Université Claude Bernard Lyon 1
M1G de mathématiques : algèbre
Année 2023–2024

Rappels d'algèbre linéaire et premières représentations.

I Rappels sur le polynôme minimal et la diagonalisation

On fixe un $\mathbb{C}$-espace vectoriel V de dimension finie et on considère un endomorphisme u de V.

1° Polynômes d'endomorphismes

a) Soit P un polynôme de $\mathbb{C}[X]$. Rappeler la définition de $P(u)$.
b) Soit Q un autre polynôme de $\mathbb{C}[X]$, vérifier que $(P+Q)(u) = P(u)+Q(u)$ et que $(PQ)(u) = P(u) \circ Q(u)$.
c) Montrer que si P et Q sont premiers entre eux alors

$$\operatorname{Ker}(PQ)(u) = \operatorname{Ker} P(u) \oplus \operatorname{Ker} Q(u).$$

d) En déduire que les espaces propres de u sont en somme directe.

2° Polynôme minimal

a) Montrer que u admet un polynôme annulateur (non nul). Serait-ce nécessairement le cas, si V était de dimension infinie ?
b) Rappeler la définition du polynôme minimal de u. Justifier qu'il est unique.
Par la suite, on notera m_u le polynôme minimal de u.
c) Montrer que m_u divise tout polynôme annulateur de u.
d) Que vaut $m_{\lambda \mathrm{id}_V}$ pour λ nombre complexe ?
e) Calculer le polynôme minimal de la matrice $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathscr{M}_2(\mathbb{C})$.
f) Soit W un sous-espace vectoriel de V stable par u. Montrer que $m_{u_{\restriction W}}$ divise m_u.
g) En déduire que les valeurs propres de u correspondent aux racines de m_u.

3° Diagonalisation

On dit que u est diagonalisable s'il existe une base B de V telle la matrice de u dans B est diagonale.
a) Montrer que u est diagonalisable si et seulement s'il existe une base de V formée de vecteurs propres de u si et seulement si V est égal à la somme directe des espaces propres de u.
b) Montrer que u est diagonalisable si et seulement si m_u est à racines simples.
c) Cette dernière condition est-elle toujours suffisante si on remplace le corps $\mathbb{C}$ par $\mathbb{R}$ ou $\mathbb{F}_p$?

4° Aparté :polynôme caractéristique

a) Rappeler l'énoncé du théorème de Cayley-Hamilton.
b) Qu'en déduit-on entre m_u et le polynôme caractéristique de u ?

5° Diagonalisations simultanées

a) Soit v un endomorphisme de V qui commute avec u. Vérifier que les espaces propres de u sont stables par v.
b) En déduire que si u et v sont diagonalisables alors ils le sont dans une base commune.
c) On considère une famille $u_1, \ldots, u_r$ d'endomorphismes de V diagonalisables. Montrer que $u_1, \ldots, u_r$ sont simultanément diagonalisable (c.à.d. dans une base commune) si et seulement s'ils commutent deux à deux entre eux.

6° Deux applications des rappels précédents aux représentations (vues en cours)

Soit (ρ, V) une représentation d'un groupe fini G.

a) Montrer que pour tout $g \in G$, $\rho(g)$ est un automorphisme diagonalisable ayant comme valeurs propres des racines de l'unité.

b) Montrer de plus que si le groupe G est abélien et la représentation ρ est irréductible, alors cette représentation est de degré 1 (c.à.d. $\dim V = 1$).

c) Ces résultats resteraient-ils vrais si on remplace $\mathbb{C}$ par $\mathbb{R}$?

d) Donner un exemple de représentation matricielle $\rho : (\mathbb{Z}/2\mathbb{Z}, +) \to \mathrm{GL}_2(\mathbb{F}_2)$ tel que $\rho(\bar{1})$ est triangulaire non diagonalisable.

II Premiers exemples de représentations

1° Les groupes cycliques

a) Justifier que toute représentation (ρ, V) du groupe $(\mathbb{Z}/2\mathbb{Z}, +)$ correspond à la donnée d'une symétrie s sur V.

b) Généraliser le résultat précédent à tout groupe cyclique.

c) À quelle donnée correspond une représentation irréductible d'un groupe cyclique.

2° Représentations de degré 1 de $\mathfrak{S}_n$

a) Montrer qu'il n'y a que deux morphismes de $\mathfrak{S}_n$ vers $\mathbb{C}^*$.

b) En déduire les deux uniques représentations de degré 1 (à isomorphismes près).

3° Triangle équilatéral et groupe $\mathfrak{S}_3$

a) En considérant les symétries d'un triangle équilatéral, construire une représentation de degré 2 du groupe symétrique $\mathfrak{S}_3$.

b) En donner une réalisation matricielle à coefficients entiers.

c) Cette représentation est-elle irréductible ?

III Une représentation de $\mathfrak{S}_3$ (Inspiré du partiel de novembre 2021)

On considère le groupe $\mathfrak{S}_3$ d'ordre 6. On rappelle qu'il est engendré par $(1\,2\,3)$ et $(1\,2)$ et on admettra que si un groupe H contient deux éléments R et S d'ordres respectifs 3 et 2 tels que $SRS = R^{-1}$, il existe un morphisme $\varphi : \mathfrak{S}_3 \to H$ tel que $\varphi((1\,2\,3)) = R$ et $\varphi((1\,2)) = S$.

1. Vérifier qu'il existe une représentation matricielle $\rho : \mathfrak{S}_3 \to \mathrm{GL}_3(\mathbb{C})$ telle que
$$\rho((1\,2\,3)) = \begin{pmatrix} 0 & 2 & 1 \\ -1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} \quad \text{et} \quad \rho((1\,2)) = \begin{pmatrix} 1 & -1 & -2 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$
2. (a) Justifier rapidement que si ρ n'est pas irréductible, elle contient une sous-représentation de degré 1.
   (b) Montrer qu'il existe une telle sous-représentation si et seulement s'il existe un vecteur propre commun à $\rho((1\,2\,3))$ et $\rho((1\,2))$.
   (c) Démontrer que dans une telle sous-représentation, la restriction de $\rho((1\,2\,3))$ admet 1 comme valeur propre.
   (d) Vérifier que 1 est en effet valeur propre de $\rho((1\,2\,3))$ et déterminer l'espace propre correspondant que l'on notera V_1.
   (e) Vérifier que V_1 est une sous-représentation de $(\rho, \mathbb{C}^3)$ de degré 1 (c.à.d. un sous-espace stable de dimension 1).
   Identifier (à isomorphisme près) la représentation obtenue (ρ_1, V_1).
   (f) Justifier que (ρ_1, V_1) est l'unique sous-représentation de degré 1 de $(\rho, \mathbb{C}^3)$.
3. En déduire qu'il existe une sous-représentation irréductible (ρ_2, V_2) de degré 2 de $(\rho, \mathbb{C}^3)$ telle que $\mathbb{C}^3 = V_1 \oplus V_2$. En donner une réalisation matricielle.

IV Dualité en algèbre linéaire et représentation duale

On fixe un $\mathbb{C}$-espace vectoriel V de dimension finie.
a) Rappeler la définition de l'espace dual de V noté V^*.
Soit $(e_1, \ldots, e_n)$ une base de V. On considère la famille de formes linéaires $(e_1^*, \ldots, e_n^*)$ définie par

$$\forall i, j \in \{1, \ldots, n\},\ e_i^*(e_j) = \delta_{ij} \text{ où } \delta_{ij} \text{ est le symbole de Kronecker.}$$

b) Expliciter les formes linéaires $(e_1^*, \ldots, e_n^*)$ dans le cas où $V = \mathbb{C}^n$ et $(e_1, \ldots, e_n)$ est sa base canonique.
c) Montrer que $(e_1^*, \ldots, e_n^*)$ est une base de V^* et en déduire un isomorphisme entre V et V^*.
d) Cet isomorphisme est-il canonique (c.à.d. est-il indépendant de la base choisie $(e_1, \ldots, e_n)$) ?
Soit u un endomorphisme de V.
e) Montrer que l'application ${}^t u : V^* \to V^*,\ \ell \mapsto \ell \circ u$ est un endomorphisme de V^*.
f) Vérifier que si u est un automorphisme de V alors ${}^t u$ est un automorphisme de V^* d'inverse ${}^t(u^{-1})$.
g) Montrer que la matrice de ${}^t u$ dans la base $(e_1^*, \ldots, e_n^*)$ est égale à la transposée de celle de u dans la base $(e_1, \ldots, e_n)$.
Soit (ρ, V) une représentation d'un groupe fini G. On définit

$$\rho^* : G \to \mathrm{GL}(V^*),\ g \mapsto {}^t\rho_V(g)^{-1}.$$

h) Montrer que (ρ^*, V^*) est une représentation de G.
i) Soit $g \in G$. En choisissant une base de diagonalisation de $\rho(g)$, montrer que

$$\operatorname{tr} \rho^*(g) = \overline{\operatorname{tr} \rho(g)}.$$

Autrement dit, le caractère de ρ^* est égal au conjugué du caractère de ρ, c'est-à-dire

$$\chi_{V^*} = \overline{\chi_V}.$$

j) [Isomorphisme canoniqe avec le bidual] À tout vecteur $v \in V$, on associe « naturellement » la forme linéaire sur V^* : $\lambda_V : V^* \to \mathbb{C},\ \ell \mapsto \ell(v)$.
Montrer que l'application $\lambda : V \to V^{**},\ v \mapsto \lambda_v$ est un isomorphisme.

A Glossaire

représentation :

- une *représentation d'un groupe (fini)* G est un couple (ρ, V) où V est un espace vectoriel complexe de dimension finie non réduit à $\{0\}$ et $\rho : G \to \mathrm{GL}(V)$ est un morphisme de groupes ; autrement dit, il s'agit d'une action de G sur V par applications linéaires ;
- dans la littérature, une représentation (ρ, V) pourra être notée (V, ρ) et par abus, on sous-entend souvent ρ et on parle de « la représentation V » ;
- parfois, on désignera ou on définira une représentation (ρ, V) par uniquement un morphisme $\rho_V : G \to \mathrm{GL}(V)$;
- par identification de $\mathrm{GL}_n(\mathbb{C})$ et $\mathrm{GL}(\mathbb{C}^n)$, un morphisme $\rho : G \to \mathrm{GL}_n(\mathbb{C})$ définit une représentation $(\rho, \mathbb{C}^n)$ de G que l'on appellera *représentation matricielle* de G ;
- étant donnée une représentation (ρ, V) de G, le choix d'une base B de V induit un morphisme $G \to \mathrm{GL}(\mathbb{C}^n),\ g \mapsto \mathrm{Mat}_B(\rho(g))$, qui est une représentation matricielle de G isomorphe à (ρ, V) ;

degré d'une représentation : le *degré* d'une représentation (ρ, V) est simplement la dimension de V ;

morphisme de représentations (ou opérateurs d'entrelacement) : étant données deux représentations (ρ, V) et (ρ', V'), un *morphisme de représentations* est une application linéaire $\varphi : V \to V'$ telle que $\rho'(g) \circ \varphi = \varphi \circ \rho(g)$ pour tout g de G, i.e. qui fait commuter tous les diagrammes

$$\begin{tikzcd} V \arrow[r, "\varphi"] \arrow[d, "\rho(g)"'] & V' \arrow[d, "\rho'(g)"] \\ V \arrow[r, "\varphi"] & V' \end{tikzcd}$$

les morphismes de représentations forment un sous-espace vectoriel de $\mathrm{Hom}(V, V')$ que l'on notera $\mathrm{Hom}(\rho_V, \rho_{V'})$ (il est souvent noté dans la littérature $\mathrm{Hom}_{\mathbb{C}G}(V, V')$) ;

isomorphisme de représentations : un *isomorphisme de représentations* est un morphisme de représentations bijectif ;

sous-représentation : étant donnée une représentation (ρ, V), on dit que qu'un sous-espace W de V est *stable (ou G-invariant)* s'il est stable par tous les $\rho(g)$ $(g \in G)$; dans ce cas, on obtient *ipso facto* une *sous*-représentation $\rho_W : G \to \mathrm{GL}(W)$ en prenant pour $\rho_W(g)$ l'endomorphisme induit par la restriction de $\rho(g)$ à W ; par abus, on dira que W est une *sous-représentation* de (ρ, V) ;

représentation irréductible : une représentation (ρ, V) est *irréductible* si elle a pour unique sous-représentation elle-même ;

somme directe de deux représentations : étant données deux représentations (ρ_1, V_1) et (ρ_2, V_2), on obtient une représentation $(\rho_1 \oplus \rho_2, V_1 \oplus V_2)$ où

— la somme directe $V_1 \oplus V_2$ correspond à l'espace vectoriel des couples (v_1, v_2) et

— le morphisme $\rho_1 \oplus \rho_2 : G \to \mathrm{GL}(V_1 \oplus V_2)$ est défini par

$$(\rho_1 \oplus \rho_2)(g)(v_1, v_2) = \big(\rho_1(g)(v_1), \rho_2(g)(v_2)\big) \ \ (g \in G,\ v_1 \in V_1,\ v_2 \in V_2);$$

dans une base B de $V_1 \oplus V_2$ construite à partir des bases B_1 et B_2 de V_1 et V_2, on obtient alors pour tout $g \in G$

$$\mathrm{Mat}_B((\rho_1 \oplus \rho_2)(g)) = \begin{pmatrix} \mathrm{Mat}_{B_1}(\rho_1(g)) & 0 \\ 0 & \mathrm{Mat}_{B_2}((\rho_2(g)) \end{pmatrix};$$

représentation $\mathrm{Hom}(V, W)$: étant données deux représentations (ρ, V) et (π, W), on obtient une représentation $(\mathrm{Hom}_{\rho,\pi}, \mathrm{Hom}(V, W))$ où le morphisme $\mathrm{Hom}_{\rho,\pi} : G \to \mathrm{GL}(\mathrm{Hom}(V, W))$ est défini par

$$\mathrm{Hom}_{\rho,\pi}(g)(\varphi) = \pi(g) \circ \varphi \circ \rho(g^{-1}) \ \ (g \in G,\ \varphi \in \mathrm{Hom}(V, W));$$

lemme de Schur : un morphisme non nul entre deux représentations irréductibles est un isomorphisme ; un endomorphisme de représentation est une homothétie ;

théorème de Maschke : dans une représentation complexe de dimension finie (V, ρ) d'un groupe fini G, tout sous-espace stable par les $\rho(g)$ $(g \in G)$ admet un supplémentaire stable ; un corollaire est que toute représentation complexe de dimension finie peut s'écrire comme somme directe de représentations irréductibles ;

caractère d'une représentation : — le *caractère* d'une représentation (ρ, V) est la fonction $\chi_V : G \to \mathbb{C}$, $g \mapsto \mathrm{tr}\, \rho(g)$;

— c'est une fonction *de classe* (de conjugaison), i.e. on a $\chi_V(g) = \chi_V(g')$ si g et g' sont conjugués ;

— le caractère *caractérise* la représentation, c'est-à-dire, deux représentations (ρ, V) et (π, W) sont isomorphes si et seulement si $\chi_V = \chi_W$;

— $\chi_{V \oplus W} = \chi_V + \chi_W$;

— $\chi_{\mathrm{Hom}(V,W)} = \overline{\chi_V} \chi_W$.