)\otimes(bX+dY) - (bX+dY)\otimes(aX+cY)\\ &= (ab-ba)(X\otimes X) + (cd-dc)(Y\otimes Y) +\\ &\qquad + (ad-bc)(X\otimes Y) + (cb-da)(Y\otimes X) = X\otimes Y - Y\otimes X.\end{aligned}$$

Vérifions que ψ est un entrelaceur :

$$\begin{aligned}\psi(\pi_m\otimes\pi_n)(g)(P\otimes Q) &= \psi(P(aX+cY, bX+dY)\otimes Q(aX+cY, bX+dY))\\ &= P(aX+cY, bX+dY) \times Q(aX+cY, bX+dY)\\ &= (PQ)(aX+cY, bX+dY) = \pi_{m+n}(g)(\psi(P\otimes Q))\end{aligned}$$

Par linéarité on peut remplacer $P\otimes Q$ dans l'égalité précédente par n'importe quel élément de $V_m\otimes V_n$. Cela montre en fait que la somme directe des représentations π_n sur $\mathbb{C}[X,Y]$ agit par des morphismes d'anneaux.

En appliquant ce principe et la première partie de la question on peut alors écrire :

$$\begin{aligned}(\pi_m\otimes\pi_n)(g)((X\otimes Y - Y\otimes X)(P\otimes Q)) &= (\pi_1\otimes\pi_1)(g)(X\otimes Y - Y\otimes X) \times (\pi_{m-1}\otimes\pi_{n-1})(g)(P\otimes Q)\\ &= (X\otimes Y - Y\otimes X)(\pi_{m-1}\otimes\pi_{n-1})(g)(P\otimes Q).\end{aligned}$$

Cela montre que ϕ est un entrelaceur.

4b) L'image par ψ de la base $(X^kY^{m-k}\otimes X^lY^{n-l})$ est la famille $(X^{k+l}Y^{m+n-(k+l)})$, qui coïncide, à des répétitions près, avec la base canonique de V_{m+n}. Donc ψ est surjective.

Notons par ailleurs que l'anneau $\mathbb{C}[X,Y]\otimes\mathbb{C}[X,Y]$ est intègre : en effet il est isomorphe à $\mathbb{C}[X,Y,X',Y']$, qui est intègre, via l'application $(X^kY^l\otimes X^pY^q \mapsto X^kY^lX'^pY'^q)$. L'injectivité de ϕ est alors évidente.

Enfin on remarque que

$$\psi\phi(P\otimes Q) = \psi(XP\otimes YQ - YP\otimes XQ) = XYPQ - XYPQ = 0.$$

Par linéarité il s'ensuit que $\psi\phi = 0$ donc $\operatorname{Im}\phi \subset \operatorname{Ker}\psi$. Mais d'autre part

$$\dim\operatorname{Ker}\psi = \dim(V_n\otimes V_m) - \dim\operatorname{Im}\psi = (n+1)(m+1) - (m+n+1) = mn = \dim\operatorname{Im}\phi,$$

donc $\operatorname{Im}\phi = \operatorname{Ker}\psi$.

4c) Admettons que les représentations de dimension finie des groupes compacts sont sommes directes de représentations irréductibles. Alors, l'image de ϕ dans $V_m\otimes V_n$, qui est isomorphe à $V_{m-1}\otimes V_{n-1}$ en tant que représentation, admet une sous-représentation supplémentaire W, que ψ envoie isomorphiquement sur V_{m+n} d'après 4b). On a donc $V_m\otimes V_n \simeq (V_{m-1}\otimes V_{n-1}) \oplus V_{n+m}$, et les règles de fusion annoncées s'ensuivent par une récurrence immédiate. On notera que V_0 est la représentation triviale de $SU(2)$ et vérifie clairement $V_0\otimes V_0 \simeq V_0$.

Notons que la sous-représentation supplémentaire W s'obtient très simplement comme $W = (\operatorname{Im}\phi)^\perp$ si on dispose d'un produit scalaire invariant sur $V_m\otimes V_n$. Or il est facile de donner un tel produit scalaire sur chaque V_n, en posant $\|P\|^2 = \int P(x,y)^2\exp(-(x^2+y^2))dxdy$.

5a) On a pour toute permutation $\rho \in \mathfrak{S}_n$:

$$\sigma_n(\rho)S = \frac{1}{n!}\sum_{\tau\in\mathfrak{S}_n}\sigma_n(\rho\tau) = S.$$

Cela montre que $\operatorname{Im} S \subset F_n$ et, en sommant sur ρ, que $S^2 = S$. Par ailleurs si $v \in F_n$ on a $\sigma_n(\tau)(v) = v$ pour toute permutation τ, donc $S(v) = v$. Ainsi $F_n \subset \operatorname{Im} S$.

5b) Soit B_k l'ensemble des tenseurs élémentaires de longueur n en e_1 et e_2 qui contiennent k occurences de e_1. Ainsi $\bigcup B_k$ est la base canonique de E_n. Il est clair que $\mathfrak{S}_n$ agit transitivement sur B_k via σ_n. Pour tout $v \in B_k$ on a donc $S(v) = f_k$, et $S(v) \in \operatorname{Vect}\{w \mid w \in B_k\}$. Ainsi (f_k)

est l'image d'une base, donc c'est une famille génératrice de $\operatorname{Im} S = F_n$, et elle est libre car les sous-espaces $\operatorname{Vect}\{w \mid w \in B_k\}$ sont en somme directe.

6a) Par linéarité il suffit de vérifier l'égalité sur les tenseurs élémentaires $\zeta_1 \otimes \cdots \otimes \zeta_n$. Posons $\xi_k = \rho_1(g)\zeta_k$, on a alors

$$\begin{aligned}\rho_n(g)\sigma_n(\tau)(\zeta_1 \otimes \cdots \otimes \zeta_n) &= \rho_n(g)(\zeta_{\tau^{-1}(1)} \otimes \cdots \otimes \zeta_{\tau^{-1}(n)}) = \xi_{\tau^{-1}(1)} \otimes \cdots \otimes \xi_{\tau^{-1}(n)} \\ &= \sigma_n(\tau)(\xi_1 \otimes \cdots \otimes \xi_n) = \sigma_n(\tau)\rho_n(g)(\zeta_1 \otimes \cdots \otimes \zeta_n).\end{aligned}$$

Soit $v \in F_n$ et $g \in SU(2)$. Pour toute permutation $\tau \in \mathfrak{S}_n$ on a $v = \sigma_n(\tau)(v)$ donc $\rho_n(g)(v) = \rho_n(g)\sigma_n(\tau)(v) = \sigma_n(\tau)\rho_n(g)(v)$, ce qui montre que $\rho_n(g)(v) \in F_n$.

6b) Considérons l'application linéaire $\phi_1 : E_1 \to V_1$ définie par $\phi_1(e_1) = X$, $\phi_1(e_2) = Y$. Il est clair que ϕ_1 entrelace les représentations ρ_1, π_1. En composant $\phi_1^{\otimes n}$ avec la multiplication de $\mathbb{C}[X, Y]$, qui est un entrelaceur d'après 4a), on obtient une application $\phi_n : E_n \to V_n$ qui entrelace ρ_n, π_n, et est donnée par la formule

$$\phi_n(e_{i_1} \otimes \cdots \otimes e_{i_n}) = Z_{i_1} \cdots Z_{i_n},$$

où on note $Z_1 = X$, $Z_2 = Y$. Il est clair que ϕ_n est surjective et que $\phi_n \circ \sigma_n(\tau) = \phi_n$ pour toute permutation $\tau \in \mathfrak{S}_n$, par commutativité de la multiplication de $\mathbb{C}[X, Y]$. En particulier $\phi_n(S - \mathrm{id}) = 0$, donc $E_n = F_n + \operatorname{Ker} \phi_n$. Comme $\dim F_n = n + 1 = \dim V_n$, la somme est directe et la restriction de ϕ_n à F_n est un isomorphisme.

On peut en fait interpréter E_n comme l'espace des polynômes homogènes de degré n en deux indéterminées non-commutatives, et ϕ_n est alors l'application quotient naturelle obtenue en laissant commuter les indéterminées.

Algèbres de Taft et q-nombres (corrigé)

1a) Pour $q \neq 1$ on a $(k)_q = (1 - q^k)/(1 - q)$ qui ne s'annule pas si q n'est pas une racine de l'unité. Dans ce cas, les q-factorielles ne s'annulent jamais, donc les q-coefficient binômiaux sont bien définis. Lorsque q est une racine primitive n^{e} de l'unité, la q-factorielle $(k)!_q$ est nulle **ssi** $k \geq n$, donc le q-coefficient $\binom{k}{l}_q$ est bien défini pour $k - n < l < n$.

1b) On calcule le membre de gauche, en utilisant le fait que $(l)_q + q^l(k - l)_q = (k)_q$:

$$\begin{aligned}\binom{k-1}{l-1}_q + q^l\binom{k-1}{l}_q &= \frac{(k-1)!_q}{(k-l)!_q(l-1)!_q} + \frac{q^l(k-1)!_q}{(k-1-l)!_q(l)!_q} \\ &= (k-1)!_q\frac{(l)_q + q^l(k-l)_q}{(l)!_q(k-l)!_q} = \frac{(k)!_q}{(l)!_q(k-l)!_q} = \binom{k}{l}_q.\end{aligned}$$

Notons que si q est une racine primitive n^{e} de l'unité, ce calcul est valable si $k - n < l < n$.

1c) Comme dans le cas « classique », on procède par récurrence sur k. Pour $k = 0$ on a au membre de droite $k = l = 0$ et $\binom{0}{0}_q = 1$. Supposons le résultat vrai pour $k = n - 1$, on écrit

$$\begin{aligned}(a+b)^n = (a+b)\sum_{l=0}^{n-1}\tbinom{n-1}{l}_q a^l b^{n-l-1} &= \sum_{l=0}^{n-1}\tbinom{n-1}{l}_q(a^{l+1}b^{n-l-1} + q^l a^l b^{n-l}) \\ &= \sum_{l=1}^{n-1}(\tbinom{n-1}{l-1}_q + q^l\tbinom{n-1}{l}_q)a^l b^{n-l} + \tbinom{n-1}{n-1}_q a^n b^0 + \tbinom{n-1}{0}_q q^0 a^0 b^n,\end{aligned}$$

ce qui donne le résultat voulu grâce à la question précédente et au fait que les q-coefficients binômiaux des deux derniers termes valent 1. On note que les calculs jusqu'à ce rang n sont valables même dans le cas où q est une racine primitive n^{e} de l'unité, en convenant que $\binom{n}{0}_q = \binom{n}{n}_q = 1$.

De plus, tous les coefficients $\binom{n}{l}_q$ avec $0 < l < n$ sont biens définis mais nuls, et on obtient donc la formule $(a + b)^n = a^n + b^n$ dans le cas où q est une racine primitive n^{e} de l'unité. On notera l'analogie avec l'additivité du morphisme de Frobenius dans les corps de caractéristique positive.

2a) Notons $f_k = e_k$, $e_{n+k} = e_k$ et $f_{n+k} = 0$ pour $k = 0, \dots, n-1$. On a alors $\sigma^k(e_i \otimes f_j) = e_{i+k} \otimes f_j$ et $\tau^l(e_i \otimes f_j) = q^{li} e_i \otimes f_{j+l}$ pour i, j, k, $l = 0, \dots, n-1$. En particulier on voit que $\sigma^n = \mathrm{id}$ et $\tau^n = 0$. De plus

$$\tau\sigma(e_i \otimes e_j) = q^{i+1}(e_{i+1} \otimes e_{j+1}) = q\sigma\tau(e_i \otimes e_j)$$

pour tous i, j. On voit ainsi que σ, τ vérifient les relations de définition de $T_n(q)$, donc il existe un unique morphisme d'algèbres $\phi : T_n(q) \to L(E)$ tel que $\phi(g) = \sigma$ et $\phi(x) = \tau$. On a de plus $\sigma^k \tau^l(e_0 \otimes e_0) = e_k \otimes f_l$.

2b) Le dernier calcul de la question précédente montre que l'application $(a \mapsto \phi(a)(e_0 \otimes e_0))$ de $T_n(q)$ dans E envoie $g^k x^l$ sur $e_k \otimes f_l$. Comme $(e_k \otimes f_l)$, avec k, $l = 0, \dots n-1$, est libre dans E, c'est aussi le cas de $(g^k x^l)$ dans $T_n(q)$. Par ailleurs il est clair que les relations de définition de $T_n(q)$ permettent d'écrire tout produit des générateurs g, x comme multiple scalaire d'un produit « ordonné » $g^k x^l$ avec $0 \le k$, $l \le n-1$. Donc la famille considérée est également génératrice.

3a) Comme précédemment, il suffit de vérifier que G, X vérifient les relations de définition de $T_n(q)$. On utilise la dernière remarque de la question 1c), grâce au fait que q est une racine primitive n^{e} de l'unité et que $ba = qab$ si $b = 1 \otimes x$ et $a = x \otimes g$:

$$G^n = g^n \otimes g^n = 1 \otimes 1 = 1, \quad X^n = (x \otimes g + 1 \otimes x)^n = 1^n \otimes x^n + x^n \otimes g^n = 0,$$
$$XG = g \otimes xg + xg \otimes g^2 = q(g \otimes gx) + q(gx \otimes g^2) = qGX.$$

Cela montre l'existence et l'unicité de Δ. On obtient de même celles de ϵ en remarquant que 1, $0 \in \mathbb{C}$ vérifient évidemment les mêmes relations.

3b) Comme $(\Delta \otimes \mathrm{id})\Delta$, $(\mathrm{id} \otimes \Delta)\Delta$, $(\epsilon \otimes \mathrm{id})\Delta$ et $(\mathrm{id} \otimes \epsilon)\Delta$ sont des morphismes d'algèbres, il suffit de vérifier les relations demandées sur les générateurs g, x. Les calculs sont faciles :

$$(\Delta \otimes \mathrm{id})\Delta(g) = g \otimes g \otimes g = (\mathrm{id} \otimes \Delta)\Delta(g),$$
$$(\Delta \otimes \mathrm{id})\Delta(x) = 1 \otimes 1 \otimes x + 1 \otimes x \otimes g + x \otimes g \otimes g = (\mathrm{id} \otimes \Delta)\Delta(x)$$
$$(\epsilon \otimes \mathrm{id})\Delta(g) = g, \quad (\mathrm{id} \otimes \epsilon)\Delta(x) = x.$$

3c) Comme à la question précedente, il suffit de vérifier que $\tilde{g}$, $\tilde{x}$ vérifient les relations de définition de $T_n(q)$, mais dans $T_n(q)^{\mathrm{op}}$. Les puissances de $\tilde{g}$ et $\tilde{x}$ sont les mêmes dans les deux algèbres, et on obtient facilement les identité $\tilde{g}^n = 1$, $\tilde{x}^n = 0$. D'autre part on a

$$\tilde{x} \cdot_{\mathrm{op}} \tilde{g} = g^{-1}(-xg^{-1}) = -qxg^{-2} = q(-xg^{-1})g^{-1} = q\, \tilde{g} \cdot_{\mathrm{op}} \tilde{x}.$$

Vérifions maintenant l'axiome de l'antipode sur les générateurs :

$$m(\mathrm{id} \otimes S)\Delta(g) = m(g \otimes S(g)) = gg^{-1} = 1 = \epsilon(g)1$$
$$m(\mathrm{id} \otimes S)\Delta(x) = 1 \times (-xg^{-1}) + x \times g^{-1} = 0 = \epsilon(x)1,$$

et de même avec S à gauche. Par ailleurs, supposons l'axiome vérifié sur b, $c \in T_n(q)$. En utilisant la notation de Sweedler cela s'écrit par exemple $\sum b_{(1)} S(b_{(2)}) = \epsilon(b)1$, $\sum c_{(1)} S(c_{(2)}) = \epsilon(c)1$. On peut alors écrire, en utilisant l'antimultiplicativité de S :

$$m(\mathrm{id} \otimes S)\Delta(bc) = m(\mathrm{id} \otimes S)(\Delta(b)\Delta(c)) = \sum m(\mathrm{id} \otimes S)(b_{(1)}c_{(1)} \otimes b_{(2)}c_{(2)})$$
$$= \sum b_{(1)}c_{(1)} S(c_{(2)}) S(b_{(2)}) = \epsilon(c) \sum b_{(1)} S(b_{(2)}) = \epsilon(c)\epsilon(b)1 = \epsilon(bc)1.$$

Il s'ensuit que l'axiome de l'antipode est vérifié sur n'importe quel produit des générateurs, par récurrence sur la longueur du produit, et donc sur n'importe quel élément de $T_n(q)$, par linéarité.

3d) On a $S(g^k x^l) = S(x)^l S(g)^k = (-xg^{-1})^l g^{-k} = q^{l-1}(-x)^l g^{-(k+l)}$. En particulier il est clair que S permute les vecteurs de la base $(g^k x^l)$ à des constantes non nulles près, donc S est bijective. Par ailleurs on a $S^2(g) = g$ et $S^2(x) = -S(g^{-1})S(x) = gxg^{-1} = q^{-1}x$. Donc pour tout $k \in \mathbb{N}$:

$$S^{2k}(g) = g, \quad S^{2k}(x) = q^{-k}x, \quad S^{2k+1}(g) = g^{-1}, \quad S^{2k+1}(x) = -q^{-k}xg^{-1}.$$

Comme q est une racine primitive n^{e} de l'unité, S est d'ordre $2n$.

4) On écrit l'invariance à droite sur les vecteurs de la base naturelle en utilisant, comme en 3a), la q-formule du binôme :

$$(\phi\otimes\mathrm{id})\Delta(g^k x^l) = (\phi\otimes\mathrm{id})((g^k\otimes g^k)(x\otimes g + 1\otimes x)^l) = \sum_{i=0}^{l} \binom{l}{i}_q \phi(g^k x^i) g^{k+i} x^{l-i} = \phi(g^k x^l)1.$$

Lorsque i varie de 0 à l, on remarque que $l-i$ prend au plus une fois les valeurs $0, \ldots, n-1$, ainsi que $k+i$ modulo n. La somme est donc une décomposition dans la base $(g^k x^l)$, et comme $1 = g^0 x^0$ on peut déduire de l'identité vectorielle ci-dessus les identités scalaires $\phi(g^k x^i) = 0$ pour tous k, l, $i = 0, \ldots, n-1$ tels que $0 \leq k,\ l \leq n-1$, $0 \leq i \leq l$ et $(k+i \neq 0 \mod n$ ou $l-i \neq 0)$. On notera que les q-coefficients binômiaux qui apparaissent ne sont jamais nuls car $(l)!_q \neq 0$ si q est une racine primitive n^{e} de l'unité et $l < n$.

Pour $i < n-1$ on peut prendre $l = i+1$ et les conditions précédentes sont vérifiées, si bien que $\phi(g^k x^i) = 0$ pour n'importe quel k. Si $i = n-1$, les conditions sont également vérifiées pour $k \neq 1$ et on a alors à nouveau $\phi(g^k x^{n-1}) = 0$. On en déduit que ϕ est nécessairement multiple de la forme linéaire qui envoie tous les $g^k x^l$ sur 0, sauf $g x^{n-1}$ qui est envoyé sur 1. Il est facile de vérifier que cette forme vérifie l'équation d'invariance à droite.

On voit en particulier qu'il n'y a pas de forme linéaire invariante unifère sur $T_n(q)$.