Algèbre VI

Correction de l'examen partiel du 4 avril 2014

Exercice 1 — 1. Les vecteurs $\begin{pmatrix} 1 \\ 0 \\ z_3 \\ z_4 \end{pmatrix}$ et $\begin{pmatrix} 0 \\ 1 \\ z'_3 \\ z'_4 \end{pmatrix}$ appartiennent au plan P si et seulement si $(z_3, z_4) = (-i, 1-i)$ et $(z'_3, z'_4) = (1+i, i)$. Les vecteurs $u = \begin{pmatrix} 1, 0, -i, 1-i \end{pmatrix}$ et $u' = \begin{pmatrix} 0, 1, 1+i, i \end{pmatrix}$ constituent donc l'unique famille de la forme voulue contenue dans P. Ces deux vecteurs sont linéairement indépendants, donc ils fournissent une base de P puisque dim P = 2.

2. Appliqué à la base (u, u') de P, le procédé de Gram-Schmidt conduit à la base orhonormale $(\varepsilon_1, \varepsilon_2)$, où

$$\varepsilon_1 = \frac{u}{||u||} = \frac{1}{2} \begin{pmatrix} 1 \\ 0 \\ -i \\ 1-i \end{pmatrix}$$

et

$$\varepsilon_2 = \frac{u' - (\varepsilon_1, u')\varepsilon_1}{||u' - (\varepsilon_1, u')\varepsilon_1||} = \frac{\sqrt{2}}{4} \begin{pmatrix} 1-i \\ 2 \\ 1+i \\ 0 \end{pmatrix}.$$

3. La projection orthogonale sur le plan P est l'application $\pi : \mathbf{C}^4 \to \mathbf{C}^4$ définie par la formule

$$\pi(v) = (\varepsilon_1, v)\varepsilon_1 + (\varepsilon_2, v)\varepsilon_2.$$

Tous calculs faits, on obtient l'expression suivante :

$$\pi \begin{pmatrix} z_1 \\ z_2 \\ z_3 \\ z_4 \end{pmatrix} = \frac{1}{4} \begin{pmatrix} 2z_1 + (1-i)z_2 + (1+i)z_4 \\ (1+i)z_1 + 2z_2 + (1-i)z_3 \\ (1+i)z_2 + 2z_3 + (1-i)z_4 \\ (1-i)z_1 + (1+i)z_3 + 2z_4 \end{pmatrix}.$$

Exercice 2 — 1. Pour tous $x, y, z \in \mathbf{C}^n$ et tout $\lambda \in \mathbf{C}$,

$$(x, y + \lambda z)_{\mathrm{G}} = \frac{1}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} (g(x), g(y) + \lambda g(z)) = \frac{1}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} [(g(x), g(y)) + \lambda(g(x), g(z))] = (x, y)_{\mathrm{G}} + \lambda(x, z)_{\mathrm{G}}$$

et

$$(y, x)_{\mathrm{G}} = \frac{1}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} (g(y), g(x)) = \frac{1}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} \overline{(g(x), g(y))} = \overline{\frac{1}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} (g(x), g(y))} = \overline{(x, y)_{\mathrm{G}}},$$

donc $(.,.)_{\mathrm{G}}$ est une forme hermitienne.

Le nombre réel

$$(x, x)_{\mathrm{G}} = \frac{1}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} (g(x), g(x))$$

est une somme de termes positifs, donc est positif. Il s'annule si et seulement si $(g(x), g(x)) = 0$ pour tout $g \in \mathrm{G}$, donc si et seulement si $g(x) = 0$ pour tout $g \in \mathrm{G}$. Puisque les éléments de G sont des automorphismes, ceci ne se produit que si $x = 0$. La forme hermitienne $(.,.)_{\mathrm{G}}$ est donc définie positive.

Soit $h \in \mathrm{G}$. L'application $\mathrm{G} \to \mathrm{G}$, $g \mapsto g \circ h$ est une bijection, donc

$$(h(x), h(y))_{\mathrm{G}} = \frac{1}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} (g(h(x)), g(h(y)) = \frac{1}{|\mathrm{G}|} \sum_{k \in \mathrm{G}} (k(x), k(y)) = (x, y)_{\mathrm{G}}$$

en utilisant le changement d'indice $k = g \circ h$. Ainsi, l'action du groupe G sur $\mathbf{C}^4$ se fait par *isométries* de la forme hermitienne $(.,.)_{\mathrm{G}}$.

2. La base canonique de $\mathbf{C}^4$ est orthonormale pour le produit hermitien usuel.

L'automorphisme φ transforme une base orthonormale de l'espace hermitien $(\mathbf{C}^4, (.,.))$ en une base de l'espace hermitien $(\mathbf{C}^4, (.,.)_{\mathrm{G}})$, donc définit une isométrie entre ces deux espaces hermitiens. En effet, pour tous vecteurs $v = \sum_i z_i e_i$ et $v' = \sum_i z'_i e_i$,

$$(\varphi(v), \varphi(v'))_{\mathrm{G}} = \left(\sum_i z_i \varphi(e_i), \sum_j z'_j \varphi(e_j) \right)_{\mathrm{G}} = \left(\sum_i z_i e'_i, \sum_j z'_j e'_j \right)_{\mathrm{G}} = \sum_i \overline{z_i} z'_i = (v, v').$$

On en déduit immédiatement que l'automorphisme φ^{-1} définit une isométrie entre les espaces hermitiens $(\mathbf{C}^4, (.,.)_{\mathrm{G}})$ et $(\mathbf{C}^4, (.,.))$: pour tous $v, v' \in \mathbf{C}^4$,

$$(\varphi^{-1}(v), \varphi^{-1}(v')) = (\varphi(\varphi^{-1}(v)), \varphi(\varphi^{-1}(v'))_{\mathrm{G}} = (v, v')_{\mathrm{G}}.$$

D'après la question précédente, tout élément g de G définit un automorphisme de $\mathbf{C}^4$ qui est une isométrie pour le produit hermitien $(.,.)_{\mathrm{G}}$. Il découle alors des deux observation précédentes que l'application $\varphi^{-1} \circ g \circ \varphi$ est une isométrie de $\mathbf{C}^4$ pour le produit hermitien usuel, donc un élément de $\mathrm{U}_n(\mathbf{C})$: en effet, pour tous $v, v' \in \mathbf{C}^4$,

$$(\varphi^{-1}(g(\varphi(v))), \varphi^{-1}(g(\varphi(v')))) = (g(\varphi(v)), g(\varphi(v')))_{\mathrm{G}} = (\varphi(v), \varphi(v')))_{\mathrm{G}} = (v, v').$$

3. L'application

$$\Phi : \mathrm{G} \to \mathrm{GL}_n(\mathbf{C}), \qquad g \mapsto \varphi^{-1} \circ g \circ \varphi$$

est un morphisme de groupes injectif et donc induit un isomorphisme entre G et le sous-groupe $\Phi(\mathrm{G})$ de $\mathrm{GL}_n(\mathbf{C})$. Ce dernier étant contenu dans $\mathrm{U}_n(\mathbf{C})$ en vertu de la question précédente, nous avons démontré que G est isomorphe à un sous-groupe de $\mathrm{U}_n(\mathbf{C})$.

Exercice 3 — 1. Pour tous $\mathrm{P}, \mathrm{Q}, \mathrm{R} \in \mathbf{C}[\mathrm{X}]_n$ et tout $\lambda \in \mathbf{C}$,

$$(\mathrm{P}, \mathrm{Q} + \lambda \mathrm{R}) = (\mathrm{P}, \mathrm{Q}) + \lambda (\mathrm{P}, \mathrm{R})$$

(linéarité de l'intégrale) et

$$(\mathrm{Q}, \mathrm{P}) = \overline{(\mathrm{P}, \mathrm{Q})},$$

donc la forme considérée est hermitienne.

Étant donné $\mathrm{P} \in \mathbf{C}[\mathrm{X}]_n$, on a

$$(\mathrm{P}, \mathrm{P}) = \frac{1}{2\pi} \int_0^{2\pi} |\mathrm{P}(e^{it})|^2 \, \mathrm{d}t \geqslant 0.$$

Si $(\mathrm{P}, \mathrm{P}) = 0$, alors la fonction continue et positive $(t \mapsto |\mathrm{P}(e^{it})|^2)$ est identiquement nulle sur $[0, 2\pi]$, donc le polynôme P admet une infinité de racines dans $\mathbf{C}$ et nécessairement $\mathrm{P} = 0$. On a ainsi vérifié que la forme hermitienne considérée est définie positive.

2. Quels que soient les entiers $p, q \in \{0, \ldots, n\}$,

$$(\mathrm{X}^p, \mathrm{X}^q) = \frac{1}{2\pi} \int_0^{2\pi} e^{-iqt} e^{ipt} \, \mathrm{d}t = \begin{cases} 1 & \text{si } p = q \\ \frac{1}{p-q} \left[e^{i(p-q)t} \right]_0^{2\pi} & \text{si } p \neq q \end{cases} = \begin{cases} 1 & \text{si } p = q \\ 0 & \text{si } p \neq q \end{cases}$$

donc la base canonique de $\mathbf{C}[\mathrm{X}]_n$ est orthonormale.

3. En vertu de la question précédente,

$$||\mathrm{P}||^2 = 1 + |a_{m-1}|^2 + \ldots + |a_0|^2.$$

Ceci implique en particulier $||\mathrm{P}|| \geqslant 1$, avec égalité si et seulement si $\mathrm{P} = \mathrm{X}^m$.

Par ailleurs,

$$||\mathrm{P}||^2 = (\mathrm{P}, \mathrm{P}) = \frac{1}{2\pi} \int_0^{2\pi} |\mathrm{P}(e^{it})\ \mathrm{d}t \leqslant \frac{1}{2\pi} \int_0^{2\pi} \mathrm{M}^2\ \mathrm{d}t = \mathrm{M}^2$$

et donc $||\mathrm{P}|| \leqslant \mathrm{M}$ puisque ces deux nombres réels sont positifs. On en déduit la minoration

$$1 \leqslant ||\mathrm{P}|| \leqslant \mathrm{M}.$$

4. Si $\mathrm{M} = 1$, alors $||\mathrm{P}|| = 1$ et donc $\mathrm{P} = \mathrm{X}^m$. Réciproquement, si $\mathrm{P} = \mathrm{X}^m$, alors

$$\mathrm{M} = \sup_{t \in \mathbf{R}} |e^{imt}| = \sup_{t \in \mathbf{R}} 1 = 1.$$

Ainsi, $\mathrm{M} = 1$ si et seulement si P est un monôme.

Exercice 4 — 1. Posons $d = \mathrm{pgcd}(a, n)$. Comme $d|a$, l'inclusion $\langle \overline{a} \rangle \subset \langle \overline{d} \rangle$ est immédiate.

Pour obtenir l'inclusion réciproque, considérons une relation de Bézout

$$d = ap + nq, \quad p,\ q \in \mathbf{Z}.$$

En réduisant modulo n, on obtient $\overline{d} \in \langle \overline{a} \rangle$ et donc $\langle \overline{d} \rangle \subset \langle \overline{a} \rangle$.

2. Vérifions tout d'abord que cette application est injective. Si d et d' sont deux diviseurs positifs de n tels que $\langle \overline{d} \rangle = \langle \overline{d'} \rangle$, alors il existe des entiers u, v, u', v' tels que

$$d' = du + nv \quad \text{ et } \quad d = d'u' + nv'.$$

Puisque $d|n$ (resp. $d'|n$), la première (resp. la seconde) égalité implique $d|d'$ (resp. $d'|d$) et donc $d = d'$.

Tout sous-groupe de $\mathbf{Z}/n\mathbf{Z}$ est cyclique, donc de la forme $\langle \overline{m} \rangle$ pour un certain entier m. La question 1 permet d'écrire $\langle \overline{m} \rangle = \langle \overline{d} \rangle$ avec $d = \mathrm{pgcd}(m, n)$. Ceci démontre la surjectivité de l'application considérée puisque d est un diviseur positif de n.

3. Supposons que le groupe A soit cyclique, donc isomorphe à $\mathbf{Z}/n\mathbf{Z}$ pour un certain entier $n \geqslant 1$. D'après la question précédente, deux sous-groupes distincts de A sont isomorphes à $\langle \overline{d} \rangle$ et $\langle \overline{d'} \rangle$, où d et d' sont deux diviseurs positifs distincts de n. Ces sous-groupes sont d'ordres respectifs n/d et n/d', donc ils ne sont pas isomorphes.

Nous avons ainsi démontré l'implication (Non (a)) $\Rightarrow$ (Non (b)), qui équivaut à l'implication (b) $\Rightarrow$ (a).

4. En vertu du théorème de structure des groupes abéliens finis, il existe $r \geqslant 1$ et des entiers positifs $d_1, d_2, \ldots, d_r$ tels que

$$d_2 | d_1, \ldots, d_r | d_{r-1}$$

et

$$\mathrm{A} \simeq \mathbf{Z}/d_1\mathbf{Z} \times \mathbf{Z}/d_2\mathbf{Z} \times \ldots \times \mathbf{Z}/d_r\mathbf{Z}.$$

Si le groupe A n'est *pas* cyclique, alors $r \geqslant 2$. Les r-uplets $x = (\overline{0}, \overline{1}, \overline{0}, \ldots, \overline{0})$ et $y = (\overline{d_1/d_2}, \overline{0}, \ldots, \overline{0})$ engendrent deux sous-groupes cycliques distincts de $\mathbf{Z}/d_1\mathbf{Z} \times \mathbf{Z}/d_2\mathbf{Z} \times \ldots \times \mathbf{Z}/d_r\mathbf{Z}$, tous deux d'ordre d_2. On voit ainsi que A contient deux sous-groupes cycliques distincts isomorphes.

Nous avons ainsi démontré l'implication (a) $\Rightarrow$ (b).

Exercice 5 — 1. L'implication (ii) $\Rightarrow$ (i) est facile : chaque caractère χ de A envoie l'élément neutre de A sur l'élément neutre de $\mathbf{C}^\times$, donc $a \neq e$ si $\chi(a) \neq 1$.

Démontrons maintenant l'implication (i) $\Rightarrow$ (ii). Si l'élément a de A est non trivial, le sous-groupe $\langle a \rangle$ qu'il engendre est isomorphe à $\mathbf{Z}/m\mathbf{Z}$ avec $m = \mathrm{ord}(a) \geqslant 2$. Choisissons une racine primitive m-ième de l'unité $\omega \in \mathbf{C}$. L'application

$$\chi_0 : \langle a \rangle \to \mathbf{C}^\times, \quad a^k \mapsto \omega^k$$

est bien définie et il s'agit d'un caractère du groupe $\langle a \rangle$ tel que $\chi_0(a) = \omega \neq 1$.

Par application du théorème de prolongement, il existe un caractère χ de G tel que $\chi_{|\langle a \rangle} = \chi_0$. Puisque

$$\chi(a) = \chi_0(a) \neq 1,$$

ce caractère satisfait à la condition de (ii).

Remarque — On peut également aborder cette question en mettant à profit l'isomorphisme canonique de bidualité

$$\mathrm{G} \tilde{\to} \widehat{\widehat{\mathrm{G}}}, \qquad a \mapsto (\chi \mapsto \chi(a)).$$

En effet, si a est un élément de A distinct de e, alors le caractère correspondant du groupe $\widehat{\mathrm{A}}$ est non trivial et il existe donc un élément χ de $\widehat{\mathrm{A}}$ tel que $\chi(a) \neq 1$.

2. Si $a = e$, alors $\chi(a) = 1$ pour tout caractère $\chi \in \widehat{\mathrm{A}}$ et donc

$$\sum_{\chi \in \widehat{\mathrm{A}}} \chi(a) = \sum_{\chi \in \widehat{\mathrm{A}}} 1 = |\widehat{\mathrm{A}}| = |\mathrm{A}|.$$

Si $a \neq e$, alors il existe un caractère $\chi_1 \in \widehat{\mathrm{A}}$ tel que $\chi_1(a) \neq 1$ (cf. question précédente). L'application $(\widehat{\mathrm{A}} \to \widehat{\mathrm{A}},\ \chi \mapsto \chi_1^{-1}\chi)$ est une bijection, donc

$$\sum_{\chi \in \widehat{\mathrm{A}}} \chi(a) = \sum_{\chi \in \widehat{\mathrm{A}}} \chi_1(a)(\chi_1^{-1}\chi)(a) = \chi_1(a) \sum_{\chi \in \widehat{\mathrm{A}}} (\chi_1^{-1}\chi)(a) = \chi_1(a) \sum_{\psi \in \widehat{\mathrm{A}}} \psi(a)$$

en faisant le changement d'indice $\psi = \chi_1^{-1}\chi$. On obtient ainsi

$$(1 - \chi_1(a)) \sum_{\chi \in \widehat{\mathrm{A}}} \chi(a) = 0, \quad \text{puis} \quad \sum_{\chi \in \widehat{\mathrm{A}}} \chi(a) = 0$$

car $\chi_1(a) \neq 1$.

Au final, nous obtenons

$$\sum_{\chi \in \widehat{\mathrm{A}}} \chi(a) = \begin{cases} |\mathrm{A}| & \text{si } a = e \\ 0 & \text{si } a \neq e. \end{cases}$$