AUTOUR DE LA DUALITÉ

par

Christophe Mourougane

1. Définitions et premières propriétés

Nous travaillerons essentiellement toujours sur un corps commutatif, mais on peut donner la

Définition. — *Si A est un anneau et M un A-module à gauche, son dual $M^\star$ est par définition le A-module à droite $M^\star := Hom_A(M, A)$ l'ensemble des morphismes de A-modules de M vers A considéré comme A-module à gauche sur lui-même, muni de la loi externe*

$$\begin{array}{rcl} M^\star \times A & \to & M^\star \\ (\varphi, \lambda) & \mapsto & \varphi \cdot \lambda = \left\{ \begin{array}{ccc} M & \to & A \\ x & \mapsto & (\varphi \cdot \lambda)(x) = \varphi(x) \cdot_A \lambda. \end{array} \right. \end{array}$$

Exercice. — *Vérifier avec les notations précédentes que $\varphi \cdot \lambda$ est un morphisme de A-modules.*

Exercice. — *Expliciter un (anti)-isomorphisme et son inverse entre A et $A^\star$.*

Remarques 1.1. —
1. Comme $\mathbb{Z}$ est un anneau intègre, le dual des $\mathbb{Z}$-modules $\mathbb{Z}/n\mathbb{Z}$ est le module nul.
2. En utilisant les matrices élémentaires ($trace(A^tE_{ij}) = a_{ij}$), on montre que l'application

$$\begin{array}{rcl} M_n(k) & \to & M_n(k)^\star \\ A & \mapsto & \left\{ \begin{array}{ccc} M_n(k) & \to & k \\ X & \mapsto & trace(A^tX) \end{array} \right. \end{array}$$

est injective puis que c'est un isomorphisme de k-espaces vectoriels. (Une autre démonstration est possible sur $\mathbb{R}$).
3. Si $(M_i)_{i\in I}$ est une famille de A-modules à gauche indexée par un ensemble I quelconque, le dual de $\oplus_{i\in I} M_i$ est

$$(\oplus_{i\in I} M_i)^\star \;\simeq\; \prod_{i\in I} M_i^\star$$

car la quantité $\sum_I \varphi_i(x_i)$ est bien définie si (x_i) est une famille presque nulle. En général, $\left(\prod_{i\in I} M_i\right)^\star \not\simeq \oplus_{i\in I} M_i^\star$ Il y a une injection naturelle de $\oplus_{i\in I} M_i^\star$ dans $\left(\prod_{i\in I} M_i\right)^\star$. Mais elle n'est pas surjective en général. Si e est un vecteur non nul d'un k-espace vectoriel E, on note u_e le vecteur $(e, e, ..., e, ...)$ de $E^{\mathbb{N}}$ et F un supplémentaire de ku_e. La forme linéaire qui s'annule sur F et qui à xu_e associe x n'est pas à support sur les vecteurs presque nuls et n'est donc pas dans la somme directe des $E^\star$.

4. Si E est un espace vectoriel normé, le dual topologique E' (des formes linéaires continues) est un sous-espace vectoriel du dual (algébrique) $E^\star$.

Exercice. — *Soit A une matrice carrée de $M_n(\mathbb{R})$ telle que pour toute matrice X de trace nulle, $trace(A^tX) = 0$. Montrer que A est une matrice scalaire.*

Définition. — *Si M est un A-module libre de rang fini n et si $\mathcal{B} = (e_1, \cdots, e_n)$ est une base de E alors l'application $e_i^{\mathcal{B}\star} = e_i^\star : E \to A$ définie sur les éléments de la base $\mathcal{B}$ par $e_i^\star(e_j) = \delta_{ij}$ est une forme linéaire sur E (qui dépend du choix de la base $\mathcal{B}$ et pas seulement de e_i) et le n-uplet $(e_1^\star, \cdots, e_n^\star)$ est une base de $E^\star$, appelée base duale de $\mathcal{B}$. En particulier on a alors l'égalité de dimension* $\dim E^\star = \dim E$.

Exercice. — *Le $\mathbb{Z}$-module $\mathbb{Z}/n\mathbb{Z}$ a-t-il une $\mathbb{Z}$-base ?*

Définition. — *La transposée ${}^tu$ d'une application A-linéaire à gauche $u : E \to F$ est l'application A-linéaire à droite*

$$\begin{aligned} {}^tu : F^\star &\to E^\star \\ \varphi &\mapsto \varphi \circ u. \end{aligned}$$

Exercice. — *Montrer que la matrice de ${}^tu : F^\star \to E^\star$ dans les bases duales $(f_1^\star, \cdots, f_m^\star)$ et $(e_1^\star, \cdots, e_n^\star)$ est la transposée de celle de $u : E \to F$ dans les bases $(e_1, \cdots, e_n)$ et $(f_1, \cdots, f_m)$.*

2. Dualité, Orthogonalité

Définition. — *Il y a une forme bilinéaire naturelle*

$$\begin{aligned} M^\star \times M &\to A \\ (\varphi, x) &\mapsto \varphi(x). \end{aligned}$$

On dit que $x \in E$ et $\varphi \in E^\star$ sont orthogonaux (pour la dualité naturelle) si $\varphi(x) = 0$. L'orthogonal N' d'un sous-module N d'un A-module à gauche M est

$$N' := \{\varphi \in M^\star,\ \forall x \in N,\ \varphi(x) = 0\}$$

L'orthogonal ${}'F$ d'un sous-module F de $M^\star$ est

$${}'F := \{x \in M,\ \forall \varphi \in F,\ \varphi(x) = 0\}.$$

Si M est un A-module à gauche et N un sous-A-module à gauche de M, notons $\pi : M \to M/N$ la projection naturelle. Alors

$$\begin{aligned} (M/N)^\star &\to N' \\ \psi &\mapsto \psi \circ \pi \end{aligned}$$

est un isomorphisme, l'isomorphisme inverse étant donné par le théorème de factorisation.

On note que si le sous-A module N admet un supplémentaire, l'application de restriction $M^\star \to N^\star$ est surjective et a pour noyau N'. On obtient alors $N^\star \simeq M^\star/N'$.

3. Lien avec les formes bilinéaires

Si E et F sont deux k-espaces vectoriels toute forme bilinéaire $b : E \times F \to k$ donne lieu à $b_d : E \to F^\star$, $x \mapsto b(x, \cdot)$ et $b_g : F \to E^\star$, $y \mapsto b(\cdot, y)$. Inversement, toute application $u : E \to F^\star$ détermine une forme bilinéaire $b_u : E \times F \to k$, $(x, y) \mapsto (u(x))(y)$.

Deux endomorphismes $u \in End(E)$ et $v \in End(F)$ sont dit adjoints pour la forme bilinéaire b si

$$\forall (x, y) \in E \times F, b(u(x), y) = b(x, v(y)) \iff b_d \circ u = {}^t v \circ b_d \iff {}^t u \circ b_g = b_g \circ v.$$

Si E est de dimension finie et si b est non dégénérée, tout endomorphisme admet un unique adjoint $u^\star := b_g^{-1} \circ {}^t u \circ b_g$.

Exercice. — *Déterminer la forme bilinéaire associée à l'application*

$$\begin{array}{ccc} M_n(k) & \to & M_n(k)^\star \\ A & \mapsto & trace(A^t.). \end{array}$$

4. Bidual

Si E est un k-espace vectoriel (plus généralement si E est un A-module qui admet une base), ayant fixé une base $\mathcal{B} = (e_i)_{i \in I}$ l'application $j : E \to E^\star$ définie sur la base $\mathcal{B}$ par $j(e_i) = e_i^\star$ est injective, mais dépend du choix de $\mathcal{B}$.

Par contre,

$$\begin{array}{rccc} \varepsilon_E : & E & \to & E^{\star\star} \\ & x & \mapsto & \left\{ \begin{array}{ccc} E^\star & \to & A \\ \varphi & \mapsto & \varphi(x) \end{array} \right. \end{array}$$

est une application A-linéaire canonique, injective si E admet une base.

Exercice. — 1. *Montrer que si $u : E \to F$ est une application linéaire le diagramme*

$$\begin{array}{ccc} E & \xrightarrow{u} & F \\ \varepsilon_E \downarrow & & \downarrow \varepsilon_F \\ E^{\star\star} & \xrightarrow{{}^{tt}u} & F^{\star\star} \end{array}$$

commute.

2. *Vérifier que ${}^t\varepsilon_E \circ \varepsilon_{E^\star} = Id_{E^\star}$. En particulier déterminer un supplémentaire naturel de $E^\star$ dans $E^{\star\star\star}$.*

5. Propriétés

On supposera désormais sauf pour quelques remarques que A est un corps commutatif noté alors k. En particulier, par le théorème de la base incomplète tout sous-espace vectoriel d'un espace vectoriel admet un supplémentaire. Si $E \neq \{0\}$, on choisit une base de E et la base duale donne des formes linéaires non-nulles. Ainsi, $E = \{0\} \iff E^\star = \{0\}$.

Exercice. — *Le sous-module $2\mathbb{Z}/8\mathbb{Z}$ du $\mathbb{Z}$-module $\mathbb{Z}/8\mathbb{Z}$ admet-il un supplémentaire ?*

Proposition 5.1. — *Soit E un k espace vectoriel et F et G deux sous-espaces vectoriels. Alors,*

(i) $(F + G)' = F' \cap G'$.
(ii) $(F \cap G)' = F' + G'$.

(iii) *Si $F' = G'$ alors $F = G$.*
(iv) $'(F') = F$.

Pour un sous-espace F de $M^\star$ l'inclusion $F \subset ('F)'$ est en général stricte. (Les sous-espaces de $M^\star$ de la forme N' sont ceux qui sont fermés pour la topologie de la convergence simple.)

Démonstration. — (ii) Montrons l'inclusion $(F \cap G)' \subset F' + G'$. On écrit $E = (F \cap G) \oplus A \oplus B \oplus C$ où A (resp.B) est un supplémentaire de $F \cap G$ dans F (resp. G) et C un supplémentaire de $F + G$ dans E. L'espace dual de la somme $E = (F \cap G) \oplus A \oplus B \oplus C$ se présente sous forme de produit $(F \cap G)^\star \times A^\star \times B^\star \times C^\star$. Les formes linéaires sur E sont alors de la forme $f = (t, a, b, c)$ avec $a \in A^\star, b \in B^\star, c \in C^\star$. Il suffit alors de remarquer que les éléments de $(F \cap G)'$ sont de la forme $(0, a, b, c)$ et s'écrivent $(0, a, 0, 0) + (0, 0, b, c)$ avec $(0, a, 0, 0) \in G'$ et $(0, 0, b, c) \in F'$.
(iv) On montre $('(F'))' = F'$ et on utilise (iii).

$\square$

Proposition 5.2. — *Soit u une application linéaire de E vers F.*
(i) *u surjectif $\iff$ ${}^t u$ injectif et plus généralement $(Imu)' = \ker {}^t u$*
(ii) *u injectif $\iff$ ${}^t u$ surjectif et plus généralement $(\ker u)' = Im {}^t u$.*
(iii) $u = 0 \iff {}^t u = 0$.

Démonstration. —
(i) $\varphi \in \ker({}^t u) \iff \varphi \circ u = 0 \iff \varphi \in (Imu)'$ et si u est surjectif, ceci implique que φ est nulle.
(ii) Si u est injectif, il existe $v : F \to E$ telle que $v \circ u = Id_E$. Alors ${}^t u \circ {}^t v = Id_{E^\star}$ et ${}^t u$ est donc surjectif.
(iii) Le sens direct est facile.
(i) Réciproquement, si ${}^t u$ est injectif, on considère $p : F \to C = cokeru = F/Imu$. Alors $p \circ u = 0$ et donc ${}^t u \circ {}^t p$ est nulle mais réalise une injection de $C^\star$ dans $E^\star$. Donc $C^\star = \{0\}$. Par (iv), $C = \{0\}$, et u est donc surjective.
(ii) Si ${}^t u$ est surjectif, on considère $\ker u \hookrightarrow E \to F$.
(iii) Si ${}^t u = 0$, on considère $E \to Imu \hookrightarrow F$. $\square$

Exercice. — *Donner des démonstrations en considérant des supplémentaires.*

Exercice. — *Etudier la surjectivité de la transposée de la multiplication par 2 dans le $\mathbb{Z}$-module $\mathbb{Z}$.*

6. Application aux systèmes linéaires

Soit

$$\begin{cases} \varphi_1(x_1, x_2, \cdots, x_n) &= b_1 \\ \varphi_2(x_1, x_2, \cdots, x_n) &= b_2 \\ \cdots\cdots\cdots & \\ \varphi_m(x_1, x_2, \cdots, x_n) &= b_m \end{cases}$$

un système linéaire à n inconnues et m équations. Supposons que les k premières formes linéaires $(\varphi_i)_{1 \leq i \leq k}$ soit linéairement indépendantes et engendrent $vect(\varphi_i)_{1 \leq i \leq m}$. Ecrivons pour $k+1 \leq j \leq m$, $\varphi_j = \sum_{1 \leq i \leq k} \lambda_{ij} \varphi_i$. Si X est une solution, pour tout $k+1 \leq j \leq m$, $b_j = \varphi_j(X) = \sum_{1 \leq i \leq k} \lambda_{ij} \varphi_i(X) = \sum_{1 \leq i \leq k} \lambda_{ij} b_i$.

Réciproquement, si ces conditions sont satisfaites, en complétant la famille libre $(\varphi_i)_{1\leq i\leq k}$ en une base de $(k^n)^\star$ et en considérant la base duale $(f_1, f_2, \cdots, f_n)$ le vecteur $X = b_1 f_1 + b_2 f_2 + \cdots + b_k f_k$ est une solution.

Exercice. — *Montrer que sur le sous-espace de k^m des données consistentes $(b_l)_{1\leq l\leq m}$ il existe une application linéaire $u \; : \; (b_l)_{1\leq l\leq m} \mapsto (x_i = \sum c_{ij}b_j)_{1\leq i\leq n}$ telle que $u(b)$ soit solution du système avec second membre (b_l).*

7. Application à l'écriture en blocs cycliques

Une matrice cyclique (ou matrice compagnon) est une matrice carrée de la forme

$$\begin{pmatrix} 0 & 0 & 0 & & & & & -a_0 \\ 1 & 0 & & & & & & -a_1 \\ 0 & 1 & 0 & & & & & -a_2 \\ 0 & 0 & 0 & \ddots & & & & \\ & & \vdots & & \ddots & & & \\ & & & \cdots & \cdots 1 & 0 & & \\ & & \vdots & & & & \ddots & \\ 0 & & 0 & & & & 1 & -a_{n-1} \end{pmatrix}$$

Son polynôme caractéristique égal à son polynôme minimal est $X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$.

Proposition 7.1. — *Pour tout endomorphisme $u \; : E \to E$ d'un k espace vectoriel E, il existe une base dans laquelle la matrice de u est diagonale par bloc, chaque bloc étant cyclique. On peut même assurer que le polynôme minimal du premier bloc est le polynôme minimal de u et que le polynôme minimal du bloc $i+1$ divise celui du bloc i.*

Démonstration. — Si le polynôme minimal de u est de degré k, il existe un vecteur y tel que $(y_i = u^{i-1}(y))_{1\leq i\leq k}$ est libre. On la complète en une base de E, on prend la base duale et on note $y_k^\star$ le dual de y_k. L'idée importante est de constater alors que $vect(y_k^\star, {}^t\!u(y_k^\star), \cdots ({}^t\!u)^{k-1}(y_k^\star))$ est stable par ${}^t\!u$ et que son orthogonal est alors un supplémentaire de $vect(y_i)_{1\leq i\leq k}$ aussi stable par u. □

Exercice. — *Compléter la démonstration précédente.*

Théorème 7.2. — *Soit a et b deux endomorphismes de E tel que tout endomorphisme u de E commutant avec a commute avec b. Alors b est un polynôme en a.*

Exercice. — *Le but est de démontrer le théorème précédent.*

1. *Montrer que les sous-espaces cycliques $E_i = vect(e_i, a(e_i), \cdots a^{k_i-1}(e_i))$ d'une décomposition cyclique de a sont stables par b.*
2. *Montrer qu'il existe g_i polynôme tel que pour tout $x \in E_i$, $b(x) = g_i(a)(x)$.*
3. *On écrit le polynôme minimal p_i du bloc E_i et $p_1 = p_i q_i$. On considère l'endomorphisme u_i de E qui envoie $a^l(e_i)$ sur $(q_i(X)X^l)(a)(e_1)$ et laisse fixe les vecteurs des autres espaces cycliques E_j. Montrer que u_i commute avec a, que $u_i b(e_i) = q_i g_i(a)(e_1)$ et $bu_i(a)(e_i) = q_i g_1(e_1)$.*
4. *Montrer que $b = g_1(a)$*

---

3 février 2010

CHRISTOPHE MOUROUGANE