QUELQUES POINTS D'ALGÈBRE (LINÉAIRE)

par Daniel Ferrand, et avec relecture par Michel Coste (Février 2008)

... le langage et les méthodes des $K[X]$-modules de type fini ne sont pas véritablement compris.
(Rapport du jury, 1997, p. 132)

1. Modules

Si A est un anneau, une structure de A-module sur un groupe abélien M consiste en une application $A \times M \to M$, qui sera notée $(a, x) \mapsto a.x$, vérifiant les propriétés 1 à 4 suivantes :

1. $\forall a \in A, \quad \forall x \in M, \quad \forall y \in M, \quad a.(x + y) = a.x + a.y.$
   L'application $x \mapsto a.x$ respecte donc la loi de groupe de M ; autrement dit, cette structure est la donnée d'une application
   $$\rho : A \longrightarrow \mathrm{End}(M).$$
2. $\forall a \in A, \quad \forall b \in A, \quad \forall x \in M, \qquad (a + b).x = a.x + b.x.$
   Autrement dit, à la somme dans A, l'application ρ fait correspondre la somme d'endomorphismes : $\rho(a + b) = \rho(a) + \rho(b)$.
3. $\forall a \in A, \quad \forall b \in A, \quad \forall x \in M, \qquad (ab).x = a.(b.x).$
   Autrement dit, au produit dans A, ρ fait correspondre la composition des endomorphismes :$\rho(ab) = \rho(a) \circ \rho(b)$.
4. $\forall x \in M, \qquad 1.x = x.$
   Ou encore : $\rho(1) = \mathrm{Id}_M$.

Bref, une structure de A-module sur le groupe abélien M est exactement un *morphisme d'anneaux* (unitaires)

$$\rho : A \longrightarrow \mathrm{End}(M).$$

Pour un A-module M et un idéal $I \subset A$, on note IM le sous-module de M formé des sommes finies $\sum a_i x_i$, avec $a_i \in I$ et $x_i \in M$; lorsque I est monogène, c'est-à-dire si $I = aA$, alors $IM = aM$.

Si $IM = 0$, c'est-à-dire si $ax = 0$ pour tout $a \in I$ et tout $x \in M$, alors on a $I \subset \mathrm{Ker}(\rho)$, de sorte que ρ se factorise en

$$A \longrightarrow A/I \longrightarrow \mathrm{End}(M);$$

autrement dit, M est un A/I-module.

Lorsque $A = K$ est un corps (commutatif), une structure de K-module n'est rien d'autre qu'une structure de K-espace vectoriel.

Rappelons qu'une K-algèbre est un anneau A muni d'un morphisme d'anneaux unitaires $\alpha : K \to A$ tel que $\alpha(K)$ soit dans le centre de A ; comme K est un corps, un tel morphisme est injectif dès que A est non nul (c'est-à-dire dès que $1_A \neq 0_A$), et permet donc d'identifier K au sous-corps $\alpha(K) \subset A$; si A et B sont des K-algèbres, un *morphisme de K-algèbres* $f : A \to B$ est un morphisme d'anneaux qui est l'identité sur le sous-corps K.

Soient M un K-espace vectoriel, et A une K-algèbre. Lorsqu'on considèrera une structure de A-module sur M, il sera toujours sous-entendu qu'elle prolongera sa structure d'espace vectoriel, ce qui s'écrit :

$$\forall \lambda \in K, \quad \forall x \in M, \qquad \lambda.x = \lambda x.$$

En vertu de la propriété 3, le fait que λ soit dans le centre de A implique que pour tout $a \in A$, on a $a.(\lambda x) = (a\lambda).x = (\lambda a).x = \lambda(a.x)$; autrement dit, que $\rho(a)$ est K-linéaire. En notant $\mathrm{End}_K(M) \subset \mathrm{End}(M)$ la K-algèbre des endomorphismes K-linéaires de M, on supposera donc toujours que ρ est un morphisme *de K-algèbres :*

$$\rho : A \longrightarrow \mathrm{End}_K(M).$$

2. Le $K[T]$-module associé à un endomorphisme

Dans toute la suite K désigne un corps et V un K-espace vectoriel de dimension finie.

On va développer l'idée suivante :

La donnée d'une application K-linéaire $u : V \to V$ équivaut à la donnée d'une structure de $K[T]$-module sur V.

Nous désignerons souvent par $u.x$ l'image $u(x)$ de x par u.
À un endomorphisme $u \in \mathrm{End}_K(V)$ est associé un unique morphisme de K-algèbres

$$\rho : K[T] \longrightarrow \mathrm{End}_K(V),$$

caractérisé par la condition : $\rho(T) = u$. L'image par ρ du polynôme $p(T) = a_0 + a_1 T + \cdots + a_n T^n \in K[T]$ est donc l'endomorphisme $p(u) = a_0 \mathrm{Id}_V + a_1 u + \cdots a_n u^n$ (Il faut peut-être insister sur le fait que u^0 est l'application identique de V, et que pour $n \geq 1$, u^n est le n-ième itéré de u). L'image du produit pq de deux polynômes est le composé des endomorphismes ; cela s'écrit

$$(pq)(u) = p(u) \circ q(u).$$

La structure de $K[T]$-module sur V peut aussi être décrite par l'application

$$K[T] \times V \longrightarrow V, \qquad (p(T), x) \mapsto p(u).x.$$

Lorsqu'on munit V de cette structure de $K[T]$-module associée à u, on le note V_u, et on parle simplement du *module* V_u.
L'image du morphisme ρ est notée par $K[u] \subset \mathrm{End}_K(V)$; c'est la sous-K-algèbre de $\mathrm{End}_K(V)$ engendrée par u, c'est-à-dire l'ensemble des endomorphismes de V qui s'expriment comme des polynômes en u.

Voici quelques traductions de notions liées à u en les notions équivalentes dans le langage des modules :

2.1 *Sous-espace stable*

« W est un sous-module de V_u » signifie : « W est un sous-espace vectoriel de V, stable sous u ».

2.2 *Annulateur*

Pour un polynôme $p \in K[T]$, les propriétés suivantes sont équivalentes :
- $p(T)$ annule V_u ;
- pour tout $x \in V, p(u).x = 0$;
- $p(u) = 0$;
- le morphisme $\rho : K[T] \longrightarrow \mathrm{End}_K(V)$ passe au quotient et se factorise par $K[T]/(p) \longrightarrow \mathrm{End}_K(V)$;
- V_u est un $K[T]/(p)$ -module.

Lorsque $p(T) = T - \lambda$, cette condition signifie que pour tout $x \in V$, $\quad u(x) = \lambda x$; noter qu'alors $K[T]/(p)$ est isomorphe à K, et que, justement, l'isomorphisme est celui qui envoie T sur λ (encore un exemple où dire que deux objets sont isomorphes sans donner l'isomorphisme, fait perdre toute l'information importante).

À un polynôme q, on peut associer *deux* modules annulés par q :

- Le sous-espace $\mathrm{Ker}(q(u))$.
- Le quotient $V/q(u)V$, où on note $q(u)V$ le sous-espace formé des éléments $q(u).x$ pour x parcourant V ; c'est le sous-espace image $\mathrm{Im}(q(u))$ de l'endomorphisme $q(u)$; comme ce sous-espace est stable pour u, l'endomorphisme u passe au quotient et définit un endomorphisme de $V/q(u)V$, lequel endomorphisme est annulé par q.

Dans certains cas, les deux modules $\mathrm{Ker}(q(u))$ et $V/q(u)V$ sont isomorphes (voir plus bas le lemme des noyaux).

2.3 *Polynôme minimal*

Comme V est de dimension finie, le noyau du morphisme $\rho : K[T] \longrightarrow \mathrm{End}_K(V)$, c'est-à-dire l'annulateur du module V_u, est un idéal principal qui est non nul puisque $\mathrm{End}_K(V)$ est de dimension finie sur K, et pas $K[T]$; il est donc engendré par un unique polynôme unitaire, nommé le *polynôme minimal* de u, et noté μ_u, ou π_u, et ici plus simplement m ; l'espace V_u est donc un $K[T]/(m)$-module. Par définition de m, le morphisme

$$K[T]/(m) \longrightarrow \mathrm{End}_K(V)$$

est injectif, de sorte qu'on obtient un isomorphisme de K-algèbres

$$K[T]/(m) \quad \xrightarrow{\sim} \quad K[u].$$

Supposons que le polynôme minimal m soit irréductible dans $K[T]$, de sorte que le quotient $L = K[T]/(m)$ soit un corps ; V_u doit être alors vu comme un L-espace vectoriel, et, par exemple, les sous-espaces stables sous u sont exactement les sous-L-espaces vectoriels.

2.4 *Sous-espace cyclique*

« V_u est un module monogène » signifie : « il existe $x \in V$ tel que pour tout $y \in V$ il existe un polynôme $p \in K[T]$ tel que $y = p(u).x$ », c'est-à-dire : « il existe $x \in V$ tel que l'espace vectoriel V soit engendré par la famille $\{x, u.x, u^2.x, \ldots\}$ ».

Si m désigne le polynôme minimal de u, ceci équivaut aussi à : il existe $x \in V$ tel que l'application $K[T] \to V$ définie par $p(T) \mapsto p(u).x$, passe au quotient et donne un *isomorphisme de $K[T]/(m)$-modules*

2.4.1
$$\varphi_x : K[T]/(m) \quad \xrightarrow{\sim} \quad V_u.$$

2.4.2 Proposition *Si V_u est cyclique l'ensemble de ses sous-espaces stables est fini. Réciproquement, si cet ensemble est fini et si le corps K est infini, alors V_u est cyclique.*

Posons $A = K[T]/(m)$, choisissons un générateur $x \in V$, comme ci-dessus, et considérons l'isomorphisme 2.4.1 $\varphi_x : A \xrightarrow{\sim} V_u$
Les sous-espaces u-stables de V correspondent via φ_x aux sous-espaces de A stables sous le produit par un quelconque polynôme, c'est-à-dire aux *idéaux de l'anneau* A. Comme A est le quotient de $K[T]$ par l'idéal engendré par m, les idéaux de A correspondent bijectivement à ceux de $K[T]$ qui contiennent m, c'est-à-dire finalement aux *diviseurs unitaires* de m, puisque $K[T]$ est principal. Ils sont en nombre fini.

Réciproquement, supposons que l'ensemble des sous-espaces u-stables de V soit fini, et soient $W_1, \ldots, W_s$ ceux qui sont *distincts de* V. Comme K est infini (il suffirait que K contienne plus de s éléments, voir Gourdon p. 110), la réunion de ces sous-espaces est distincte de V. Considérons alors un élément x de V qui ne soit dans aucun de ces W_i. Le sous-espace $\mathrm{Im}(\varphi_x) = Ax$ est stable et n'est contenu dans aucun des W_i. C'est donc V.□

2.4.3 Supposons toujours que V_u soit cyclique, de générateur x. Notons t la classe de T dans $A = K[T]/(m)$, de sorte que les éléments de A sont de la forme $p(t)$; l'application 2.4.1 s'écrit alors

$$\varphi_x(p(t)) = p(u).x.$$

Soit $v : V \to V$ un endomorphisme K-linéaire ; comme φ_x est surjective, il existe un polynôme $p(T)$ tel que $v.x = p(u).x$. Montrons que si v commute avec u, alors, pour tout $y \in V$, on a $v.y = p(u).y$, c'est-à-dire $v = p(u)$: en effet, la surjectivité de φ_x implique que tout élément y est de la forme $y = q(u).x$; on a donc

$$v.y \;=\; vq(u).x \;\overset{vu=uv}{=}\; q(u)v.x \;=\; q(u)p(u).x \;\overset{qp=pq}{=}\; p(u)q(u).x = \; p(u).y.$$

Ainsi, lorsque V est cyclique pour u, le sous-anneau de $\mathrm{End}_K(V)$ formé des endomorphismes qui commutent avec u (ce qu'on nommera plus bas le *commutant*) est formé des polynômes en u. Noter que la réciproque est vraie : si le commutant de u est formé des polynômes en u, alors V est cyclique pour u. Mais ceci est un théorème ! (voir §6)

3. Le lemme des noyaux et des quotients

Dans $K[T]$, soit $q = q_1 q_2 \ldots\ q_s$ la décomposition d'un polynôme q en produit de polynômes q_i premiers entre eux deux à deux. Le théorème chinois indique un isomorphisme d'anneaux

$$K[T]/(q) \;\xrightarrow{\sim}\; K[T]/(q_1) \times \ldots \times K[T]/(q_s).$$

On allègera l'écriture de cet isomorphisme en :

3.1 $$A \;\xrightarrow{\sim}\; A_1 \times \ldots \times\ A_s.$$

Soit $u : V \to V$ un endomorphisme tel que $q(u) = 0$ de sorte que V est un A-module. Le classique « lemme des noyaux » énonce que tout A-module se décompose en une somme directe de A_i-modules. Plus précisement, l'application canonique

3.2 $$\bigoplus_i \mathrm{Ker}(q_i(u)) \;\xrightarrow{\sim}\; V,$$

est un isomorphisme.

Il faut voir le théorème chinois et le lemme des noyaux comme deux faces de la même propriété. Voici comment.

En considérant les ensembles d'applications A-linéaires de chacun des membres de 3.1 dans V, on obtient un isomorphisme

3.3 $$\mathrm{Hom}_A(A,V) \quad \widetilde{\leftarrow} \quad \mathrm{Hom}_A(A_1,V)\oplus\cdots\oplus\mathrm{Hom}_A(A_s,V).$$

Or, une application $\alpha : A \to V$, si elle est A-linéaire est entièrement déterminée par $\alpha(1) = x$, puisque $\alpha(a) = a\alpha(1) = a.x$. Par suite l'application $\mathrm{Hom}_A(A,V) \to V, \quad \alpha \mapsto \alpha(1)$, est un isomorphisme.

On constate tout aussi simplement qu'une application A-linéaire $\alpha : A_i = K[T]/(q_i) \to V$ est déterminée par l'élément $\alpha(1) \in V$, soumis à la seule condition d'être annulé $q_i(u)$; on a donc un isomorphisme

$$\mathrm{Hom}_A(K[T]/(q_i),V) \quad \widetilde{\to} \quad \mathrm{Ker}(q_i(u)),$$

ce qui s'écrit aussi

$$\mathrm{Hom}_A(A_i,V) \quad \widetilde{\to} \quad \mathrm{Ker}(q_i(u)).$$

Ainsi, l'isomorphisme 3.2 est-il une réécriture de 3.3, et ce dernier est une conséquence théorème chinois 3.1.

Après les noyaux, il convient de considérer les images, et les quotients, et d'appliquer le théorème chinois directement à V.
En effet, comme les polynômes $q_i(T)$ sont deux à deux premiers entre eux, la relation de Bézout montre que les sous-espaces $\mathrm{Im}(q_i(u)) = q_i(u)V$ sont deux à deux étrangers, au sens suivant : pour $i \neq j$, on a $q_i(u)V + q_j(u)V = V$; le théorème chinois implique que l'application

$$V \quad \longrightarrow \quad V/q_1(u)V \oplus\cdots\oplus V/q_s(u)V$$

est surjective.

On pourrait vérifier directement que le noyau de cette application, c'est-à-dire $\cap_i q_i(u)V$ est égal à $q(u)V = 0$, et donc que c'est un isomorphisme, mais on va plutôt le déduire d'une remarque importante parce qu'elle relie entre eux ces différents points de vue.

On va montrer en effet que pour chaque i, l'application composée

(⋆) $$\mathrm{Ker}(q_i(u)) \quad \subset \quad V \quad \longrightarrow \quad V/q_i(u)V$$

est un isomorphisme.

Fixons donc un indice i ; les polynômes $p_i = q/q_i$ et q_i sont premiers entre eux ; il existe donc, d'après Bézout, des polynômes $r_i, s_i \in K[T]$ tels que

3.4 $$1 \quad = \quad r_i(T)p_i(T) + s_i(T)q_i(T).$$

Ainsi, pour tout $x \in V$, on a

$$x \quad = \quad r_i(u)p_i(u).x + s_i(u)q_i(u).x.$$

Soit $x = q_i(u).y$ un élément de $q_i(u)V$; comme $p_i(u)q_i(u) = q(u) = 0$, on a $x = s_i(u)q_i(u).x$; si on a, de plus, $x \in \mathrm{Ker}(q_i(u))$, alors $x = 0$; ainsi, $\mathrm{Ker}(q_i(u)) \cap q_i(u)V = 0$, et cela entraîne l'injectivité de l'application composée (*) ; la formule du rang montre que l'on a même une décomposition en somme directe

$$V \quad = \quad \mathrm{Ker}(q_i(u)) \oplus \mathrm{Im}(q_i(u)).$$

Cela montre la surjectivité de l'application (*).

L'égalité de Bézout 3.4 a une autre conséquence : posons $\varepsilon_i(T) = r_i(T)p_i(T)$; ce polynôme vérifie les congruences suivantes

$$\varepsilon_i \ \equiv\ 0 \bmod. q_j,\ \text{pour}\, j \neq i, \qquad \text{et} \qquad \varepsilon_i \ \equiv\ 1 \bmod. q_i.$$

(La première congruence vient de ce que q_j divise p_i lorsque $j \neq i$). On en déduit immédiatement les relations : $\sum_i \varepsilon_i \equiv 1$ mod.q et $q_i\varepsilon_i \equiv 0$ mod.q. Par suite, dans le lemme des noyaux, l'égalité

$$\sum_i \varepsilon_i(u).x \ =\ x$$

précise l'isomorphisme 3.2, en montrant, en particulier, que la composante $\varepsilon_i(u).x \in \mathrm{Ker}(q_i(u))$ s'obtient à l'aide d'un polynôme en u.

En conclusion, il convient de mettre en regard le lemme des noyaux et un « lemme des quotients », formellement analogue au théorème chinois, et de considérer simultanément les deux décompositions suivantes.

$$\bigoplus_i \mathrm{Ker}(q_i(u)) \quad \xrightarrow{\sim} \quad V \quad \xrightarrow{\sim} \quad \bigoplus_i V/q_i(u)V.$$

4. Endomorphismes semi-simples.

Soient, comme plus haut, V un espace vectoriel de dimension finie sur un corps K, et $u : V \to V$ un endomorphisme K-linéaire ; on note $A = K[u] \subset \mathrm{End}_K(V)$ la sous-K-algèbre formée des polynômes en u.

On dit que u est *semi-simple* si tout sous-espace de V stable par u admet un supplémentaire stable ; il revient au même de dire que tout sous-A-module de V_u admet un sous-A-module supplémentaire. Si A est un corps, c'est-à-dire si le polynôme minimal de u est irréductible, alors u est semi-simple. Plus généralement,

4.1 Proposition *Avec les notations qui précèdent, les propriétés suivantes sont équivalentes :*
i) L'endomorphisme u est semi-simple ;
ii) l'anneau $A = K[u]$ est réduit (i.e son seul élément nilpotent est 0) ;
iii) le polynôme minimal de u est produit de polynômes unitaires irréductibles distincts.

i $\Rightarrow$ *ii* : Soit $\alpha \in A = K[u]$ un élément nilpotent et W un A-module supplémentaire de $\alpha(V)$, d'où la décomposition $V = \alpha(V) \oplus W$; tout $x \in V$ s'écrit donc sous la forme $x = y + z$, avec $y \in \alpha(V)$ et $z \in W$; comme W est stable, on a $\alpha(z) \in W$, et par suite $\alpha(x - y) = \alpha(z) \in \alpha(V) \cap W = 0$; ainsi, $\alpha(x) = \alpha(y) \in \alpha^2(V)$; bref, $\alpha(V) = \alpha^2(V)$. Comme α est supposé nilpotent, on en déduit $\alpha(V) = 0$, c'est-à-dire $\alpha = 0$.

ii $\Rightarrow$ *iii* : Soit m le polynôme minimal de u, de sorte qu'on a un isomorphisme

$$K[X]/(m) \quad \xrightarrow{\sim} \quad K[u].$$

S'il existait un polynôme q non constant et tel que q^2 divise m, on pourrait écrire $m = pq^2$; la classe modulo m du polynôme pq serait non nulle et de carré nul, et $K[u]$ ne serait pas réduit.

iii $\Rightarrow$ *i* : Ecrivons la décomposition du polynôme minimal en produit de polynômes unitaires irréductibles distincts :

$$m = m_1 \dots . m_s.$$

Soit $W \subset V$ un sous-espace stable ; en appliquant le lemme des noyaux à V et à W on obtient les décompositions

$$\bigoplus_i \mathrm{Ker}(m_i(u)) \quad \widetilde{\longrightarrow} \quad V,$$

$$\bigoplus_i \mathrm{Ker}(m_i(u)) \cap W \quad \widetilde{\longrightarrow} \quad W.$$

Par définition, l'espace $\mathrm{Ker}(m_i(u))$ est annulé par $m_i(u)$, c'est donc un module sur l'anneau quotient $A_i = K[T]/(m_i(T))$, lequel est un corps puisque les m_i sont irréductibles ; bref, $\mathrm{Ker}(m_i(u))$ est un A_i-espace vectoriel, et son sous-espace $\mathrm{Ker}(m_i(u)) \cap W$ admet un A_i-espace supplémentaire W_i'. Force est alors de constater que $W' = \bigoplus W_i'$ est un supplémentaire de W dans V, qui est stable sous u.

5. Quelques polynômes caractéristiques

Soit $\chi_u(T) = \det(T\mathrm{Id}_V - u) = T^d + a_{d-1}T^{d-1} + \dots + a_0$ le polynôme caractéristique de u. La K-algèbre $R = K[T]/(\chi_u)$ admet pour base la famille $1, t, t^2, \dots, t^{d-1}$, où t désigne la classe de T dans R, et où $d = \dim(V)$; dans cette base la matrice de la multiplication par t est la fameuse matrice compagne de χ_u

5.1
$$\begin{pmatrix} 0 & 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & 0 & \dots & 0 & -a_2 \\ \vdots & & & & \vdots & \\ 0 & & & \dots & 0 & -a_{d-2} \\ 0 & & & \dots & 1 & -a_{d-1} \end{pmatrix}$$

Le polynôme caractéristique de cette matrice est égal à χ_u (On peut le vérifier directement, par exemple par récurrence ; mais on peut aussi remarquer que χ_u est visiblement le polynôme minimal de cette matrice, et il a le bon degré pour être égal au polynôme caractéristique).

Par définition, le K-vectoriel R est cyclique pour l'endomorphisme $r \mapsto tr$; cela montre, entre autre, qu'en général, il n'est pas isomorphe au vectoriel V muni de u. Cependant, on a le résultat important suivant, désigné parfois sous le nom de « théorème spectral ». Dans l'énoncé, on écrit $\det_R$ et $\det_V$ pour signaler clairement les espaces où opèrent les endomorphismes.

5.2 Proposition *Pour tout polynôme $q(T) \in K[T]$, on a*

$$\det{}_R(r \mapsto q(t)r) \;=\; \det{}_V(q(u)).$$

Plus généralement, le polynôme caractéristique de l'application $r \mapsto q(t)r$, et celui de $q(u)$ sont égaux.

Dans la suite l'application $R \to R$, $r \mapsto q(t)r$ sera simplement notée $q(t)$; avec cette convention, χ_t est le polynôme caractéristique de la matrice compagne, et on peut donc écrire $\chi_t = \chi_u$; la seconde partie de la proposition s'écrit $\chi_{q(t)} = \chi_{q(u)}$.

Cette deuxième assertion se déduit d'ailleurs de la première : supposons d'abord que le corps K soit infini. Pour tout $\lambda \in K$, la première égalité appliquée au polynôme $\lambda - q(T)$, donne $\det_R(\lambda - q(t)) = \det_V(\lambda \mathrm{Id}_V - q(u))$, c'est-à-dire

$$\chi_{q(t)}(\lambda) \ = \ \chi_{q(u)}(\lambda).$$

Comme cette égalité est vraie pour tous les $\lambda \in K$, et que K est infini, les polynômes $\chi_{q(t)}(T)$ et $\chi_{q(u)}(T)$ sont égaux.

En général, et en particulier si le corps K est fini, il faut considérer l'extension de corps $K \to K(X)$, et choisir une base de V ; cela permet d'identifier u à une matrice à coefficients dans K, donc, *a fortiori*, à coeffficients dans le corps $K(X)$; on applique alors l'égalité des déterminants au polynôme $X - q(T) \in K(X)[T]$ (c'est un polynôme en T, puisque X est dans le corps de base $K(X)$).

Démontrer la première assertion consiste à vérifier l'égalité de deux éléments de K ; comme toute extension de corps $K \to L$ est un morphisme injectif, on peut « grossir » le corps de base autant que nécessaire pour simplifier la situation. On peut décomposer soit le polynôme χ_u, soit le polynôme $q(T)$. Les deux procédés sont instructifs.
1) Première méthode : décomposer χ_u.

Soit $K \to L$ une extension de décomposition du polynôme caractéristique, de sorte que dans $L[T]$, on a

$$\chi_u(T) \ = \ \prod_i (T - \alpha_i).$$

On ne prétend évidemment pas que les valeurs propres soient distinctes.
Démontrons d'abord directement l'énoncé suivant qui apparaîtra plus bas comme un corollaire de la proposition.

5.3 Corollaire *Supposons que le polynôme caractéristique de u soit scindé : $\chi_u(T) = \prod_i (T - \alpha_i)$. Alors pour tout polynôme $q(T)$, on a $\det_V(q(u)) = \prod q(\alpha_i)$.*

On peut en effet trouver une base de V relativement à laquelle la matrice de u est trigonale supérieure à termes diagonaux les α_i ; on constate alors immédiatement que la matrice de $q(u)$ relativement à cette même base est trigonale supérieure à termes diagonaux les $q(\alpha_i)$, ce qui montre que $\det_V(q(u)) = \prod q(\alpha_i)$.□

Revenons à la démonstration de 5.2. On applique 5.3 d'une part à l'espace vectoriel R muni de la multiplication par t, et d'autre part à V muni de u ; ces deux endomorphismes ont χ_u pour polynôme caractéristique, comme il a été rappelé ; si ce dernier est scindé, le corollaire montre que $\det_R(q(t)) = \prod q(\alpha_i)$, et que $\prod q(\alpha_i) = \det_V(q(u))$; d'où l'égalité annoncée.□

2) Deuxième méthode : décomposer $q(T)$.
En passant à une extension de décomposition de q, on peut supposer que $q(T) = a \prod (T - \beta_i)$. Comme le déterminant est multiplicatif, il suffit de vérifier l'égalité de 5.2 lorsque q est de la forme $q(T) = T - \beta$; mais alors, $\det_R(t - \beta) = (-1)^d \det_R(\beta - t) = (-1)^d \chi_u(\beta)$. De même, $q(u) = u - \beta$, de sorte que $\det_V(u - \beta) = (-1)^d \det(\beta - u) = (-1)^d \chi_u(\beta)$; cela donne l'égalité cherchée.□

5.4 Remarque La conclusion de 5.2 reste vraie si K est un anneau (commutatif) et si V est un K-module libre de rang d ; le second procédé donne encore une démonstration à condition d'être légèrement modifié : par division euclidienne par le polynôme unitaire χ_u, on peut supposer d'abord que q est de degré $< d$; on remarque ensuite qu'on ne change pas la conclusion en remplaçant q par $p(T) = q(T) + \chi_u(T)$; mais ce polynôme p est *unitaire* de degré d ; à ce titre il admet un morphisme de décomposition $K \to L$

qui est un K-module libre ; le morphisme $K \to L$ est donc injectif. La fin de la démonstration est inchangée.

5.5 Corollaire *Le polynôme caractéristique et le polynôme minimal ont les mêmes racines (dans une extension convenable du corps de base K).*

En effet, comme le polynôme minimal $m(T)$ divise le polynôme caractéristique, toute racine de m est racine de χ_u. Par ailleurs, comme $m(u) = 0$, on a $\chi_{m(u)}(T) = T^d$; mais, si on note $\alpha_1, \ldots, \alpha_d$ les racines de χ_u (dans une extension de K), le résultat qui précède montre que $\chi_{m(u)}(T) = \prod(T - m(\alpha_i))$, donc que pour tout i, $m(\alpha_i) = 0$.□

On peut aussi terminer la démonstration de la façon suivante : la proposition 5.2 montre que $\chi_{m(t)}(T) = \chi_{m(u)}(T) = T^d$; par suite, la multiplication par $m(t)$ dans R est nilpotente ; cela équivaut à la propriété suivante :

Le polynôme caractéristique divise une puissance du polynôme minimal.

Cette assertion est équivalente à 5.5.

6. Commutant et bicommutant

On pose ici de nouveau $A = K[T]$, et on considère le A-module V_u.

Pour un endomorphisme $v \in \mathrm{End}_K(V)$, la relation de commutation $uv = vu$ se traduit simplement en : « v est A-linéaire. »
Ainsi, le commutant de u est-il le sous-anneau $C = \mathrm{End}_A(V_u) \subset \mathrm{End}_K(V)$ (Malgré son nom, le commutant n'est pas, en général, un anneau commutatif ; par exemple, si u est une homothétie, u commute avec tout autre endomorphisme, donc le commutant de u est l'anneau $\mathrm{End}_K(V)$ tout entier).

Le bicommutant est l'anneau formé des endomorphismes K-linéaires de V qui commutent avec tous le éléments de C, soit $\mathrm{End}_C(V)$.

6.1 Proposition *Le bicommutant de u est l'anneau $K[u]$.*

La démonstration utilise la décomposition, due à Frobenius, de V_u en somme directe d'espaces cycliques. Il existe, en effet, un isomorphisme de A-modules

$$V_u \simeq A_1 \oplus A_2 \oplus \ldots \oplus A_s, \tag{6.1.1}$$

où $A_i = A/p_iA$, et où les polynômes p_i vérifient les relations $p_i \mid p_{i+1}$. Le dernier polynôme de la liste, p_s est donc le polynôme minimal de u, et on a un isomorpisme de K-algèbres $K[u] \simeq A_s$.

Soit f un élément du bicommutant, c'est-à-dire une application qui commute avec celles qui sont A-linéaires ; on va raisonner sur le membre de droite de 6.1.1. Montrons d'abord que f est diagonal au sens où il envoie le facteur A_i sur lui-même : soit π_i la projection sur ce facteur, c'est-à-dire l'endomorphisme A-linéaire défini par

$$\pi_i(a_1 + \ldots + a_s) = a_i.$$

Par hypothèse, on a $f \circ \pi_i = \pi_i \circ f$; cela se traduit simplement en : $f(A_i) \subset A_i$; de plus, comme f est A-linéaire, la restriction de f à A_i est simplement la multiplication par un élément $\alpha_i \in A_i$. Par ailleurs, comme p_i divise p_s, on dispose des morphismes de passage au quotient $A_s \to A_i$; ce sont des applications A-linéaires ; comme f doit commuter avec ces morphismes, l'image de α_s dans A_i est égale à α_i ; l'application f est donc égale à la multiplication par α_s ; c'est un élément de $A_s = K[u]$. □

Pour déterminer le commutant, posons

$$C_{ij} = \mathrm{Hom}_A(A_j, A_i),$$

(l'inversion de l'ordre des indices est délibérée !). Alors l'isomorphisme

$$C := \mathrm{End}_A(A_1 \oplus \ldots \oplus A_s) = \prod_{i,j} C_{ij}$$

est plus explicite si on voit C comme un tableau (une matrice) de modules

$$C = \begin{pmatrix} C_{11} & C_{12} & \ldots & C_{1s} \\ C_{21} & C_{22} & \ldots & C_{2s} \\ \vdots & & & \vdots \\ C_{s1} & C_{s2} & \ldots & C_{ss} \end{pmatrix}$$

Il faut donc déterminer ces modules C_{ij}. Plus généralement, soient p et q des éléments d'un anneau principal A ; une application A-linéaire $A/pA \to A/qA$ est déterminée par l'image de 1, c'est-à-dire par la classe mod. q d'un élément $a \in A$, et la seule contrainte sur a est que

$$ap \in qA.$$

On voit immédiatement que a doit être un multiple de $\mathrm{ppcm}(p,q)/p$, ou encore, un multiple de $q/\mathrm{pgcd}(p,q)$.

Supposons que p divise q, c'est-à-dire que $q = pr$, donc que $\mathrm{pgcd}(p,q) = p$. Précisons les modules $\mathrm{Hom}_A(A/pA, A/qA)$ et $\mathrm{Hom}_A(A/qA, A/pA)$. Pour le premier, on a l'isomorphisme (de A-modules)

$$A/pA \quad \widetilde{\longrightarrow} \quad \mathrm{Hom}_A(A/pA, A/qA), \qquad 1 \mapsto (x \bmod p \ \longmapsto \ (q/p)x \bmod q)$$

Pour le second, l'inclusion $qA \subset pA$ montre qu'il existe une application canonique $A/qA \to A/pA$, à savoir le morphisme surjectif d'anneaux associé à cette inclusion ; on a donc un isomorphisme de A-modules

$$A/pA \quad \widetilde{\longrightarrow} \quad \mathrm{Hom}_A(A/qA, A/pA), \qquad 1 \mapsto (x \bmod q \ \longmapsto \ x \bmod p)$$

Revenant aux C_{ij}, et compte-tenu de l'hypothèse $p_k \mid p_l$ pour $k \leq l$, on a donc un isomorphisme

$$C_{ij} \ \simeq \ A_{\inf(i,j)}.$$

Le commutant est donc isomorphe (comme A-module) à la matrice (de A-modules)

$$\begin{pmatrix} A_1 & A_1 & A_1 & A_1 & \ldots & A_1 \\ A_1 & A_2 & A_2 & A_2 & \ldots & A_2 \\ A_1 & A_2 & A_3 & A_3 & \ldots & A_3 \\ \vdots & \vdots & \vdots & & & \vdots \\ A_1 & A_2 & A_3 & & \ldots & A_s \end{pmatrix}$$

(Les A_i sont disposés « en équerre »). Lorsqu'on utilise cet isomorphisme, il ne faut pas oublier que le produit dans l'anneau C est donné par les applications usuelles $C_{ij} \times C_{jk} \to C_{ik}$ provenant de la composition des applications

$$(A_j \to A_i, \quad A_k \to A_j) \longmapsto \quad A_k \to A_j \to A_i.$$

Mais celles-ci sont perturbées par les isomorphismes $C_{ij} \simeq A_{\inf(i,j)}$ dégagés plus haut ; ainsi, par exemple, l'application $A_1 \times A_1 \to A_1$, associée à $C_{12} \times C_{21} \to C_{11}$ est celle à laquelle on pense d'abord, mais multipliée par p_2/p_1.

Pour le calcul de la dimension de C, la nature du produit dans C n'intervient heureusement pas, et l'isomorphisme indiqué suffit ; il montre que A_1 apparaît $2s-1 = 2(s-1)+1$ fois ; A_2 apparaît $2(s-2)+1$ fois, etc. Finalement, on trouve la *dimension du commutant* :

$$\dim_K(C) = \sum_{i=1}^{s} (2(s-i)+1) \deg(p_i).$$

Comme $\sum \deg(p_i) = \dim_K(V)$, cette formule montre en particulier que $\dim(C) \geq \dim(V)$ et qu'on a l'égalité si et seulement si V_u est cyclique (i.e $s = 1$).