# ALGEBRE
# CHAPITRE 6 (ETAT 6)
# §5 - ENDOMORPHISMES DES ESPACES VECTORIELS

Rédaction n° 090

Nombre de pages : 23

Nombre de feuilles : 23



Algèbre Chapitre VI

Etat 6

Endomorphismes d'Espaces vectoriels

$\boxed{90}$

~~Schwartz-Girard~~ - Delsarte 2 (dans l'ordre)

ALGEBRE - Chapitre 6 (Etat 6)

A 90

## §5 - Endomorphismes des espaces vectoriels .



APPENDICE - Endomorphismes semblables sur un anneau .



---

## Commentaires .

Le rédacteur a suivi autant qu'il était possible les instructions de la Tribu (notamment en ce qui concerne les n° 1,2 et 6) . Il a trouvé commode de subdiviser le reste en 3 numéros (3,4,5 sauf erreur) , les deux derniers étant d'ailleurs parfaitement interchangeables . Les seules innovations sont :

a) Une définition en forme pour les endomorphismes réductibles à la forme diagonale .

b) Une proposition en petits caractères (Prop.10) pour dire que la décomposition chérie de Chevalley peut se faire sur un corps parfait et pas seulement sur un algébriquement clos (il me semble qu'on en a besoin) . Le congrès jugera si on doit la mettre en gros caractères , ou la vider . Dans tous les cas , démission !

c) Le polynome caractéristique d'un produit tensoriel a été calculé au moyen de la décomposition locale (ou primaire , ou ...etc) et non au moyen de la forme triangulaire . Mais le rédacteur s'en fout .

d) Dans l'Appendice , le rédacteur a essayé d'expliciter la démonstration du th. d'Hamilton-Cartan due à Henri Cayley . Mal lui en a pris , car il a eu besoin d'un tas (2) de formules sur les produits intérieurs qui avaient été gracieusement oubliées au Chap.III; dans ces conditions , il propose d'abandonner H-C à son triste sort et de vider le n°3 de l'Appendice .

Enfin , le rédacteur s'est persuadé expérimentalement que l'on ne gagnerait rien à vouloir remettre la "montagne tensorielle" au début du paragraphe 5 : le seul avantage serait de supprimer les 11 lignes de démonstration de la prop.7 , et les inconvénients seraient tels qu'un lecteur "moyen" n'arriverait jamais à ladite prop.7 !

---

 3

## § 5 - Endomorphismes des espaces vectoriels .

Notations - Dans ce paragraphe , nous considérerons des espaces vectoriels , notés $E, F, \ldots$ , sur des corps commutatifs $k, K$ , ... dont les éléments seront désignés par des minuscules grecques , . Les endomorphismes de $E$ seront notés $u, v, \ldots$ . Enfin , si $u$ et $v$ sont deux endomorphismes de $E$ , et $x \in E$ , on écrira :

$u.x$ , $uv.x$ , $uv$ au lieu de : $u(x)$ , $(u_\circ v)(x)$ , $u_\circ v$ .

1 . Le module associé à un endomorphisme .

Soit $E$ un espace vectoriel de dimension finie sur un corps commutatif $K$ , et $u$ un endomorphisme de $E$ . Désignons par $K[X]$ l'algèbre des polynomes en une indéterminée $X$ sur le corps $K$ . Si $P(X) \in K[X]$, et si $x \in E$ , posons :

$$(I) \qquad P(X).x = P(u).x \quad .$$

On définit ainsi une application bilinéaire de $K[X] \times E$ dans $E$ qui définit sur $E$ une structure de $K[X]$-module unitaire . Nous désignerons $E$ , muni de cette structure , par $E_u$ (il est en effet évident que cette structure dépend de l'endomorphisme $u$ considéré) .

Réciproquement , tout $K[X]$-module $E'$ , qui est de dimension finie sur $K$ , peut être obtenu de cette façon : il suffit de considérer l'endomorphisme $u$ : $u.x = X.x$ .

Nous voyons ainsi que la donnée d'un couple $(E,u)$ est équivalente à celle d'un module $E_u$ ; cf. Chap. II, § 7 , n° 9 . Comme l'anneau $K[X]$ est un anneau principal (Chap. IV, § 1 , Prop. 7) , on peut appliquer à $E_u$ les résultats des paragraphes précédents , et étudier ainsi le couple $(E,u)$ . C'est ce que nous ferons dans ce n° .

Certains résultats de ce paragraphe peuvent être généralisés au cas où l'on ne suppose pas que $E$ est un espace vectoriel sur un corps $K$ , mais seulement que $E$ est un $A$-module unitaire , $A$ désignant un anneau commutatif ( Cf. Appendice).

Avant d'appliquer au module $E_u$ les résultats en question , il nous faut traduire certaines notions , du langage "modules" dans le langage "espace vectoriel à endomorphisme" . Ainsi :

"$V$ est sous-module de $E_u$" équivaut à : " $V$ est un sous-espace vectoriel de $E$ , stable pour $u$".

"$V$ est un sous-module monogène" équivaut à : "il existe $x \in V$ , tel que

 

V soit engendré (sur K) par les éléments $u^i.x$ $(i=0,1,2,\dots)$ ".

" $\mathfrak{a}$ est l'annulateur du sous-module V" équivaut à : "$\mathfrak{a}$ est l'idéal des polynomes $P(X) \in K[X]$ tels que pour tout $x \in V$, $P(u).x = 0$ ". Le polynome unitaire g tel que $\mathfrak{a} = (g)$ est dit le polynome minimal de la restriction de u à V.

"$E_u$ est monogène et d'annulateur $\mathfrak{a} = (g)$" (avec $g(X) = \alpha_0 + \dots + \alpha_{n-1}X^{n-1} + X^n$) équivaut à : " Il existe un élément $x \in E$, tel que les éléments $u^i.x$ $(i=0,1,\dots,n-1)$ forment une base de E, et que l'on ait : $g(u).x = 0$ ". Autrement dit, on peut trouver une base de E, telle que la matrice $\underline{U}$ de u par rapport à cette base soit la matrice:

$$(\mathrm{II}) \qquad \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & -\alpha_0 \\ 1 & 0 & 0 & \dots & 0 & -\alpha_1 \\ 0 & 1 & 0 & \dots & 0 & -\alpha_2 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 & -\alpha_{n-2} \\ 0 & 0 & 0 & \dots & 1 & -\alpha_{n-1} \end{pmatrix}.$$

Ceci étant on a d'abord :

LEMME 1. Soit E un espace vectoriel de dimension finie n sur un corps commutatif K, et soit u un endomorphisme de E. Le K[X]-module $E_u$, défini par la formule (I), est un module de torsion de type fini.

Soit $(e_i)$ $(1 \leq i \leq n)$ une base de E ; comme K[X] contient K, les $(e_i)$ forment un système de générateurs du K[X]-module $E_u$, qui est donc bien de type fini.

D'autre part, si $E_u$ n'était pas un module de torsion, il contiendrait un sous-module isomorphe à K[X], ce qui est impossible puisque K[X] est de dimension infinie sur K.

Nous allons maintenant traduire la décomposition d'un module de torsion de type fini qui fait l'objet du théorème 1 du 2 :

PROPOSITION 1 - Soit E un espace vectoriel de dimension finie n sur un corps commutatif K et u un endomorphisme de E dont le polynome minimal est q(X) ; pour tout polynome unitaire irréductible p(X) divisant q(X), soit $M_p$ le sous-espace vectoriel de E formé des éléments x tels que : $p(u)^N.x = 0$ pour N assez grand. Alors E est somme directe des $M_p$, et il existe des polynomes $s_p$ tels que, pour tout $x \in E$, le composant de x dans $M_p$ soit égal à $s_p(u).x$.

Remarque . D'après le § 2 , le polynome minimal de u sur $M_p$ est égal à la plus grande puissance de p qui divise q .

De même , ~~ax~~ d'après le th.2,§4 , le module $E_u$ est isomorphe à une somme directe de modules monogènes $F_j = K[X]/\mathfrak{a}_j$ $(j=1,\dots r)$ , où les idéaux $\mathfrak{a}_j$ sont distincts de $K[X]$, et tels que $\mathfrak{a}_j \subset \mathfrak{a}_{j+1}$ . On sait que les $\mathfrak{a}_j$ sont uniquement déterminés par les conditions précédentes . Comme , en outre , $E_u$ est de torsion , on a : $\mathfrak{a}_1 = (q) \neq 0$ ; comme $E_u$ est de dimension n , on a : $r \leqslant n$ . ~~XXXXXXXXXXXXXXXXXXXXXX~~ Posons $\mathfrak{a}_j = (h_j)$ $(1 \leqslant j \leqslant r)$ , $h_j$ étant un polynome unitaire , et considérons la suite de polynomes $(q_i)$ $(1 \leqslant i \leqslant n)$ définie par :

$$\text{(III)} \quad \begin{cases} q_i(X) = 1 & \text{si} \quad i \leqslant n-r \\ q_i(X) = h_{n-i+1}(X) & \text{si} \quad n-r < i \leqslant n . \end{cases}$$

Il est clair que la connaissance des polynomes $q_i$ est équivalente à celle des polynomes $h_j$ , et que l'on a encore :

$$E_u = \sum_i K[X]/(q_i) \text{ , cette somme étant directe.}$$

Traduisant ces résultats , on obtient :

PROPOSITION 2 - Soit E un espace vectoriel de dimension finie n sur un corps commutatif K et u un endomorphisme de E . Il existe n polynomes unitaires $q_i(X) \in K[X]$, tels que $q_i$ divise $q_{i+1}$ et que E soit somme directe de n sous-espaces $V_i$ , stables pour u , ~~XXXXXXXXXXXXXXXXXXXX~~ monogènes , et sur lesquels le polynome minimal de u est égal à $q_i$ . Les polynomes $q_i(X)$ sont déterminées de façon unique par les conditions précédentes , et $q_n = q$ n'est autre que le polynome minimal de u sur E .

Remarque - On peut aussi exprimer la proposition précédente en disant qu'il existe une base de E par rapport à laquelle u soit représentée par une matrice U de la forme :

$$\begin{pmatrix} A_1 & 0 & 0 & \dots & 0 & 0 \\ 0 & A_2 & 0 & \dots & 0 & 0 \\ 0 & 0 & A_3 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & A_{n-1} & 0 \\ 0 & 0 & 0 & \dots & 0 & A_n \end{pmatrix}$$

où chaque matrice $A_i$ est une matrice de la forme (II) , relative au polynome $g(X) = q_i(X)$ . En particulier , les matrices $A_i$ sont vides

?

(terminologie obscure)

pour $i \leqslant n-r$ , d'après les formules (III) .

DEFINITION 1 . Les notations étant celles de la proposition 2 , les $n$ polynomes unitaires $q_i(X)$ $(1 \leqslant i \leqslant n)$ sont appelés les invariants de similitude de l'endomorphisme $u$ (et de toute matrice $\underline{U}$ représentant $u$ par rapport à une base quelconque de $E$ ) .

Le n-ème invariant de similitude est donc le polynome minimal de $u$ (Prop.2) . Autrement dit , pour que $p(u)=o$ ,$p$ étant un polynome arbitraire de $K[X]$, il faut et il suffit que $p$ soit divisible par $q_n$.

La terminologie introduite est justifiée par le résultat suivant:

COROLLAIRE I - Pour que deux endomorphismes $u$ et $u'$ de deux espaces vectoriels $E$ et $E'$ de dimension finie (ou pour que les matrices $\underline{U}$ et $\underline{U}'$ de $u$ et $u'$ par rapport à des bases quelconques de $E$ et $E'$) soient semblables (chap.II, § 6,n°11) , il faut et il suffit qu'ils aient même invariants de similitude .

En effet dire que $u$ et $u'$ ont même invariants de similitude équivaut à dire que $E_u$ et $E'_{u'}$ sont isomorphes (§ 4,th.2) , c'est à dire qu'il existe un isomorphisme linéaire $g$ de $E$ sur $E'$ tel que $u' = gug^{-1}$, ce qui exprime justement que $u$ et $u'$ sont semblables .

COROLLAIRE 2 - Si les polynomes $q_i(X)$ $(1 \leqslant i \leqslant n)$ sont les invariants de similitude d'une matrice carrée $\underline{U}$ d'ordre $n$ sur un corps $K$ ,ce sont encore les invariants de similitude de $\underline{U}$ sur toute extension $K'$ de $K$ .

En effet , étant donnés $n$ polynomes $q_i$ tels que $q_i$ divise $q_{i+1}$ , dire que ce sont les invariants de similitude de $\underline{U}$ signifie que $\underline{U}$ est semblable (sur $K$) à un matrice $\underline{V}$ qui est une matrice diagonale de matrices de la forme (II) ,relatives aux $q_i$ ; il est clair que ceci reste valable , a fortiori , sur $K'$ .

COROLLAIRE 3 - Si deux matrices carrées à coefficients dans le corps commutatif $K$ sont semblables sur le corps $K'$ , extension de $K$ , elles le sont sur $K$ .

Cela résulte immédiatement des corollaires 1 et 2 ci-dessus .

Nous donnerons dans l'Appendice une méthode de calcul des invariants de similitude ; cette méthode mettra en évidence le fait que leurs coefficients se calculent rationnellement à partir des coefficients de la matrice .

Traduisons maintenant la proposition 7 du §4 , donnant la décomposition d'un module en somme directe de sous-modules indécomposables :

PROPOSITION 3 - Soit E un espace vectoriel de dimension finie n sur un corps commutatif K , et u un endomorphisme de E . Alors E est somme directe de sous-espaces $V_k$ , stables pour u , monogènes , et sur lesquels le polynome minimal de u est une puissance d'un polynome irréductible: $(p_k)^{n_k}$ . Dans une telle décomposition , le nombre de sous-espaces $V_k$ sur lesquels le polynome minimal de u est égal à $p^n$ (p polynome irréductible , $n \geqslant 1$) est déterminé de façon unique.

. La connaissance des $(p_k)^{n_k}$ est équivalente à celle des invariants de similitude de u : on passe des uns aux autres par le procédé expliqué au §4,n°8,Remarques. En outre , on passe immédiatement de la décomposition donnée dans la proposition 3 aux décompositions données dans les propositions 1 et 2 .

2 . Endomorphismes sur un corps de base algébriquement clos .

Supposons que le corps de base K soit algébriquement clos ; tout polynome unitaire irréductible sur K est alors de la forme :

$$p(X) = X - \alpha \qquad ( \alpha \in K ) ,$$

d'après la définition même des corps algébriquement clos (Chap.V, §4, déf.1) . Ceci permet d'énoncer la proposition 1 sous la forme suivante :

PROPOSITION 4 - Soit E un espace vectoriel de dimension finie n sur un corps K algébriquement clos , et u un endomorphisme de E dont le polynome minimal est q(X) . Pour tout $\alpha \in K$ , racine du polynome q , soit $M_\alpha$ le sous-espace vectoriel de E formé des éléments x tels que $(u-\alpha)^N.x = 0$ pour N assez grand . Alors E est somme directe des $M_\alpha$ et il existe des polynomes $s_\alpha$ tels que , pour tout $x \in E$ , le composant de x dans $M_\alpha$ soit égal à $s_\alpha(u).x$ .

On peut aussi exprimer les propriétés précédentes en disant que $u-\alpha$ <u>est nilpotent sur</u> $M_\alpha$ .

De même , K étant toujours supposé algébriquement clos , on peut appliquer à l'endomorphisme u la proposition 3 . Les polynomes $p_k$ ne sont autres que les $X-\alpha$ , et l'on voit que E est somme directe de sous-espaces stables, monogènes , et sur lesquels le polynome minimal de u est de la forme $(X-\alpha)^m$ . Soit $E_{m,\alpha}$ un tel sous-espace , et $E'_{m,\alpha}$ le $K[X]$-module associé ; $E'_{m,\alpha}$ est donc isomorphe à $K[X]/(X-\alpha)^m$ , et cet isomorphisme transforme l'endomorphisme u en la multiplication par X . Il en résulte que $u-\alpha$ est transformé en la multiplication par $X-\alpha$ , et en posant $Y=X-\alpha$ , on voit que $E'_{m,\alpha}$ peut être identifié à $K[Y]/(Y^m)$ , l'endomorphisme $u-\alpha$ étant transformé par cette identification en la multiplication par Y . Or , on a vu au n°1 que l'on pouvait représenter la multiplication par Y au moyen de la matrice :

$$\begin{pmatrix} 0 & 0 & 0 & \dots & 0 & 0 \\ 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & \dots & 1 & 0 \end{pmatrix} .$$

Il en résulte que l'on peut représenter u par la matrice :

$$\underline{U}_{m,\alpha} = \begin{pmatrix} \alpha & 0 & 0 & \dots & 0 & 0 \\ 1 & \alpha & 0 & \dots & 0 & 0 \\ 0 & 1 & \alpha & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & \alpha & 0 \\ 0 & 0 & 0 & \dots & 1 & \alpha \end{pmatrix}$$

DEFINITION 2 - <u>La matrice</u> $\underline{U}_{m,\alpha}$ <u>ci-dessus est dite matrice de Jordan d'ordre</u> m <u>relative à</u> $\alpha$ .

Nous avons ainsi montré :

PROPOSITION 5 - <u>Soit</u> <u>U</u> <u>une matrice à coefficients dans un corps</u> K <u>algébriquement clos</u> ; <u>il existe une matrice semblable à</u> <u>U</u> <u>et qui est un tableau diagonal de matrices de Jordan</u> .

(Le lecteur n'aura pas de peine à traduire ce résultat de la forme matricielle dans la forme "endomorphismes") .

<u>Remarques</u> - 1. La conclusion de la proposition 5 subsiste si l'on

remplace l'hypothèse "K est algébriquement clos" par la suivante:"K contient toutes les racines du polynome minimal de $\underline{U}$ " . En effet , les polynomes irréductibles qui interviennent dans la proposition 3 sont des diviseurs du polynome minimal , donc sont encore du premier degré , et la méthode précédente s'applique sans changement .

2. Il résulte de la proposition 3 que , si $\underline{U}$ est semblable à un tableau diagonal de matrices de Jordan , ces matrices sont bien déterminées par $\underline{U}$ .

3. Lorsque l'on connait les matrices de Jordan qui interviennent dans la décomposition de la matrice $\underline{U}$ , on peut calculer immédiatement les invariants de similitude de $\underline{U}$ . La méthode est calquée sur celle exposée au §4,n°8,Remarque3 : on écrit sur une même ligne les $(X-\alpha)^m$ relatifs au même $\alpha$ , et on complète par des 1 , de façon à avoir n termes ($\underline{U}$ étant d'ordre n) ; les $(X-\alpha)^m$ sont rangés par ordre d'exposants décroissants. Ceci fait , on obtient les invariants de similitude en formant les produits des termes qui sont dans une même colonne . Par exemple , pour la matrice :

$$\underline{A} = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} ,$$

on écrirait :

$$\begin{matrix} (X-2) & , 1 & , 1 \\ (X-1)^2 & , 1 & , 1 \end{matrix}$$

et les invariants de similitude seraient : $(X-1)^2(X-2)$ , 1 , 1 .

COROLLAIRE - *Toute matrice à coefficients dans un corps algébriquement clos est semblable à une matrice triangulaire* .

Rappelons (Chap.II, §6,n°5,Ex.V) qu'une matrice $\underline{U} = (u_{ij})$ est dite *triangulaire* si $u_{ij}=0$ pour $j > i$ , c'est à dire si elle n'a que des zéros au-dessus de sa diagonale . Le corollaire résulte alors du fait que toute matrice de Jordan est triangulaire et qu'un tableau diagonal de matrices triangulaires est encore une matrice triangulaire .

## 3 . Valeurs propres et vecteurs propres .

DEFINITION 3- *Soit E un espace vectoriel* de dimension finie n *sur un corps commutatif K , u un endomorphisme de E , $\underline{U}$ la matrice de u par rapport à une base*

($e_i$) de E ? On dit qu'un élément $x \in E$ est un vecteur propre de u ( et de U ) s'il existe $\alpha \in K$ tel que $u.x = \alpha x$ ; si $x \neq o$ , le scalaire $\alpha$ (qui est entièrement déterminé par x) est appelé valeur propre de u (et de U ) .

Exemple - Pour que le vecteur ~~propre~~ de base $e_i$ soit un vecteur propre de la matrice $U = (u_{jk})$ , il faut et il suffit que $u_{ki} = o$ pour tout $k \neq i$ (autrement dit , la colonne d'indice i doit se réduire à son terme diagonal) ; dans ces conditions , le vecteur propre $e_i$ correspond à la valeur propre $\alpha_i = u_{ii}$ . Ainsi dans une matrice triangulaire (par exemple dans une matrice de Jordan) , le vecteur de base d'indice ~~n~~ est vecteur propre (si la matrice est d'ordre ~~n~~) ; dans une matrice diagonale , tous les vecteurs de base sont vecteurs propres et il est clair que ceci caractérise les matrices diagonales .

Pour déterminer les valeurs propres de la matrice U , on est amené à introduire le polynome caractéristique de U :

DEFINITION 4 - Soit U une matrice carrée d'ordre n sur un corps commutatif K . On appelle polynome caractéristique de U et on note $\chi_U(X)$ le déterminant de la matrice $X.1_n - U$ (matrice à coefficients dans $K[X]$) :

$$\chi_U(X) = \det(X.1_n - U) .$$

Il résulte immédiatement du développement d'un déterminant que le polynome caractéristique de U est un polynome unitaire de degré n .

Si u est un endomorphisme de l'espace vectoriel E , on peut définir l'endomorphisme $X.1 - u$ , endomorphisme du module $E[X] = K[X] \otimes E$ , obtenu à partir de E par extension de l'anneau des scalaires à $K[X]$ (cf. Chapitre III , § 2 , n°1) . Si U est la matrice de u par rapport à la base ($e_i$) , ($X.1_n - U$) est la matrice de $X.1 - u$ par rapport à ($e_i$) considéré comme base du $K[X]$-module $E[X]$ . Il en résulte que :

$$\det(X.1 - u) = \det(X.1_n - U) ,$$

ce qui montre que $\det(X.1_n - U)$ ne dépend pas de la matrice U choisie pour représenter u , et permet d'appeler ce polynome polynome caractéristique de l'endomorphisme u . En termes matriciels , ceci signifie que les polynomes caractéristiques de deux matrices semblables sont égaux , ce qui est d'ailleurs facile à obtenir par un calcul direct .

 11

Nous noterons $\chi_u(X)$ le polynome caractéristique de u .

PROPOSITION 6 - Pour qu'un élément $\alpha \in K$ soit valeur propre de l'endomorphisme u , il faut et il suffit qu'il soit racine du polynome caractéristique de u .

En effet , dire que $\alpha$ est valeur propre de u signifie que $\alpha.1 - u$ n'est pas inversible , donc que $\chi_u(\alpha) = \det(\alpha.1 - u) = o$ .

PROPOSITION 7 - Soit u un endomorphisme d'un espace vectoriel de dimension finie n E sur un corps commutatif K , $\chi_u(X)$ le polynome caractéristique de u , $q_i(X)$ $(i=1,\dots,n)$ les invariants de similitude de u . On a :

$$\chi_u(X) = q_1(X).q_2(X)\dots q_n(X) .$$

( Bien entendu , les propositions 6 et 7 sont aussi valables pour les matrices) .

Comme ni les invariants de similitude ni le polynome caractéristique ne changent par extension du corps de base , on peut supposer ce dernier algébriquement clos . D'après la proposition 5 , il existe alors une base de E telle que la matrice de u par rapport à cette base soit un tableau diagonal de matrices de Jordan $U_{m_i,\alpha_i}$ $(i =1,\dots q)$

Il résulte du calcul des invariants de similitude (n°2, Remarque 3) que le produit de ces derniers est égal à $\prod_i (X-\alpha_i)^{m_i}$ .

D'autre part , on sait que le déterminant d'une matrice triangulaire est égal au produit des termes diagonaux (Chap.III, §6,n°4,Ex.2) d'où le fait que $\det(X.1 - u)$ est aussi égal à $\prod_i (X-\alpha_i)^{m_i}$ , ce qui démontre la proposition .

COROLLAIRE 1 - Avec les notations de la proposition précédente , soit $q(X)$ le polynome minimal de u ; $q(X)$ divise $\chi_u(X)$ et $\chi_u(X)$ divise $q^n(X)$ . En particulier , le polynome minimal et le polynome caractéristique de u ont les mêmes racines , à savoir les valeurs propres de u .

Puisque $q(X) = q_n(X)$ (Prop.2), il est clair que $q(X)$ divise $\chi_u(X)$ . D'autre part , puisque chaque $q_i$ divise $q_n$, $\chi_u$ divise $q^n$ .

COROLLAIRE 2 - (théorème d'Hamilton-Cayley) Pour tout endomorphisme u , on a : $\chi_u(u) = o$ .

Cela résulte immédiatement du fait que $\chi_u(X)$ est un multiple du polynome minimal de u (Cor.1) .

COROLLAIRE 3 - Pour qu'un endomorphisme u soit nilpotent , il est nécessaire et suffisant que son polynome caractéristique soit égal à $X^n$ .

Cela résulte immédiatement du corollaire 1 ci-dessus .

Remarque - Soit G un groupe abélien fini d'ordre N ; on vérifie immédiatement que le produit des diviseurs élémentaires de G est égal à N . Ainsi , on voit apparaitre une analogie entre le polynome caractéristique d'une matrice , et l'ordre d'un groupe abélien fini . Cette analogie se poursuit assez loin ; par exemple , le théorème d'Hamilton-Cayley correspond au résultat suivant , bien connu : pour tout $x \in G$ , on a $Nx = o$ . Il est d'ailleurs facile de donner du théorème d'Hamilton-Cayley une démonstration directe , calquée sur celle de ce résultat (cf.Exercice ) .

4 . Réduction à la forme diagonale .

DEFINITION 5 . Soit E un espace vectoriel de dimension finie n sur un corps commutatif K et u un endomorphisme de E . On dit que u est réductible à la forme diagonale s'il existe une base $(e_i)$ de E par rapport à la quelle la matrice de u soit une matrice diagonale .

Il revient au même de dire que l'on peut trouver une base de E formée de vecteurs propres de u , ou encore que les vecteurs propres de u engendrent E .

PROPOSITION 7 . Soit E un espace vectoriel de dimension finie n sur un corps commutatif K et u un endomorphisme de E , réductible à la forme diagonale . Pour toute valeur propre $\alpha$ de u , soit $V_\alpha$ le sous-espace propre correspondant , c'est à dire l'ensemble des $x \in E$ tels que $u.x = \alpha x$ . Alors E est somme directe des $V_\alpha$ .

. Soit $(e_i)$ une base de E telle que la matrice $\underline{U} = (u_{ij})$ de u par rapport à $(e_i)$ soit diagonale . Pour tout $\alpha \in K$ , désignons par $J_\alpha$ l'ensemble formé des indices i tels que $u_{ii} = \alpha$ . Soit $x \in V_\alpha$ et écrivons x sous la forme :

$$x = \sum_i x_i e_i \ .$$

On a : $u.x = \sum_i u_{ii} x_i e_i = \sum_i \alpha x_i e_i$ , ce qui équivaut à : $x_i = o$ pour $i \notin J_\alpha$ .

~~On voit donc que V admet une base formée des $(e_i)$~~

On voit donc que $V_\alpha$ admet pour base la famille des $(e_i)_{i \in J_\alpha}$ ; la proposition en résulte immédiatement .

On comparera utilement la proposition précédente à la proposition 4 .

PROPOSITION 8 - Soit E un espace vectoriel de dimension finie n sur un corps commutatif K , et u un endomorphisme de E . Pour que u soit réductible à la forme diagonale , il faut et il suffit que le polynome minimal de u , q(X) , ait toutes ses racines dans K et que celles-ci soient simples .

Remarquons d'abord que toute matrice carrée d'ordre 1 est une matrice de Jordan . Si donc u est réductible à la forme diagonale , la matrice U correspondante est une matrice diagonale de matrices de Jordan d'ordre 1 , et , d'après le n°2 ,Remarque 3 , q(X) est égal à un produit de facteurs linéaires distincts deux à deux .

Réciproquement , si q(X) est de cette forme , on peut représenter u par une matrice diagonale de matrices de Jordan (puisque toutes les racines de q sont dans K) , et ces matrices sont toutes d'ordre 1 d'après le raisonnement qui vient d'être fait . Ceci achève la démonstration .

dire que la condition n'est pas nécessaire

COROLLAIRE 1 - Si le polynome caractéristique de u a toutes ses racines dans K et si elles sont distinctes deux à deux , u est réductible à la forme diagonale .

Cela résulte du fait que le polynome minimal divise le polynome caractéristique .

Ça résulte des définitions et non de la Prop. 8

COROLLAIRE 2 - Tout endomorphisme nilpotent réductible à la forme diagonale est nul .

En effet , son polynome minimal est de la forme $X^r$ $(r \geqslant 1)$ puisque l'endomorphisme est nilpotent ; d'autre part , ses racines doivent être distinctes ; c'est donc qu'il est égal à X ,cqfd.

On a vu au cours de la démonstration de la proposition 8 qu'une matrice de Jordan ne pouvait être semblable à une matrice diagonale que si son ordre était égal à 1 . Il existe donc des endomorphismes qui ne sont pas réductibles à la forme diagonale . On a cependant :

14

PROPOSITION 9 - *Soit* $E$ *un espace vectoriel de dimension finie* $n$ *sur un corps algébriquement clos* $K$ , *et* $u$ *un endomorphisme de* $E$ . *On peut écrire* $u$ *d'une façon et d'une seule sous la forme* $u = s + n$ , *où* $s$ *et* $n$ *sont des endomorphismes permutables* , $s$ *étant réductible à la forme diagonale , et* $n$ *nilpotent* .
*Dans ces conditions* , $s$ *et* $n$ *sont des polynomes en* $u$ .

Supposons qu'il existe un couple $(s,n)$ répondant aux conditions données dans la première partie de l'énoncé ; nous allons voir qu'il est unique . Soit $\alpha$ une valeur propre de $s$ , et $V_\alpha$ le sous-espace propre correspondant . Comme $s$ et $u$ permutent (puisque $u = s + n$ ) , $V_\alpha$ est stable pour $u$ , en vertu du lemme suivant :
LEMME 2 - *Soient* $g$ *et* $h$ *deux endomorphismes permutables . Tout sous-espace propre* $V_\alpha$ *de* $g$ *est stable pour* $h$ .

En effet , si $x \in V_\alpha$ , on a : $gh.x = hg.x = h.\alpha x = \alpha h.x$ , ce qui signifie que $h.x \in V_\alpha$ .

Le sous-espace $V_\alpha$ est donc stable pour $u$ et $n$ ; comme $s$ coincide sur $V_\alpha$ avec l'homothétie de rapport $\alpha$ , $u-\alpha$ coincide sur $V_\alpha$ avec $n$ , donc est nilpotent sur $V_\alpha$ . Ceci signifie que $V_\alpha$ est contenu dans le sous-espace $M_\alpha$ des éléments $x \in E$ tels que $(u-\alpha)^N.x = o$ pour $N$ assez grand . Comme $E$ est somme directe des $V_\alpha$ (Prop.7) et somme directe des $M_\alpha$ (Prop.4) , il suit de là que $V_\alpha = M_\alpha$ . On voit alors que $s$ est bien déterminé par $u$ : sur chaque $M_\alpha$ c'est l'homothétie de rapport $\alpha$ .

Inversement , définissons $s$ par la condition précédente , et posons : $n = u-s$ . Il est clair que $s$ est réductible à la forme diagonale et que $n$ est nilpotent . Reste à voir que $s$ et $n$ sont des polynomes en $u$ (ce qui entraînera qu'ils sont permutables) ; il suffit d'ailleurs de le voir pour $s$ . Or , d'après la proposition 4 , il existe des polynomes $q_\alpha$ tels que , pour tout $x \in E$ , le composant de $x$ dans $M_\alpha$ soit $q_\alpha(u).x$ . On a alors $s = \sum_\alpha \alpha\, q_\alpha(u)$ , ce qui achève la démonstration .

*Remarque* . Soit $\underline{U}$ la matrice de $u$ ; on a $\underline{U} = \underline{S} + \underline{N}$ , où $\underline{S}$ est semblable à une matrice diagonale , $\underline{N}$ nilpotente , et $\underline{S}$ et $\underline{N}$ sont des polynomes en $\underline{U}$ (à coefficients dans $K$) . On peut préciser ceci :

PROPOSITION 10 - *Si les coefficients de* $\underline{U}$ *sont dans un sous-corps parfait* $k$ *de* $K$ , *il en est de même des coefficients de* $\underline{S}$ *et de* $\underline{N}$ .

15

Soit $\sigma$ un k-automorphisme de K , et notons $P_\sigma$ le polynome obtenu à partir d'un polynome $P \in K[X]$ en effectuant l'automorphisme $\sigma$ sur ses coefficients ; de même , notons $\underline{A}_\sigma$ la matrice transformée de la matrice $\underline{A}$ en effectuant l'automorphisme $\sigma$ sur ses coefficients . Il est clair que , si $\underline{A} = P(\underline{B})$ , on a : $\underline{A}_\sigma = P_\sigma(\underline{B}_\sigma)$ .

Considérons alors les matrices $\underline{S}_\sigma$ et $\underline{N}_\sigma$ . Comme $\underline{U}_\sigma = \underline{U}$ , on a : $\underline{U} = \underline{S}_\sigma + \underline{N}_\sigma$ ; en outre , $\underline{S}_\sigma$ est réductible à la forme diagonale , $\underline{N}_\sigma$ est nilpotente , et si $\underline{S} = P(\underline{U})$ , on a $\underline{S}_\sigma = P_\sigma(\underline{U})$ . Il résulte alors de l'unicité de la décomposition de $\underline{U}$ que $\underline{S}_\sigma = \underline{S}$ et $\underline{N}_\sigma = \underline{N}$ , ce qui signifie que , pour tout $\sigma$ , les coefficients de $\underline{S}$ et $\underline{N}$ sont invariants par $\sigma$ . D'après la définition des corps parfaits (Chap.V, § 7,n°3,déf.2) ceci entraîne que ces coefficients sont dans k , cqfd.

5 ? <u>Propriétés du polynome caractéristique</u> .

Soit E un espace vectoriel de dimension finie n sur un corps K , et u un endomorphisme de E . Nous avons défini au n°3 le <u>polynome caractéristique</u> de u : $\chi_u(X) = \det(X.1 - u)$ . Si $(e_i)$ est une base de E , par rapport à la quelle la matrice de u est $\underline{U}$ , on a aussi : $\chi_u(X) = \chi_{\underline{U}}(X) = \det(X.\underline{1}_n - \underline{U})$ .

Les coefficients du polynome caractéristique sont également des invariants de l'endomorphisme u , c'est à dire ne dépendent que du couple (E,u) , et non de la matrice $\underline{U}$ choisie pour représenter u . Ainsi , le terme constant est égal à $\chi_u(o) = (-1)^n \det(u)$ . Cherchons le coefficient de $X^{n-1}$ ; pour cela , posons $\underline{U} = (u_{ij})$ et considérons le développement de $\det(X.\underline{1}_n - \underline{U})$ . Dans ce développement , les termes contenant $X^{n-1}$ doivent provenir d'au moins (n-1) facteurs diagonaux , donc en fait de n ; ce sont les mêmes que ceux du produit $\prod_i (X-u_{ii})$ . Le coefficient cherché est donc : $-\sum_i u_{ii} = -\mathrm{Tr}(u)$ . On a obtenu ainsi :

PROPOSITION 11 - <u>Soit</u> E <u>un espace vectoriel de dimension finie</u> n <u>sur un corps commutatif</u> K , <u>et soit</u> u <u>un endomorphisme de</u> E . <u>Le polynome caractéristique de</u> u <u>est de la forme</u> :

(1) $$\chi_u(X) = X^n - \mathrm{Tr}(u).X^{n-1} + \dots + (-1)^n \det(u) .$$

Nous allons maintenant donner des relations entre les polynomes caractéristiques de u et d'un polynome en u :

PROPOSITION 12 - <u>Soit</u> E <u>un espace vectoriel de dimension finie</u> n <u>sur un corps K algébriquement clos</u> , u <u>un endomorphisme de</u> E , <u>et</u>

16

$\chi_u(X) = \prod_i (X-\alpha_i)$ la décomposition en facteurs linéaires de son polynome caractéristique . Si q est un polynome à coefficients dans K, le polynome caractéristique de q(u) est donné par :

$$(2) \qquad \chi_{q(u)}(X) = \prod_i (X - q(\alpha_i)) ,$$

sa trace et son déterminant par :

$$(3) \qquad Tr(q(u)) = \sum_i q(\alpha_i) \quad , \qquad (4) \quad det(q(u)) = \prod_i q(\alpha_i) \quad .$$

Il est clair que les formules (3) et (4) résultent des formules (1) et (2) . Il nous suffit donc de prouver la formule (2) .

Pour cela , choisissons une base de E telle que la matrice $\underline{U} = (u_{ij})$ de u par rapport à cette base soit une matrice triangulaire ; c'est possible d'après le corollaire à la proposition 5 . Il résulte de la formule donnant le produit de deux matrices triangulaires que la matrice $q(\underline{U})$ est triangulaire , et que son terme diagonal d'indice i est égal à $q(u_{ii})$ . D'autre part , si $\underline{V} = (v_{ij})$ est une matrice triangulaire , la matrice $X.\underline{1}_n - \underline{V}$ l'est également , et l'on a $\chi_{\underline{V}}(X) = det(X.\underline{1}_n - \underline{V}) = \prod_i (X-v_{ii})$ . Appliquant alors ce résultat à $\underline{U}$ et à $q(\underline{U})$ , on voit que :

$$\chi_{\underline{U}}(X) = \prod_i (X-u_{ii}) \qquad \text{et} \qquad \chi_{q(\underline{U})}(X) = \prod_i (X-q(u_{ii})) ,$$

ce qui démontre la formule (2) .

COROLLAIRE 1 . La condition nécessaire et suffisante pour que q(u) soit inversible est que q soit étranger à $\chi_u$ .

En effet , dire que q et $\chi_u$ sont étrangers équivaut à dire que q et $\chi_u$ n'ont pas de racine commune , c'est à dire , d'après la formule (4) , que $det(q(u)) \neq 0$ .

Remarque . Etre étranger à $\chi_u$ équivaut à être étranger au polynome minimal de u , d'après le Cor.1 à la proposition 7 . Le corollaire précédent résulte donc immédiatement de la Prop.3 du §1 ,n°2 .

COROLLAIRE 2 . Si $r \in K(X)$ est une fraction rationnelle à coefficients dans K , la condition nécessaire et suffisante pour que u soit substituable dans r (Chap.IV , §3 ,n°2) est que chacune des valeurs propres $\alpha_i$ de u le soit . Lorsqu'il en est ainsi on a les formules :

$$\chi_{r(u)}(X) = \prod_i (X-r(\alpha_i)) \ ; \ Tr(r(u)) = \sum_i r(\alpha_i) \ ; \ det(r(u)) = \prod_i r(\alpha_i) \ .$$

Ecrivons r sous la forme : r=p/q , où p et q sont des polynomes étrangers . Pour que u soit substituable dans r , il faut et il suffit que q(u) soit inversible , ~~àtmèxèaxpremièrexassertionxx~~ c'est-à dire (Cor.1) que q soit étranger à $\chi_u$ , d'où la première assertion.

Supposons donc que q soit étranger à $\chi_u$ ; d'après l'identité de Bezout , il existe des polynomes g et h tels que $qg + h\chi_u = 1$ ; on a alors $q(\alpha_i)g(\alpha_i) = 1$ pour tout i , et $q(u)g(u) = 1$ ( d'après le théorème d'Hamilton-Cayley) . On a donc :

$$r(u) = p(u)g(u) ,$$

et en appliquant la formule (2) , il vient :

$$\chi_{r(u)}(X) = \chi_{p(u)g(u)}(X) = \prod_i (X-p(\alpha_i)g(\alpha_i)) = \prod_i (X-r(\alpha_i)) .$$

Les deux autres formules résultent immédiatement de celle-là .

COROLLAIRE 3 - <u>On a , pour tout entier</u> $s \geqslant o$ , $Tr(u^s) = \sum_i \alpha_i^s$ ; <u>cette formule est encore valable pour</u> $s < o$ , <u>à condition que</u> u <u>soit inversible</u> .

C'est un cas particulier du corollaire précédent .

COROLLAIRE 4 - <u>Si le corps</u> K <u>est de caractéristique nulle , pour que l'endomorphisme</u> u <u>soit nilpotent</u> , <u>il faut et il suffit que</u> $Tr(u^s) = o$ <u>pour</u> $s=1,\dots n$ .

Si u est nilpotent , ses valeurs propres $\alpha_i$ sont nulles et $Tr(u^s) = o$ pour tout s d'après le Cor.3 .

Réciproquement , si $Tr(u^s) = \sum_i \alpha_i^s = o$ pour $s=1,\dots,n$ , les valeurs propres $\alpha_i$ sont toutes nulles puisque K est de caractéristique nulle (Chap.V,App.I,Cor. à la Prop.4) , et u est nilpotent .

COROLLAIRE 5 - <u>La matrice</u> $Y.\underline{1}_n - \underline{U}$ <u>est inversible dans l'anneau des matrices carrées sur le corps</u> K(Y) <u>des fractions rationnelles sur</u> K . <u>En outre , si</u> $\chi'_{\underline{U}}$ <u>désigne la dérivée du polynome</u> $\chi_{\underline{U}}$ , <u>on a</u> :

$$Tr((Y.\underline{1}_n-\underline{U})^{-1}) = \chi'_{\underline{U}}(Y)/\chi_{\underline{U}}(Y) .$$

En effet , on peut considérer $(Y.\underline{1}_n - \underline{U})$ comme une fraction rationnelle en $\underline{U}$ , à coefficients dans K(Y) : il suffit de prendre $r(X) = (Y-X)^{-1}$ . Le corollaire résulte alors immédiatement du corollaire 3 et de la formule :

~~HH(HHHH)HHHH~~

$\sum_i 1/(Y-\alpha_i) = \chi'_U(Y)/\chi_U(Y)$ (Chap.V,App.I,n°3,formule (3) ) .

Nous allons maintenant déterminer le polynome caractéristique du produit tensoriel de deux endomorphismes :

PROPOSITION 13 - Soit E (resp.E') un espace vectoriel de dimension finie sur un corps K algébriquement clos , u (resp.u') un endomorphisme de E (resp.E') et $\chi_u(X) = \prod_i (X-\alpha_i)^{n_i}$ (resp. $\chi_{u'}(X) = \prod_j (X-\beta_j)^{m_j}$) les décompositions en facteurs linéaires de leurs polynomes caractéristiques ( les $\alpha_i$ et les $\beta_j$ étant distincts) . Alors le polynome caractéristique de l'endomorphisme $u\otimes u'$ de l'espace vectoriel $E\otimes E'$ est donné par la formule :

$$\chi_{u\otimes u'}(X) = \prod_{i,j} (X - \alpha_i\beta_j)^{n_i m_j}$$

Soit $V_i$ (resp.$V'_j$) le sous-espace de E (resp.E') formé des éléments x tels que $(u-\alpha_i)^N.x = o$ pour N assez grand (resp.$(u'-\beta_j)^N.x = o$ ) . Si $N_i$ (resp.$M_j$) est la dimension de $V_i$ (resp.$V'_j$) , il résulte de la proposition 7 que le polynome caractéristique de u (resp.u') est le produit des $(X-\alpha_i)^{N_i}$ (resp. des $(X-\beta_j)^{M_j}$ ) , d'où le fait que $N_i = n_i$ et $M_j = m_j$ .

D'autre part , d'après la proposition 4 appliquée à E et E', $E\otimes E'$ est somme directe des $V_i\otimes V'_j$ . Montrons maintenant le lemme suivant :

LEMME 3 - L'endomorphisme $u\otimes u' - \alpha_i\beta_j$ est nilpotent sur $V_i\otimes V'_j$ .

Ecrivons en effet :

$$u\otimes u' - \alpha_i\beta_j = (u-\alpha_i)\otimes u' + \alpha_i\otimes(u'-\beta_j) .$$

Les deux endomorphismes qui figurent au second membre sont nilpotents (sur $V_i\otimes V'_j$) et commutent . Or , si A et B sont nilpotents et commutent , A+B est nilpotent comme il résulte tout de suite de la formule du binôme (Chap.I,Rect.,p.58) .

Le lemme étant démontré, on voit que $E\otimes E'$ est somme directe des $V_i\otimes V'_j$ , qui sont stables pour $u\otimes u'$ et sur lesquels $(u\otimes u'-\alpha_i\beta_j)$ est nilpotent . Comme la dimension de $V_i\otimes V'_j$ est $n_i m_j$ , il résulte du raisonnement qui a été fait dans la première partie de cette démonstration que $\chi_{u\otimes u'}(X) = \prod_{i,j} (X-\alpha_i\beta_j)^{n_i m_j}$ , cqfd.

# APPENDICE

## Endomorphismes semblables sur un anneau .

Nous allons généraliser certains résultats du §5 aux endomorphismes des modules sur un anneau .

Dans tout ce qui suit , A désignera un anneau commutatif à élément unité, non nécessairement intègre , E un A-module unitaire et u un endomorphisme de E .

### 1 . Le module associé à un endomorphisme .

Désignons par $A[X]$ l'anneau des polynomes en une indéterminée X sur l'anneau A . Si $P \in A[X]$, et $x \in E$ , posons :

$$P.x = P(u).x \quad ;$$

l'application $(P,x) \rightarrow P.x$ définit sur E une structure de $A[X]$-module unitaire , que nous désignerons par $E_u$ .

On notera que les sous-modules de $E_u$ ne sont autres que les sous-A-modules de E qui sont stables pour u .

PROPOSITION 1 - *Soient u et u' deux endomorphismes des A-modules E et E' , et g une application de E dans E' . Pour que g soit une application A-linéaire telle que $g_{\circ}u = u'_{\circ}g$ , il faut et il suffit que g soit une application $A[X]$-linéaire .*

Si g est $A[X]$-linéaire , on a $g(P(u).x) = P(u').g(x)$ pour tous $P \in A[X]$ et $x \in E$ . En prenant pour P une constante , on voit que g est A-linéaire , et en prenant $P=X$ , on voit que $g_{\circ}u = u'_{\circ}g$ .

Réciproquement , si cette dernière relation a lieu et si g est A-linéaire , il suffit de vérifier que $g_{\circ}u^n = u'^n{}_{\circ}g$ . Ceci se fait par récurrence sur n : lorsque n=o , la relation est vraie , et si elle est vraie pour n-1 , on peut écrire :

$$g_{\circ}u^n = u'^{n-1}{}_{\circ}g_{\circ}u = u'^n{}_{\circ}g \qquad \text{, cqfd.}$$

On dit que deux endomorphismes u,u' de deux A-modules E,E' sont *semblables* (resp. *équivalents*) s'il existe un isomorphisme g de E sur E' (resp. des isomorphismes h de E sur E' et k de E' sur E) tels que $u' = g_{\circ}u_{\circ}g^{-1}$ (resp. $u' = h_{\circ}u_{\circ}k$) ; ces définitions sont les généralisations naturelles de celles qui ont été données pour les matrices

(Chap.II, § 6 , n$^{os}$ 10 et 11) . Ceci étant , il résulte de la proposition 1 le corollaire suivant :

COROLLAIRE - Soient $u$ et $u'$ deux endomorphismes des A-modules E et E' ; pour que $u$ et $u'$ soient semblables , il faut et il suffit que les A[X]-modules $E_u$ et $E'_{u'}$ soient isomorphes .

2 . Le module E[X] .

Nous avons défini au début du n° précédent une application canonique : $A[X]\times E \longrightarrow E$ , qui nous a servi à définir la structure de A[X]-module de E . Cette application est A-bilinéaire comme on le voit tout de suite . Elle se prolonge donc canoniquement en une application A-linéaire $\varphi$ du produit tensoriel $E[X] = A[X]\otimes E$ dans E : si $P\in A[X]$ et $x\in E$ , on a :

$$(1) \qquad \varphi(P\otimes x) = P(u).x$$

Le A-module E[X] peut aussi être considéré comme le module obtenu à partir de E par extension de l'anneau des scalaires à A[X] (Chap.III § 2) et peut donc être muni d'une structure de A[X]-module , définie par : $Q.(P\otimes x) = (QP)\otimes x$ . Dans ce qui suit , nous considérerons toujours E[X] comme muni de cette dernière structure . L'endomorphisme $u$ de E se prolonge alors en un A[X]-endomorphisme de E[X], que nous noterons encore $u$ , et qui est défini par :

$$u(P\otimes x) = P\otimes u.x \quad .$$

Il résulte de cette formule que l'on a : $\varphi\circ u = u\circ\varphi$ (2)

D'autre part , on a :

$$\varphi(Q.(P\otimes x)) = \varphi((QP)\otimes x) = QP(u).x = Q.(\varphi(P\otimes x)) \ , \quad (3)$$

autrement dit , l'application $\varphi$ est A[X]-linéaire . Comme son image est égale à E tout entier (puisque $\varphi(1\otimes x) = x$) , on voit qu'on a obtenu le résultat suivant :

PROPOSITION 2 - Soit E[X] le A[X]-module obtenu par extension à A[X] de l'anneau d'opérateurs A du module E . L'application $\varphi$ définie par la formule (1) identifie le A[X]-module $E_u$ au quotient de E[X] par son noyau $\overset{-1}{\varphi}(0) = N$ .

Remarque - L'intérêt de la proposition précédente tient à ce que , dans les cas les plus importants , E est un module libre sur A , et $E[X]$ est de ce fait un module libre sur $A[X]$ . On a donc représenté $E_u$ canoniquement comme quotient d'un module libre , ce qui facilite l'étude de sa structure ; voir n°4 par exemple .

Introduisons maintenant l'endomorphisme $Y = X - u$ de $E[X]$ ; d'après les formules (2) et (3) , on a :

$\varphi_\circ Y = \varphi_\circ X - \varphi_\circ u = X_\circ\varphi - u_\circ\varphi = (X-u)_\circ\varphi = o$ (puisque les endomorphismes $X$ et $u$ coincident sur $E$) .

Si nous désignons par $M$ l'image de $E[X]$ par l'endomorphisme $Y$ , on a donc $M \subset N$ . En fait , on a le résultat plus précis suivant :

PROPOSITION 3 - <u>Soient</u> $E$ <u>un</u> $A$-<u>module</u> , $u$ <u>un endomorphisme de</u> $E$ , $E[X] = A[X]\otimes E$ . <u>Le noyau</u> $N$ <u>de l'application</u> $A[X]$-<u>linéaire</u> $\varphi$ <u>de</u> $E[X]$ <u>sur le</u> $A[X]$-<u>module</u> $E_u$ <u>est identique à l'image</u> $M$ <u>de</u> $E[X]$ <u>par l'endomorphisme</u> $Y = X-u$ .

Il nous suffit de montrer que $N \subset M$ . Pour cela remarquons d'abord que , les monômes $(X^i)$ formant une base du $A$-module $A[X]$, tout élément $e \in E[X]$ s'écrit d'une façon et d'une seule sous la forme :

$$e = \sum_i X^i \otimes x_i \quad ,$$

où $x_i \in E$ pour tout $i$ ( les $x_i$ étant tous nuls , sauf un nombre fini d'entre eux) .

Si $e \in N$ , on a $\varphi(e) = \sum_i u^i . x_i = o$ , et l'on peut donc écrire :

$$e = \sum_i (X^i \otimes x_i - 1\otimes u^i . x_i) \quad .$$

Or l'élément $X^i \otimes x_i - 1\otimes u^i . x_i$ peut aussi s'écrire $(X^i - u^i)(1\otimes x_i)$ ; comme les endomorphismes $X$ et $u$ permutent , $X^i - u^i$ est un multiple de l'endomorphisme $X-u = Y$ , et l'on a bien $e \in M$ , cqfd.

COROLLAIRE - <u>Les notations étant celles de la proposition précédente</u> , <u>soit</u> $u'$ <u>un endomorphisme d'un</u> $A$-<u>module</u> $E'$. <u>Pour que les endomorphismes</u> $u$ <u>et</u> $u'$ <u>soient semblables , il faut et il suffit qu'il existe deux isomorphismes</u> $g$ <u>et</u> $g_1$ <u>du</u> $A[X]$-<u>module</u> $E[X]$ <u>sur le</u> $A[X]$-<u>module</u> $E'[X]$ <u>tels que</u> :

$$g_\circ(X-u) = (X-u')_\circ g_1 \quad .$$

Si ces isomorphismes existent , ils définissent des isomorphismes des images $N$ et $N'$ de $E[X]$ et $E'[X]$ par $X-u$ et $X-u'$ respectivement (cela résulte tout de suite de la formule $g_\circ(X-u) = (X-u')_\circ g_1$), et, par passage au quotient, des isomorphismes de $E_u$ sur $E_{u'}$, ce qui montre bien que u et u' sont semblables (Cor. à la Prop. 1).

Réciproquement, si u et u' sont semblables, il existe un isomorphisme k de E sur E' tel que $u' = k\circ u\circ k^{-1}$, et le prolongement de k à E[X] est un isomorphisme g de E[X] sur E'[X] qui satisfait évidemment à $g_\circ(X-u) = (X-u')_\circ g$.

Remarque - Il résulte de la démonstration précédente que, si les A[X]-endomorphismes X-u et X-u' sont équivalents, ils sont semblables ; bien entendu, cette propriété n'est pas vraie pour des endomorphismes quelconques.

3 . Théorème d'Hamilton-Cayley .

Nous allons appliquer la proposition 3 pour démontrer le théorème d'Hamilton-Cayley sous des conditions plus générales que celles du § 5 .

PROPOSITION 4 - *Les notations ~~étantx~~ étant celles de la proposition 3, on suppose que E admette une base finie $(e_1,\dots,e_n)$ ; alors $(e_1,\dots,e_n)$ est une base du A[X]-module E[X] et le déterminant $\det(X-u)$ de l'endomorphisme X-u de E[X] est un polynome unitaire $\chi_u(X)$ de degré n sur A, ~~xx~~ tel que $\chi_u(u) = 0$.*

Toutes les assertions de cette proposition sont évidentes, sauf la dernière. Pour celle-ci, il suffit de montrer que l'on a pour tout i :

$$\det(X-u)e_i \in N .$$

Or, on a la formule :

(4) $$\det(X-u)e_i = (-1)^{n-i}\left[\det(X-u)(e_1\wedge e_2\wedge\dots\wedge e_n)\right] \llcorner (e'_1\wedge\dots\wedge e'_{i-1}\wedge e'_{i+1}\wedge\dots\wedge e'_n) ,$$

où $e'_i$ désigne la base duale de $e_i$, et où les produits extérieurs $\wedge$ et intérieur droit $\llcorner$ sont relatifs au A[X]-module E[X]. La formule elle-même est un cas particulier de la formule (21) du Chap. III, § 8, n°4 .

Pour calculer le produit intérieur de la formule (4) nous aurons besoin du lemme suivant :

LEMME . *Soit F un A-module unitaire ayant une base finie. Pour toute famille d'éléments $x_1,\dots,x_p \in F$ et $x' \in F^*$ (dual de F), on a :*

$$(5)\quad (x_1\wedge x_2\wedge\ldots\wedge x_p) \llcorner x' = \sum_{i=1}^{p} (-1)^{i+1}\langle x_i, x'\rangle \cdot x_1\wedge x_2\wedge\ldots\wedge x_{i-1}\wedge x_{i+1}\wedge\ldots\wedge x_p \ .$$

Le second membre de (5) est visiblement une fonction multilinéaire de $(x_1,\ldots,x_p,x')$ qui est alternée par rapport aux variables $x_1,\ldots,x_p$ . Pour montrer qu'elle coincide avec le premier membre , il suffit donc de le vérifier pour les éléments de base de F ; elle résulte alors de la formule(21) citée plus haut .

Ce lemme étant démontré , on peut calculer le produit intérieur de la formule (4) en effectuant d'abord le produit par $e'_1$ , puis par $e'_2$ , ... etc (loc.cit. formule (20)) . Mais on peut écrire :

$$\det(X-u)(e_1\wedge e_2\wedge\ldots\wedge e_n) = (Xe_1-ue_1)\wedge(Xe_2-ue_2)\wedge\ldots\wedge(Xe_n-ue_n)$$

(c'est la définition du déterminant d'un endomorphisme) .
En appliquant alors le lemme précédent , on voit que le premier membre de (4) sera égal à une combinaison linéaire à coefficients dans $A[X]$ des $Xe_j-ue_j$ ; or ces derniers sont dans N d'après la proposition 3 ; on a donc bien démontré que

$$\det(X-u)e_i \in N ,$$

ce qui achève la démonstration .

4 . <u>Cas où</u> A <u>est un corps</u> K .

Comme le module $E_u$ est isomorphe au quotient du $K[X]$-module libre $E[X]$ par le sous-module N , les invariants de similitude $q_i(X)$ de u ( § 5,n°1,déf.1) ne sont autres que les <u>facteurs invariants</u> du sous-module N par rapport au module $E[X]$ ( § 4 , n°2 , déf.1) . Or , en vertu de la proposition 3 , un système de générateurs de N est formé par les éléments $(Xe_j-1ue_j)$ , $(e_j)$ désignant une base de l'espace vectoriel E . On obtient alors , compte tenu de la Prop.3 ( §4 ,n°2) :

PROPOSITION 5 - <u>Soit</u> E <u>un espace vectoriel de dimension finie</u> n <u>sur un corps commutatif</u> K , u <u>un endomorphisme de</u> E , <u>U sa matrice par rapport à une base de</u> E . <u>Pour tout</u> m $(1 \leqslant m \leqslant n)$ , <u>le produit</u> $d_m(X) = q_1(X)\ldots q_m(X)$ <u>des</u> m <u>premiers invariants de similitude de l'endomorphisme</u> u <u>est égal au pgcd des mineurs d'ordre</u> m <u>de la matrice</u> $(X.\underline{1}_n - \underline{U})$ .

On retrouve en particulier la prop.7 du §5 .