L3 - Math VI- Représentation des groupes finis
2012-2013

Partiel - Le 21 mars 2013 - 2h00

Avertissement. La notation tiendra largement compte de la qualité de la rédaction et de la précision des arguments employés.

---

1. Produits hermitiens

Soit E un espace hermitien dont on note $(\ ,\ )$ le produit hermitien et $\|\cdot\|$ la norme.

a. Soit u et v deux vecteurs de norme un de E. Montrer que

$$\sqrt{1-|(u,v)|^2} = \|v-u(u,v)\|.$$

Réponse. Comme u et v sont de norme un, l'inégalité de Cauchy-Schwarz montre que $|(u,v)| \leq 1$. Ainsi, la racine carrée est bien définie. Comme les deux réels à comparer sont positifs ou nuls, il suffit de montrer qu'ils ont le même carré. Or, $\|v-u(u,v)\|^2 = \|v\|^2 + \|u(u,v)\|^2 - 2\Re(v,(u,v)u) = 1 + |(u,v)| - 2\Re(|(u,v)|^2) = 1-|(u,v)|^2$.

Nous admettrons le résultat suivant

Lemme . *Soit u, v et w trois vecteurs de norme un de E. Alors*

$$\sqrt{1-|(u,w)|^2} \leq \sqrt{1-|(u,v)|^2} + \sqrt{1-|(v,w)|^2}.$$

Réponse. Le lemme est délicat à prouver, c'est pour cela qu'il était admis. On peut tout d'abord remarquer qu'ajouter à w un vecteur orthogonal à u et v ne change aucun des produits hermitiens de l'inégalité. Alors, on peut se ramener au cas où w appartient à l'espace vectoriel engendré par u et v.
Si u et v sont lié l'inégalité est facile. On suppose le contraire. Soit z tel que (u,z) est une base unitaire de $Vect(u,v)$. Quitte à multiplier u et z par des nombres complexes de module 1, on peut supposer que $v = \alpha u + \beta z$ avec $\alpha, \beta \in \mathbb{R}^+$. Ecrivons aussi $w = \gamma u + \delta z$. Quitte à multiplier w par un complexe de module 1, on peut supposer que $\gamma \in \mathbb{R}^+$.
Les hypothèses s'écrivent alors $\alpha^2+\beta^2 = \gamma^2+|\delta|^2 = 1$ et la conclusion s'écrit

$$\sqrt{1-\gamma^2} \leq \sqrt{1-\alpha^2} + \sqrt{1-|\alpha\gamma+\beta\delta|^2},$$

ou encore

$$|\delta| - \beta \leq \sqrt{1-|\alpha\gamma+\beta\delta|^2}.$$

On peut élever au carré (pourquoi ?), ce qui donne après simplification

$$|\delta|^2 + \beta^2 - 2\beta|\delta| \leq \beta^2 + |\delta|^2 - 2\beta\left(\beta|\delta|^2 - \sqrt{(1-\beta^2)(1-|\delta|^2}\Re(\delta)\right)$$

ou encore

$$\beta|\delta|^2 - \sqrt{(1-\beta^2)(1-|\delta|^2}\Re(\delta) \leq |\delta|.$$

Si $\Re(\delta) \geq 0$, c'est facile. Sinon on utilise l'inégalité arithmético-géométrique sur $\sqrt{(1-\beta^2)(1-|\delta|^2}$ et le fait que $\Re(\delta) \leq |\delta|$. Il suffit alors de montrer

$$\beta|\delta| \leq \frac{\beta^2+|\delta|^2}{2}$$

c'est-à-dire l'inégalité arithmético-géométrique. OUF ! Voilà pourquoi cela était admis.

b. Soit $E = M_n(\mathbb{C})$ l'espace des matrices muni du produit hermitien $(\ ,\ )$ pour lequel la base canonique est unitaire. Pour $A, B \in M_n(\mathbb{C})$, exprimer (A,B) à l'aide de la trace.

Réponse. On a $(A,B) = tr({}^t\bar{A}B)$. En effet, le coefficient (i,i) de ${}^t\bar{A}B$ vaut $\sum_k \bar{a}_{ki}b_{ki}$. Donc la trace est $\sum_{k,i} \bar{a}_{ki}b_{ki}$.

c. Montrer que si A et B sont deux matrices unitaires de taille n alors
$$\sqrt{n^2 - |tr(AB)|^2} \leq \sqrt{n^2 - |tr(A)|^2} + \sqrt{n^2 - |tr(B)|^2}.$$

Réponse. Il suffit d'appliquer le lemme aux 3 vecteurs de norme un de $M_n(\mathbb{C})$, $u = \frac{1}{\sqrt{n}}{}^t\bar{A}$, $v = \frac{1}{\sqrt{n}} I_n$ et $w = \frac{1}{\sqrt{n}} B$.

2. Matrices hermitiennes

Soit $V = \mathbb{C}^n$ et $(e_1, \dots, e_n)$ les vecteurs de la base canonique de V. On notera les vecteurs de V comme des matrices à n lignes et 1 colonne.

a. Soit $A \in M_n(\mathbb{C})$ telle que ${}^t\bar{A} = A$, c'est-à-dire hermitienne. Montrer que les valeurs propres de A sont réelles.

Réponse. Soit λ une valeur propre et X un vecteur propre associé. Alors $AX = \lambda X$ et ${}^t\bar{X}AX = \lambda \|X\|^2$. Par ailleurs, ${}^t\bar{X}AX =^t ({}^t\bar{X}AX) =^t X^t A\bar{X} =^t X\bar{A}\bar{X} = \overline{{}^t\bar{X}AX}$. Donc ${}^t\bar{X}AX$ est réel. Donc λ est réel.

Un produit hermitien $(\cdot, \cdot)$ est dit *positif* si $(X, X) \geq 0$ pour tout $X \in V$.

b. Montrer que les assertions suivantes sont équivalentes

(1) Toutes les valeurs propres de A sont positives ou nulles ;

(2) Le produit hermitien de matrice A est positif.

On dira alors que A est *positive*.

Réponse. Pour X vecteur propre de valeur propre λ, on a $(X, X)_A =^t \bar{X}AX = \lambda \|X\|^2$. Donc la première assertion découle de la deuxième. Réciproquement toutes les valeurs propres sont positives. Par le théorème de réduction il existe une matrice unitaire U, une matrice diagonale Δ à coefficients positifs telles que $A =^t \bar{U}DU$. Alors, pour tout X, ${}^t\bar{X}AX =^t \overline{UX}D(UX) \geq 0$.

c. Soit φ une forme linéaire sur V. Montrer que l'application $(\cdot, \cdot)_\varphi : V \times V \longrightarrow \mathbb{C}$ définie par $(X, Y)_\varphi = \overline{\varphi(X)}\varphi(Y)$ est une forme hermitienne positive.

Réponse. Toutes les assertions de la définition sont faciles.

d. Soit L la matrice de φ dans la base canonique. Montrer que la matrice de $(\cdot, \cdot)_\varphi$ dans la base canonique est ${}^t\bar{L}L$.

Réponse. Puisque $\varphi(X) = LX$, pour tout $X, Y \in V$, on a $(X, Y)_\varphi = \overline{LX}LY$. Comme $LX \in \mathbb{C}$, on a ${}^t(LX) = LX$. Donc $(X, Y)_\varphi =^t \bar{X}^t\bar{L}LY$. Il suit que la matrice de $(\cdot, \cdot)_\varphi$ dans la base canonique est ${}^t\bar{L}L$.

e. Soit A une matrice hermitienne positive de rang un. Déduire de ce qui précède qu'il existe $z_1, \dots, z_n \in \mathbb{C}$ tels que $A = (\bar{z}_i z_j)$.

Réponse. Comme A est diagonalisable de rang 1, ses valeurs propres sont $\lambda, 0, \dots, 0$, avec $\lambda \neq 0$. Comme de plus A est hermitienne positive $\lambda \in \mathbb{R}^{+*}$. Considérons la matrice
$$\Delta = \begin{pmatrix} \lambda & & & \\ & 0 & & \\ & & \ddots & \\ & & & 0 \end{pmatrix}$$
et le vecteur ligne $L = (\sqrt{\lambda}\, 0 \cdots 0)$. On constate que $\Delta =^t \bar{L}L$.

Comme A est normale, un théorème du cours montre qu'il existe une matrice unitaire U telle que $A = U^{-1}\Delta U$. Alors, $A = U^{-1}\, {}^t\bar{L}LU =^t \bar{U}^t\bar{L}LU =^t \overline{LU}LU$. Posons $LU = (z_1 \cdots z_n)$. On a alors $A = (\bar{z}_i z_j)$.

Si $A = (a_{ij})$ et $B = (b_{ij})$ sont deux éléments de $M_n(\mathbb{C})$, on note $C = A \circ B$ l'élément de $M_n(\mathbb{C})$ dont le coefficient (i,j) vaut $a_{ij}b_{ij}$. On note $(\cdot,\cdot)_B$ et $(\cdot,\cdot)_C$ les produits hermitiens dont B et C sont les matrices dans la base canonique.

On suppose B est hermitienne et A est hermitienne positive de rang 1. Trouver un endomorphisme σ de V tel que $(X,X)_C = (\sigma(X),\sigma(X))_B$.

Réponse. Remarquons tout d'abord que $A \circ B$ est hermitienne, donc $(\cdot,\cdot)_C$ est un produit hermitien. Soit $X \in V$ de coordonnées $x_1,\dots,x_n$. Alors $(X,X)_C =^t \bar{X}CX = \sum_{i,j}(c_{ij}\bar{x}_i x_j) = \sum_{i,j}(b_{ij}\bar{z}_i zj\bar{x}_i x_j) = \sum_{i,j} b_{ij}(\overline{z_i x_i} zjx_j) = (Y,Y)_B$, où Y est le vecteur de coordonnées $z_1x_1,\dots,z_nx_n$. L'application $X \longmapsto Y$ est la multiplication par la matrice diagonale $\mathrm{diag}(z_1,\dots,z_n)$. Elle est donc linéaire et convient pour σ.

f. En supposant de plus que B est positive, montrer que C est positive.

Réponse. Avec les notations de la question précédente, on a pour tout $X \in V$, $(X,X)_C = (\sigma(X),\sigma(X))_B \geq 0$.

g. On suppose maintenant que A et B sont hermitiennes positives mais on ne fait plus d'hypothèse sur le rang de A. Montrer que C est hermitienne positive.

Indication. Utiliser le fait suivant $(A_1 + \cdots + A_r) \circ B = (A_1 \circ B) + \cdots + (A_r \circ B)$.

Réponse. Notons r le rang de A. On réduit A, sous la forme

$$A = U \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix} U^{-1},$$

avec U unitaire et $\lambda_{r+1} = \cdots = \lambda_n = 0$. Pour $i = 1,\dots,r$, considérons la matrice A_i obtenue en remplaçant tous le λ_k pour $k \neq i$ par 0. Alors, les A_i sont hermitiennes positives et de rang 1. Donc chaque $A_i \circ B$ est hermitiennes positive d'après la question précédente. Puisque $(A_1 + \cdots + A_r) \circ B = (A_1 \circ B) + \cdots + (A_r \circ B)$, nous avons donc écrit $A \circ B$ comme une somme de matrices hermitiennes positives. Donc elle est hermitienne positive.

3. Groupes d'ordre p^2

Soit p un nombre premier.

a. Donner, à isomorphisme près, tous les groupes abéliens d'ordre p^2. On pensera à justifier que les groupes présentés comme distincts sont 2 à 2 non isomorphes.

Réponse. En application du théorème de classification du cours G est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^2$ ou $\mathbb{Z}/p^2\mathbb{Z}$. Le deuxième de ces groupes contient un élément d'ordre p^2, le premier non. Ils ne sont donc pas isomorphes.

Le but de l'exercice est de montrer qu'enlever l'hypothèse d'abélianité ne permet pas de construire d'autre groupes de cardinal p^2.

Un sous-groupe H d'un groupe G sera dit *central* si tout élément de H commute avec tout élément de G.

b. Soit G un groupe et H un sous-groupe central de G.

(1) Montrer que H est distingué dans G.

Réponse. Pour tout $g \in G$ et $h \in H$, on a $ghg^{-1} = hgg^{-1} = h \in H$. Donc H est distingué.

(2) On suppose que G/H est cyclique. Montrer qu'il existe $a \in G$ tel que toute classe à gauche de G/H peut s'écrire a^kH pour un entier k et en déduire que G est abélien.

Réponse. Soit a dans G dont la classe aH engendre G/H. Alors pour tout bH il existe k tel que $Hb = bH = (aH)^k = a^kH$.

c. Soit p un nombre premier et G un groupe d'ordre p^2.

(1) Soit $g_0 \in G$. Et soit $H_0 := \{z \in G, zg_0 = g_0 z\}$ le centralisateur de g_0. On considère l'application $\varphi : G/H_0 \to G$, donnée par $\varphi(\bar{g}) = gg_0g^{-1}$. Montrer que l'application φ est bien définie et qu'elle est injective.

Réponse. Soit g_1 et g_2 dans G tels que $g_1H_0 = g_2H_0$. Alors il existe $h \in H_0$ tel que $g_2 = g_1h$. Alors $g_2g_0g_2^{-1} = g_1hg_0h^{-1}g_1^{-1} = g_1g_0g_1^{-1}$. Donc φ est bien définie.
Soit g_1 et g_2 dans G tels que $\varphi(g_1H) = \varphi(g_2H)$. Alors $g_1g_0g_1^{-1} = g_2g_0g_2^{-1}$. En multipliant à gauche et à droite par g_1^{-1} et g_1, il vient $g_0 = g_1^{-1}g_2g_0g_2^{-1}g_1 = (g_2^{-1}g_1)^{-1}g_0(g_2^{-1}g_1)$. Donc $g_2^{-1}g_1 \in H_0$. Ceci montre l'injectivité.

(2) En déduire que le cardinal d'une classe de conjugaison est une puissance de p.

Réponse. La classe de conjugaison de g_0 est l'image de φ. Son cardinal est donc égal à celui de G/H_0, c'est-à-dire à $\frac{|G|}{|H_0|}$. En particulier, il divise $|G| = p^2$ et est donc une puissance de p.

(3) Pourquoi l'ensemble des classes de conjugaison forment-elles une partition de G ? Montrer qu'il existe un élément g_0 qui commute avec tout G, autre que l'élément neutre.

Réponse. Les classes de conjugaison sont les orbites de l'action de G sur lui-même par conjugaison. Elles forment donc une partition de G.
On déduit de cette partition que le cardinal de G est la somme des cardinaux des classes de conjugaison. Ces classes ont pour cardinal 1, p ou p^2. Soit k le nombre de classes de conjugaison et $c_1, \ldots, c_k$ leurs cardinaux rangés par ordre croissant. Comme la classe de l'élément neutre est de cardinal 1, $c_1 = 1$.
Si par l'absurde, aucun élément non trivial ne commute à tous les éléments de G alors les c_i pour $i \geq 2$ sont différents de 1, c'est-à-dire égaux à p ou p^2. Or $p^2 = |G| = \sum_i c_i = 1 + \sum_{i\geq 2} c_i$. On a une contradiction ($\bar{0} = \bar{1}$) en réduisant modulo p cette égalité.

d. Montrer que G est abélien.

Réponse. On reprend l'argument précédent. Puisque $p^2 = |G| = \sum_i c_i = 1 + \sum_{i\geq 2} c_i$, les c_k valent 1 ou p (p^2 est impossible). Le nombre de $i \in \{1, \ldots, k\}$ tels que c_i est congru à 0 modulo p. Donc il est égal à p ou p^2.
S'il est égal à p^2, cela signifie que toutes les classes de conjugaison sont des singletons. Donc que G est abélien.
Supposons qu'il est égal p. Notons Z l'ensemble des éléments h dont la classe est de cardinal 1, c'est-à-dire tels que $gh = hg$ pour tout $g \in G$. Alors Z est un sous-groupe de cardinal p. Soit g_0 dont la classe est de cardinal p. Bien sûr, $g_0 \notin Z$. De plus, le H_0 de la question c.(1) contient Z et g_0. Donc H_0 est de cardinal au moins $p+1$. Puisque ce cardinal divise p^2, il vaut p^2. Donc la classe de conjugaison de g_0 est réduite à un élément. Contradiction.

4. Une question de cours

Soit G un groupe abélien fini et g un élément de G différent de l'élément neutre. Montrer que

$$\sum_{\chi \in \hat{G}} \chi(g) = 0.$$

Réponse. Le groupe H engendré par g est un groupe cyclique de cardinal $r \geq 2$. Il existe un caractère χ_0 de H tel que $\chi_0(g)$ est une racine ω primitive r^{ime} de l'unité. Par le lemme d'extension du cours, il existe un caractère $\tilde{\chi}_0$ de G tel que $\tilde{\chi}_0(g) = \chi_0(g)$.
Considérons l'application $\hat{G} \longrightarrow \hat{G}, \chi \longmapsto \tilde{\chi}_0\chi$. Comme $\hat{G}$ est un groupe, cette application est une bijection. En réindéxant la somme de l'énoncé grâce à cette bijection on trouve

$$S := \sum_{\chi \in \hat{G}} \chi(g) = \sum_{\chi \in \hat{G}} \tilde{\chi}_0\chi(g) = \tilde{\chi}_0(g) \sum_{\chi \in \hat{G}} \chi(g) = \tilde{\chi}_0(g)S.$$

Comme $\tilde{\chi}_0(g) \neq 1$, on en déduit que $S = 0$.