Algèbre Chap VIII

MODULES ET ANNEAUX SEMI SIMPLES

§§7 et 8 (Etat 7)

n°245

Aux commentaires de la Tribu, le rédacteur ajoute les suivants. Page 37, cor.4 au "théorème de densité". A renvoyer, sous une forme plus générale, à l'appendice sur les représentations linéaires d'une algèbre, où il faudra prouver (comme conséquence immédiate du théorème de densité) : Si à toute classe λ de représentations linéaires irréductibles de dimension finie de A, on fait correspondre l'espace A'_λ de ses coefficients, la somme des A'_λ est directe. Ce résultat, indépendant de la caractéristique, implique aussitôt le cor.4 : en car.0, une représentation linéaire semi-simple de dim. finie est caractérisée par son caractère. Dire aussi que le caractère d'une représentation irréductible n'est jamais identiquement nul.

Page 40, prop.4, dire explicitement dans l'énoncé que le dual de $\mathcal{L}_A(S,M)$ est $\mathcal{L}_A(M,S)$.

Page 41, prop.5, ajouter en corollaire : Les sous-modules du module semi-simple isotypique $T \otimes_D S$ correspondent biunivoquement aux sous espaces vectoriels de l'espace vectoriel à droite T sur D. Le cor. 3 du th.1 du par.1 a été manifestement mis rien que pour ça, et on veut pouvoir référer au résultat mis sous la forme où il sert. Notons qu'il donne sans autre démonstration la forme générale des idéaux à gauche où à droite d'un anneau simple $A = \mathcal{L}_D(V) = V' \otimes_D V$, résultat qui me semble mériter d'être mis au n°4 du par. 4 (structure des anneaux simples) par exemple en proposition après la prop.11.

Page 47, remplacer les lignes 5-8 par : prouve que le bicommutant de M, c'est-à-dire $\mathcal{L}_D(M)$, s'identifie à celui de A_s, c'est-à-dire A.

Page 57, autre corollaire à la prop.2 : le radical d'une somme directe de modules est identique à la somme directe des radicaux, celui d'un produit de modules est contenu dans le produit des radicaux.

Page 18. Le théorème de Krull-Remak-Schmidt Le rédacteur est convaincu qu'il faut le garder, pour les raisons suivantes :

1) Son intérêt intrinsèque est indéniable, il est de plus manifestement indispensable si on veut classifier des modules non semi-simples, p.ex. les représentations linéaires de dim. finie d'un groupe qui se permettrait de ne pas être semi-simple (p.ex. le groupe des $x \longrightarrow ax+b$); et il n'est pas dit que Bourbaki (ou un lecteur) ne doive faire de telles classifications.

2) Appliquant K-R-S au module A_s, où A est un anneau d'Artin, on trouve la décomposition, unique à automorphisme intérieur près, de l'identité en somme de projecteurs orthogonaux indécomposables. D'où, p.ex. le th. de K-R-S pour un object M d'une catégorie abélienne tel que l'anneau A des endomorphismes de M soit d'Artin (Ce qui peut arriver même si M n'est pas de longueur finie, ex : faisceaux analytiques cohérents sur une variété hol. compacte).

3) En particulier, K-R-S donne donc le théorème analogue pour les fibrés vectoriels anal. resp. algébriques sur une variété analytique resp. algébrique. Or d'après Atiyah, ce résultat est absolument indispensable pour une étude poussée des fibrés vectoriels, car seules les classes de fibrés indécomposables ont quelque chance de former (pour une dimension et une classe topologique donnée) une variété irréduc-

tible.

Quant aux raisons données contre K.R.S., je dirai simplement que ce n'est pas sa faute s'il est valable aussi pour les groupes non commutatifs (la même chose pourrait d'ailleurs se dire de la plupart des sorites des par.1.2.3 !) et que ce n'est pas une raison pour se défendre de l'utiliser dans le cas abélien. Mêmes remarques concernant l'argument : K.R.S. marche aussi dans les classes abéliennes ; de plus, les cas utiles semblent se ramener comme il a été dit au cas traité, via le corollaire sur les idempotents dans un anneau d'Artin (que je demande à être mis en corollaire). En tous cas, il semble probable que si Bourbaki ne met pas K.R.S. ici, il n'en parlera pas non plus ailleurs, (jusqu'au jour où il sera canulé).

Sur les modules A-étendus. Le rédacteur n'a pas vu de place raisonnable au par.1 où en parler. Au contraire, ça semble venir assez naturellement en un n°5 au par.4, à titre d'illustration de la méthode de commutation. Il réfère donc (au par.8) à une proposition 7 du par.4, qui reste à insérer, (lemme 1 du par.7, ancienne rédaction). Le rédacteur s'aperçoit d'ailleurs que ce résultat ne "résulte" pas de Chap.II, par.5 prop.10, mais lui est identique, et il serait ridicule de ne pas le dire explicitement (ce qui n'empêche pas de donner la jolie démonstration de Koszul).

n° 245

§7. Produit tensoriel de corps commutatifs

Familles d'endomorphismes deux à deux permutables

d'un espace vectoriel .... p. 4

1. Extension des scalaires et radical. 2 Produit tensoriel de deux corps commutatifs. 3 Extensions composées. 4 Endomorphismes semi-simples et endomorphismes diagonalisables d'un espace vectoriel. 5 Opérateurs absolument semi-simples. 6 Familles d'endomorphismes semi-simples ou diagonalisables permutables. 7 Décomposition canonique d'une algèbre commutative. 8 Décomposition canonique d'un automorphisme.

§8. Radical et semi-simplicité d'un produit tensoriel

Modules séparables .... p. 31

1. Produit tensoriel avec un module simple. 2. Modules et algèbres séparables : critères de séparabilité. 3. Produit tensoriel avec un module séparable. 4. Semi-simplicité d'un produit tensoriel de modules. 5. Modules simples sur un produit tensoriel d'algèbres.

Projet d'addition au Chapitre VIII d'algèbre p.45

Projet d'addition à l'appendice I du chapitre III p.47

§ 7 Produit tensoriel de corps commutatifs
Familles d'endomorphismes deux à deux permutables
d'un espace vectoriel.

A partir du n°2 du présent §, tous les corps et toutes les algèbres envisagés sont supposés commutatifs. A partir du n°4, tous les espaces vectoriels envisagés sont de dimension finie.

1. Extension des scalaires et radical.

PROPOSITION 1. - Soient B et C deux anneaux, φ un homomorphisme de B dans C, N un B-module, considérons $C \otimes_B N$ comme un C-module à gauche et soit f l'application canonique $n \longrightarrow 1 \otimes n$ de N dans $C \otimes_B N$. Alors on a

(1) $$f^{-1}(\mathcal{R}_C(C \otimes_B N)) \subset \mathcal{R}_B(N)$$

Montrons d'abord que si N est simple, le premier membre de (1) est nul : en effet soit n un élément non nul de N, N étant simple c'est un générateur de N donc f(n) est un générateur de $C \otimes_B N$, donc n'est pas contenu dans le radical de $C \otimes_B N$ (puisque ce dernier est distinct de $C \otimes_B N$ en vertu de par. 6, n°2, prop. 1). Donc n n'est pas élément du premier membre de (1), qui est par suite nul. Prouvons maintenant le cas général, c'est-à-dire que si $n \in N$ est dans le premier membre de (1), il est annulé par tout homomorphisme u de N dans un B-module simple P. En effet, u définit un homomorphisme $1 \otimes u$ de $C \otimes_B N$ dans $C \otimes_B P$, et comme f(n) est dans le radical de $C \otimes_B N$ son image est dans le radical de $C \otimes_B P$, or cette image est aussi l'image canonique de u(n) dans $C \otimes_B P$, donc u(n) est nul en vertu de ce qui précède.

Dans la suite de ce numéro, nous considérons deux algèbres A et B sur un corps commutatif k, que nous identifions à des sous-algèbres

$A \otimes 1$ resp. $1 \otimes B$ de leur produit tensoriel $C = A \otimes_k B$. Si M est un A-module, N un B-module, alors $M \otimes_k N$ est muni d'une structure de C-module naturelle, définie par la condition $(a \otimes b).(m \otimes n) = (am) \otimes (bn)$ quels que soient $a \in A$, $b \in B$, $m \in M$ et $n \in N$. En particulier, prenant pour M le A-module A_s, $A \otimes_k N$ se trouve muni canoniquement d'une structure de C-module. D'ailleurs, comme $A \otimes_k N = (A \otimes_k B) \otimes_B N = C \otimes_B N$, on voit que ce C-module s'identifie au module déduit de N par extension à C de l'anneau des scalaires B. Nous identifierons N à un sous-groupe de $A \otimes_k N$ par l'application $n \longrightarrow 1 \otimes n$.

On notera que dans le cas où $N = B_s$, la structure de C-module qu'on vient d'envisager sur $A \otimes_k N = C$ n'est autre que la structure de C-module à gauche de C_s.

PROPOSITION 2. - *Soient* A *et* B *deux algèbres sur un corps* k, $C = A \otimes_k B$, *et* N *un* B-*module. On a*

$$(2) \qquad \mathcal{R}_C(A \otimes_k N) \cap N \subset \mathcal{R}_B(N)$$

et cette inclusion devient une égalité dans chacun des deux cas suivants

a) A *est de dimension finie sur* k, *où* N *est un* B-*module de type fini et* A *est réunion d'une famille filtrante croissante de sous algèbres de dimension finie sur* k (par exemple, A est une extension algébrique de k).

b) $N = B_s$, *et le radical de* B *est un idéal nilpotent*.

L'inclusion (2) est un cas particulier de (1). Prouvons l'égalité dans (2) quand A est de dimension finie sur k, il suffit de prouver que le radical de $A \otimes_k N$ contient celui de N, donc que tout homomorphisme v de $A \otimes_k N$ dans un C-module simple P s'annule sur le radical de N. Pour ceci, il suffit de montrer que le radical $\mathcal{R}_B(P)$ de

P en tant que B-module est nul. Or les homothéties dans P définies par les éléments de A sont des endomorphismes pour la structure de B-module, donc $\mathfrak{R}_B(P)$ est à la fois un sous-B-module et un sous-A-module, donc un sous-C-module, et P étant simple, $\mathfrak{R}_B(P)$ est donc réduit à $\{0\}$ ou identique à P. Mais P étant simple et A de dimension finie, on voit aussitôt que P est un B-module de type fini, donc $\mathfrak{R}_B(P) \neq \mathfrak{P}$ (par. 6, n°2, prop. 1), ce qui prouve bien $\mathfrak{R}_B(P) = \{0\}$.

Supposons N engendré par un nombre fini d'éléments $x_1, x_2, \ldots, x_n$, et A réunion d'une famille filtrante croissante $(A_i)_{i \in I}$ de sous algèbres de dimension finie sur k. Soit $x \in \mathfrak{R}_B(N)$, prouvons que $x \in \mathfrak{R}_C(A \otimes_k N)$. Comme les x_j engendrent le C-module $A \otimes_k N$, il suffit de montrer (par. 6, prop. 3) que, quels que soient les éléments c_j $(1 \leq j \leq n)$ de C, les éléments $x_j + c_j x$ engendrent encore le C-module $A \otimes_k N$. Or il existe un i tel que les c_j appartiennent tous à $C_i = A_i \otimes_k B$. D'après ce qui a déjà été démontré on a $x \in \mathfrak{R}_{C_i}(A_i \otimes_k N)$ donc les $x_j + c_j x$ engendrent le C_i-module $A_i \otimes_k N$, donc le C-module engendré dans $A \otimes_k N$ par ces éléments contient N et est par suite égal à $A \otimes_k N$, ce qui achève la démonstration.

Enfin, supposons que $\mathfrak{R}(B)$ soit nilpotent, soit ℓ un entier naturel tel que $\mathfrak{R}(B)^{\ell} = 0$. Comme l'idéal bilatère J engendré par $\mathfrak{R}(B)$ dans C est formé des sommes finies $\sum a_i r_i$ $(a_i \in A,\ r_i \in \mathfrak{R}(B))$ et que A commute à B, on voit aussitôt que l'on a aussi $J^k = 0$, donc J est contenu dans le radical de C, donc $\mathfrak{R}(B) \subset \mathfrak{R}(C)$. La proposition 2 est démontrée.

PROPOSITION 3. - <u>Soient</u> B <u>une algèbre sur un corps</u> k, A <u>un corps contenant</u> k <u>dans son centre</u>, $C = A \otimes_k B$, <u>et</u> N <u>un</u> B-<u>module</u>. <u>Alors le</u>

<u>radical du</u> C-<u>module</u> $A \otimes_k N$ <u>est</u> A-<u>étendu</u> (par.4, n°5 définition 1) <u>si l'une des deux conditions suivantes est vérifiée</u> :

a) k <u>est le corps des invariants d'un groupe d'automorphismes de</u> A

b) A <u>est un corps commutatif extension séparable de</u> k, N <u>est de type fini</u>.

Prouvons d'abord la conclusion dans l'hypothèse a). On vérifie aussitôt que si u est un automorphisme de A laissant fixe les éléments de k, alors l'endomorphisme $u \otimes 1$ de l'espace k-vectoriel $A \otimes_k N$ permute entre eux les sous-C-modules de cet espace, donc aussi les sous-C-modules maximaux, donc laisse stable l'intersection de ces derniers, c'est à dire le radical $\mathcal{R}_C(A \otimes_k N)$. La conclusion résulte alors de par.4, n°5, prop.7.

Plaçons nous maintenant dans l'hypothèse b), soit V l'intersection de $\mathcal{R}_C(A \otimes_k N)$ avec N, il faut prouver $\mathcal{R}_C(A \otimes_k N) \subset A \otimes_k V$. Soit $x = \sum_{i=1}^{m} a_i \otimes n_i$ un élément du radical de $A \otimes_k N$, on peut supposer les a_i linéairement indépendants sur k, tout revient à montrer qu'alors les n_i sont aussi dans le radical de $A \otimes_k N$ (et par suite dans V). Soit Ω une clôture algébrique de A, u un k-automorphisme de Ω, alors $(u \otimes 1)(x) = \sum u(a_i) \otimes n_i$ est dans le radical du module $u(A) \otimes_k N$ sur l'anneau $u(A) \otimes_k B$, donc d'après la proposition 2,a) il est aussi dans le radical du module $\Omega \otimes_k N$ sur l'anneau $C' = \Omega \otimes_k B$. Or A étant séparable on peut trouver m k-automorphismes u_j de A' tels que la matrice $(u_j(a_i))$ soit inversible. Alors pour des $\lambda_i \in \Omega$ donnés $(1 \leq i \leq m)$ on peut trouver des $\mu_j \in \Omega$ tels que $\sum_j \mu_j u_j(a_i) = \lambda_i$ pour tout i. Comme $\sum_j \mu_j (u_j \otimes 1)(x) = \sum \lambda_i \otimes n_i$ est dans le radical de $\Omega \otimes_k N$ et ceci quels que soient les $\lambda_i \in \Omega$, il s'ensuit que les n_i sont dans le radical de $\Omega \otimes_k N$, donc aussi dans le radical de $A \otimes_k N$, en vertu de l'inclusion de la proposition 2 appliquée au produit tensoriel $\Omega \otimes_A (A \otimes_k N)$. Cela achève la démonstration. (N.B. Si on arrivait à se débarrasser de l'hypothèse de finitude sur N dans prop. 2, a), on s'en débarrasserait aussi dans prop. 3, b) et ailleurs).

COROLLAIRE 1. - *Sous les conditions* a) *ou* b) *de la proposition* 3, *on a* $\mathcal{R}_C(A \otimes_k N) \subset A \otimes_k \mathcal{R}_B(N)$

Cela résulte en effet aussitôt de la proposition 3 et de l'inclusion (2) dans la proposition 2.

COROLLAIRE 2. - *Soient* B *une algèbre sur un corps* k, N *un* B-*module* K *une extension séparable de* k. *Alors on a la formule* $\mathcal{R}_{K \otimes_k B}(K \otimes_k N) = K \otimes_k \mathcal{R}_B(N)$ *dans chacun des cas suivants* :

a) K *est de degré fini sur* k *ou* N *est un* B-*module de type fini*.

b) N = B, *et le radical de* B *est nilpotent* (par exemple B est une algèbre d'Artin).

En effet, en vertu de la proposition 3, on a $\mathcal{R}_{K \otimes_k B}(K \otimes_k N) = K \otimes_k V$ où V est l'intersection du premier membre avec N, or dans les cas a) et b) cette intersection est précisément $\mathcal{R}_B(N)$ en vertu de prop. 2.

2. *Produit tensoriel de deux corps commutatifs*.

THEOREME 1. - *Soient* E *et* F *deux extensions d'un corps* k, *on suppose* E *ou* F *séparable sur* k. *Alors* $E \otimes_k F$ *est une* k *algèbre sans radical*.

C'est un cas particulier de prop. 3, b).

COROLLAIRE 1. - *Soient* E *et* F *deux extensions du corps* k, *l'une des deux étant séparable et l'une des deux étant de degré fini. Alors*

$E \otimes_k F$ est une k-algèbre composée d'un nombre fini de corps.

En effet, si par exemple E est de degré fini, alors $E \otimes_k F$ est une algèbre sur F de dimension finie donc un anneau d'Artin, et comme son radical est nul en vertu du théorème 1, c'est un anneau semi-simple (par.6, th.4, cor.2). Comme il est commutatif, c'est le composé direct d'un nombre fini de corps (par.5, prop.11).

COROLLAIRE 2. - Soient k un corps commutatif, E_i $(1 \leq i \leq n)$ des extensions de k, on suppose tous les E_i sauf un au plus séparables et tous les E_i sauf un au plus de degré fini. Alors le produit tensoriel des E_i est composé direct d'un nombre fini de corps.

Si $n < 2$ il n'y a rien à démontrer, pour $n = 2$ l'énoncé se réduit au corollaire 1, pour $n > 2$ on peut supposer que les E_i avec $i \geq 3$ sont séparables et de degré fini. Le corollaire 2 résulte alors par récurrence sur n du corollaire 1.

COROLLAIRE 3. - Soient k un corps commutatif, K une extension séparable de k, $f \in k[X]$ un polynôme sans facteurs multiples dans $k[X]$. Alors f est aussi sans facteurs multiples en tant qu'élément de $K[X]$.

Dire que f est sans facteurs multiples dans $k[X]$ signifie (par.6, prop.) que l'anneau $k[X]/(f)$ est semi-simple, c'est-à-dire composé direct d'un nombre fini de corps. D'après le corollaire 1 il en résulte que son produit tensoriel avec K est aussi le composé d'un nombre fini de corps. Or ce produit tensoriel s'identifie à $K[X]/(f)$, par suite f est aussi sans facteurs multiples dans $K[X]$.

COROLLAIRE 4. - Soient k un corps commutatif, E et F deux extensions de k. Alors le radical de la k-algèbre $E \otimes_k F$ est l'ensemble de ses éléments nilpotents.

Soit Ω une clôture algébrique de E. D'après la prop.2,a), le radical de $E \otimes_k F$ est contenu dans celui de $\Omega \otimes_k F = \Omega \otimes_E (E \otimes_k F)$, on peut donc supposer E algébriquement clos. Soit K le corps des invariants du groupe des k-automorphismes de E, on a $E \otimes_k F = E \otimes_K (K \otimes_k F)$, et en vertu de prop.3 le radical de $E \otimes_k F$ est engendré par celui de $K \otimes_k F$, il suffit donc de prouver que tout élément de ce dernier est nilpotent. Soit $u = \sum x_i \otimes y_i$ un élément de $\mathfrak{R}(K \otimes_k F)$. Soit p l'exposant caractéristique de k, il existe un entier m tel que $x_i^{p^m} \in k$ pour tout i (Chap.5, par.8, prop1) d'où résulte que $u^{p^m} = \sum x_i^{p^m} \otimes y_i^{p^m}$ est dans F. Comme cet élément est dans le radical de $K \otimes_k F$ donc non inversible, et à fortiori non inversible dans le corps F, il est nul, par suite u est bien nilpotent.

__Remarque__ Soient E et F deux extensions du corps k, et supposons que E soit séparable et de degré fini sur k, on peut alors préciser la structure de $E \otimes_k F$ comme suit. Soit x un générateur de E sur k (chap.5, par.11,prop.4), $f \in k[X]$ son polynôme minimal, alors E s'identifie à $k[X]/(f)$, donc $E \otimes_k F$ s'identifie à $F[X]/(f)$. Or f étant le polynôme minimal sur k d'un élément x séparable sur k, les racines de f dans une extension quelconque de k sont toutes simples, donc f n'a pas de facteurs multiples dans $F[X]$ et s'y décompose donc en un produit de polynômes irréductibles $f_1, \ldots, f_k \in F[X]$. Par suite $F[X]/(f)$ s'identifie à la somme directe des __corps__ $F[X]/(f_i)$.

L'hypothèse de séparabilité dans le théorème 1 est essentielle, comme le montre la

PROPOSITION 4. - __Soient__ k __un corps commutatif__, K __une extension de__ k, p __l'exposant caractéristique de__ k, Ω __une clôture algébrique de__ k,

$k^{p^{-1}}$ le corps image de k par l'automorphisme inverse de l'automorphisme $x \longrightarrow x^p$ de Ω. Les conditions suivantes sur K sont équivalentes :

a) K est séparable sur k

b) Pour toute extension L de k, $K \otimes_k L$ est une k-algèbre sans radical.

c) Pour toute extension L de k, l'anneau $K \otimes_k L$ n'a pas d'éléments nilpotents non-nuls.

d) $K \otimes_k k^{p^{-1}}$ n'a pas d'éléments nilpotents non nuls.

L'implication a) $\Longrightarrow$ b) n'est autre que le théorème 1, l'implication b) $\Longrightarrow$ c) résulte du fait qu'un élément nilpotent d'un anneau commutatif est dans le radical, l'implication c) $\Longrightarrow$ d) est triviale, reste à prouver que d implique a. Supposant d) vérifié, on veut donc prouver que K est séparable sur k, c'est-à-dire (chap. 5, par. 8, prop. 3) que K et $k^{p^{-1}}$ sont linéairement disjoints sur k. Cela signifie que si x_i ($1 \leq i \leq n$) sont des éléments de K linéairement indépendants sur k, ils sont aussi linéairement indépendants sur $k^{p^{-1}}$. Soient donc a_i des éléments de $k^{p^{-1}}$ tels que $\sum a_i x_i = 0$, considérons $z = \sum x_i \otimes a_i$, on a alors $z^p = \sum x_i^p \otimes a_i^p$, or $a_i^p \in k$ d'où $x_i^p \otimes a_i^p = a_i^p x_i^p \otimes 1$ d'où $z^p = (\sum a_i^p x_i^p) \otimes 1 = 0$ puisque $\sum a_i^p x_i^p = (\sum a_i x_i)^p = 0$. Donc z est nilpotent, donc nul, donc $a_i = 0$ pour tout i, ce qui prouve que les x_i sont bien linéairement indépendants sur $k^{p^{-1}}$ et achève la démonstration.

3. Extensions composées.

Soient k un corps commutatif, E et F deux extensions de k. On appelle extension composée de E et F une extension G de k muni de la structure supplémentaire définie par la donnée de deux k-isomorphismes u de

E dans G et v de F dans G, tels que G soit le corps engendré par u(E) et v(F). Deux extensions composées (G,u,v) et (G',u',v') de E et F sont donc isomorphes si et seulement s'il existe un k-isomorphisme φ de G sur G' tel que $u' = u\varphi$, $v' = v\varphi$. Soit B une base de transcendance de F sur k, alors il est immédiat que pour toute extension composée (G,u,v) de E et F, G est algébrique sur le corps engendré par E et v(B), donc G admet une base de transcendance sur u(E) contenue dans v(B). Soit alors Ω une extension algébriquement close de E admettant une base de transcendance dont la puissance est au moins égale à celle de B, alors l'isomorphisme u^{-1} de u(E) sur E peut se prolonger en un isomorphisme f de G dans Ω. Posant G' = f(G), $v' = f \circ v$ et désignant par u' l'isomorphisme identique de E dans G', on voit donc que (G,u,v) est isomorphe à (G',u',v'). Cela prouve la première partie de la

PROPOSITION 5. - Soient k un corps, Ω une extension algébriquement close de k, E et F deux sous-extensions, on suppose que Ω admet une base de transcendance sur E ayant une puissance au moins égale à celle d'une base de transcendance de F sur k. Toute extension composée de E et F est isomorphe à une extension composée de la forme (G_v,u,v) où v est un k-isomorphisme de F dans Ω, où G_v désigne le corps engendré par v(F) et E, et u l'application identique de E dans Ω. v étant fixé, les k-isomorphismes v' de F dans Ω qui définissent une extension composée isomorphe à celle définie par v, sont exactement les composés wv, où w est la restriction à v(F) d'un E-isomorphisme de G_v dans Ω.

La première assertion résulte des réflexions qui précèdaient, la dernière est une conséquence immédiate de la définition d'un isomorphisme de deux extensions composée.

COROLLAIRE. - Si F est de degré fini n sur k, il y a au plus n extension composées deux à deux non isomorphes de E et F.

En effet, il y a au plus n k-isomorphismes de F dans Ω.

La donnée d'une extension composée (G,u,v) revient aussi à la donnée d'une extension G de k et d'un homomorphisme w de la k-algèbre $E \otimes_k F$ dans G, tel que le corps engendré par l'image de $E \otimes_k F$ soit G : en effet u et v définissent $w = u \otimes v$, et w définit inversement u et v en prenant la restriction de w à E et à F. Soit $\mathfrak{y}$ l'idéal noyau de w, alors $E \otimes_k F/\mathfrak{y}$ est isomorphe au sous-anneau $w(E \otimes_k F)$ de G, et est par suite un anneau d'intégrité ; et G, qui est le corps des fractions de $w(E \otimes_k F)$, est donc isomorphe au corps des fractions Q de l'anneau d'intégrité $E \otimes_k F/\mathfrak{y}$. On peut considérer sur Q la structure d'extension composée de E et F définie par l'application canonique w' de $E \otimes_k F$ dans Q, alors l'extension composée G est isomorphe à l'extension composée Q. D'ailleurs, si on part d'une extension composée (G',u',v') isomorphe à (G,u,v), l'idéal $\mathfrak{y}'$ qui lui correspond est évidemment identique à $\mathfrak{y}$. Inversement, partant d'un idéal $\mathfrak{y}$ dans $E \otimes_k F$ tel que l'anneau quotient $E \otimes_k F/\mathfrak{y}$ soit un anneau d'intégrité, on peut former le corps des fractions Q de cet anneau, qui est une extension de k muni d'une structure d'extension composée de E et F, grâce à l'application canonique w de $E \otimes_k F$ dans Q ; l'idéal défini par cette extension composée est $\mathfrak{y}$.

DEFINITION 1. - Soit A un anneau commutatif, $\mathfrak{y}$ un idéal dans A. On dit que $\mathfrak{y}$ est un idéal premier si $A/\mathfrak{y}$ est un anneau d'intégrité.

Comme un anneau d'intégrité n'est pas réduit à $\{0\}$, il convient de remarquer qu'un idéal premier dans A est nécessairement distinct de A.

Les réflexions qui précédaient peuvent se résumer ainsi :

PROPOSITION 6. - <u>Soient</u> E <u>et</u> F <u>deux extensions d'un corps</u> k. <u>Pour toute extension composée</u> G <u>de</u> E <u>et</u> F, <u>il existe un unique idéal premier</u> $\mathfrak{y}$ <u>dans</u> $E \otimes_k F$ <u>tel que</u> G <u>soit isomorphe à l'extension composée, corps des fractions de</u> $E \otimes_k F/\mathfrak{y}$.

De façon imagée, on peut dire que l'ensemble des types d'extensions composées de E et F est en correspondance biunivoque naturelle avec l'ensemble des idéaux premiers de $E \otimes_k F$.

PROPOSITION 7. - <u>Soient</u> E <u>et</u> F <u>deux extensions d'un corps</u> k, <u>on suppose</u> E <u>ou</u> F <u>séparable, et</u> E <u>ou</u> F <u>de degré fini. Alors il n'y a qu'un nombre fini d'extensions composées</u> (G_i, u_i, v_i) <u>inéquivalentes entre elles, et l'homomorphisme de</u> $E \otimes_k F$ <u>dans le corps composé</u> $G = \prod_i G_i$, <u>défini par les homomorphismes</u> $u_i \otimes v_i$, <u>est un isomorphisme de</u> $E \otimes_k F$ <u>sur</u> G.

En vertu du corollaire 1 du th. 1, $E \otimes_k F$ est le composé direct d'un nombre fini de corps G_i, ses idéaux sont donc les sommes directes d'un certain nombre des G_i, et on voit aussitôt qu'un tel idéal $\mathfrak{y}$ est premier si et seulement s'il contient tous les G_i sauf l'un G_{i_0}, et alors $E \otimes_k F/\mathfrak{y}$ est isomorphe à G_{i_0}. La proposition 7 résulte alors de la proposition 6.

PROPOSITION 8. - <u>Soit</u> E <u>une extension galoisienne de degré fini d'un corps</u> k, G <u>son groupe de Galois</u>, F <u>une sur-extension de</u> F. <u>On définit un isomorphisme</u> w <u>de l'algèbre</u> $E \otimes_k F$ <u>sur l'algèbre produit</u> F^G <u>par la formule</u> $w(e \otimes f) = (s(e)f)_{s \in G}$. <u>Cet isomorphisme est compatible</u>

avec les opérations de G si on pose $s(e \otimes f) = s(e) \otimes f$, et $s(a_t)_{t \in G} = (a_{ts})_{t \in G}$.

Soit Ω une clôture algébrique de F. En vertu de proposition 5, toute extension composée de E et F est équivalente à une extension (F,u,v) où v est l'application identique de F dans F et u un k-isomorphisme de E dans Ω, donc un automorphisme de E puisque E est galoisien. D'après la même proposition, ces extensions composées sont non isomorphes deux à deux. La première assertion de la proposition 8 est donc un cas particulier de proposition 7. La vérification de la deuxième est évidente.

PROPOSITION 9. - Soit E une extension d'un corps k, et soit Ω une extension algébriquement close de E. Les conditions suivantes sont toutes équivalentes :

a) E est une extension radicielle de k (Chap.5, par.8, déf.1)

b) Pour toute extension F de k, $E \otimes_k F$ n'a qu'un seul idéal premier.

c) Pour toute extension F de k, deux extensions composées de E et F sont toujours équivalentes.

b') $E \otimes_k \Omega$ n'a qu'un seul idéal premier.

c') Deux extensions composées de E et Ω sont toujours équivalentes.

b) équivaut à c), et b') équivaut à c'), en vertu de la prop.6. Comme a) signifie que tout k-isomorphisme de E dans une extension algébriquement close donnée est réduite à l'identité (Chap.5, §8, prop.1), la proposition 5 (où l'on change les rôles de E et F) montre que a) implique c). D'ailleurs c) implique trivialement c'), enfin c') implique a), car d'après la prop. 5 les types d'extensions composées de E et Ω sont en correspondance biunivoque avec les k isomorphismes de E dans Ω, cela achève la démonstration.

4. Endomorphismes semi-simples et endomorphismes diagonalisables d'un espace vectoriel.

PROPOSITION 10. - Soient u un endomorphisme d'un espace vectoriel V de dimension finie sur un corps commutatif k, A la sous-algèbre de $\mathcal{L}_k(V)$ engendrée par 1 et u. Les propriétés suivantes sont équivalentes :

a) Tout sous-espace de V stable sous u admet un supplémentaire stable sous u.

b) Le A-module V est semi-simple.

c) L'algèbre A est semi-simple.

d) Le polynôme minimal P de u est sans facteurs multiples.

Les sous-espaces vectoriels de V stables sous u sont les sous-A-modules de V, donc a) $\Longleftrightarrow$ b). L'algèbre A est isomorphe à $k[X]/(P)$ (Chap.7, par.5, n°1) donc c) $\Longleftrightarrow$ d) d'après par.6 prop. . Enfin, b) $\Longleftrightarrow$ c) d'après la proposition 3 du par.5.

DEFINITION 2. - On dit que l'endomorphisme u de V est semi-simple s'il vérifie les conditions équivalentes de la prop.10.

DEFINITION 3. - Soit un endomorphisme d'un espace vectoriel V de dimension finie sur un corps k. On dit que u est diagonal par rapport à une base $(e_i)_{i\in I}$ de V si sa matrice par rapport à cette base est une matrice diagonale, c'est-à-dire si on a $u(e_i) = c_i e_i$ $(c_i \in k)$. u est dit diagonalisable s'il existe une base de V par rapport à laquelle u soit diagonal.

PROPOSITION 11. - Soit u un endomorphisme d'un espace vectoriel de dimension finie V sur un corps k. Pour que u soit diagonalisable,

<u>il faut et il suffit que</u> u <u>soit semi-simple et que les racines de son polynôme soient toutes dans</u> k.

La nécessité de la condition est évidente, la suffisance résulte de la prop.10 du chapitre VII, par.5.

COROLLAIRE 1. - <u>Supposons</u> k <u>algébriquement clos</u>. <u>Alors les conditions suivantes sur</u> u <u>sont équivalentes</u> :

a) u <u>est semi-simple</u>

b) <u>les racines du polynôme minimal de</u> u <u>sont simples</u>

c) u <u>est diagonalisable</u>.

Ce corollaire résulte aussitôt des propositions 10 et 11.

COROLLAIRE 2. - <u>Si</u> u <u>est diagonalisable</u>, <u>sa restriction à un sous-espace vectoriel</u> w <u>stable par</u> u <u>est aussi diagonalisable</u>.

En effet, le polynôme minimal de cette restriction divise celui de u, et il suffit donc d'appliquer le critère de la prop.11.

5. <u>Opérateurs absolument semi-simples</u>.

PROPOSITION 12. - <u>Soient</u> k <u>un corps commutatif</u>, V <u>un espace vectoriel de dimension finie sur</u> k, u <u>un endomorphisme de</u> V, K <u>une extension de</u> k, $V_{(K)}$ <u>et</u> $u_{(K)}$ <u>l'espace vectoriel et l'opérateur déduits de</u> V <u>et</u> u <u>par extension du corps des scalaires à</u> K. <u>Si</u> $u_{(K)}$ <u>est semi simple alors</u> u <u>est semi-simple</u>. <u>Si</u> u <u>est semi-simple et si</u> K <u>est séparable sur</u> k, <u>alors</u> $u_{(K)}$ <u>est semi-simple</u>.

Soit $P \in k[X]$ le polynôme minimal de u, c'est aussi le polynôme minimal de $u_{(K)}$. Si P est sans facteurs multiples dans $K[X]$, il ne peut manifestement avoir de facteurs multiples dans $k[X]$. La réciproque est vraie si K est séparable sur k (th. 1, cor.3). Cela prouve la prop.

DEFINITION 4. - *Soit* u *un endomorphisme d'un espace vectoriel* V *de dimension finie sur un corps* k. *On dit que* u *est absolument semi simple si pour toute extension* K *de* k, *l'opérateur* $u_{(K)}$ *déduit de* u *par extension à* K *du corps des scalaires est semi-simple.*

Un tel endo-morphisme est donc à fortiori semi-simple, et si k est parfait la réciproque est vraie en vertu de la proposition 12.

PROPOSITION 13. - *Soient* u *un endomorphisme d'un espace vectoriel* V *de dimension finie sur un corps* k, A *l'algèbre d'endomorphismes engendrée par* 1 *et* u, k' *un corps parfait extension de* k. *Les propriétés suivantes sont équivalentes* :

a) u *est absolument semi-simple.*

b) $u_{(k')}$ *est semi-simple.*

c) *Toutes les racines du polynôme minimal* P *de* u *sont simples.*

d) A *est composée directe de corps extension séparables de* k.

a) $\Longrightarrow$ b) trivialement. Soit Ω une clôture algébrique de k', b) implique que $u_{(\Omega)}$ est semi-simple (prop. 12), donc son polynôme minimal (qui n'est autre que P) a toutes ses racines distinctes, d'où b) $\Longrightarrow$ c) c) signifie que P se décompose dans $k[X]$ en produit de polynômes irréductibles P_1 dont toutes les racines sont simples, donc que A est isomorphe au composé direct de corps $k[X]/(P_1)$, et que ces derniers sont des extensions séparables de k, d'où c) $\Longleftrightarrow$ d). Enfin c) $\Longrightarrow$ a), car soit K une extension quelconque de k, prouvons que $u_{(K)}$ est semi-simple : en effet son polynôme minimal, qui est encore P, ne peut avoir de facteurs mutiples puisque toutes ses racines sont simples par hypothèse.

6. Familles d'endomorphismes semi-simples ou diagonalisables permutables.

PROPOSITION 14. - *Soit A une algèbre commutative de dimension finie sur un corps k. Si A est semi-simple, toute sous-algèbre de A est semi-simple. Réciproquement, si A est engendré par une famille $(A_i)_{i \in I}$ de sous-algèbres semi-simples, et si k est parfait, alors A est semi-simple.*

Une sous-algèbre B de A est une algèbre d'Artin commutative, et si A est semi-simple tout élément nilpotent de A est nul, à fortiori tout élément nilpotent de B est nul donc B est sans radical (par.6, cor. du th.3), donc B est semi-simple. Pour la réciproque, on peut supposer l'ensemble d'indices I fini. Par hypothèse chaque A_i est composé d'un nombre fini de corps, qui sont des extensions de degré fini de k, par ailleurs séparables puisque k est parfait. En vertu du cor.2 au théorème 1, le produit tensoriel des A_i est donc semi-simple. Il en est donc de même de A, qui s'identifie à une algèbre quotient de ce produit tensoriel.

PROPOSITION 15. - *Soient V un espace vectoriel de dimension finie sur un corps k, $\mathfrak{F}$ une famille d'endomorphismes deux à deux permutables de V, A l'algèbre d'endomorphismes de V engendrée par $\mathfrak{F}$ et 1. Pour que V soit un A-module semi-simple, il faut et il suffit que A soit une algèbre semi-simple. Alors tout $u \in \mathfrak{F}$ est semi-simple, et la réciproque est vraie si k est parfait.*

La première assertion résulte de la prop.3 du par.5. La deuxième résulte de la proposition 14.

COROLLAIRE 1. - Soient V un espace vectoriel de dimension finie sur un corps k, u et v deux endomorphismes absolument semi-simples permutables de V, alors $u+v$ et uv sont absolument semi-simples.

COROLLAIRE 2. - Les notations étant celles de la prop.15, les propriétés suivantes sont équivalentes :

a) Tous les $u \in \mathcal{F}$ sont absolument semi-simples (définition 4)

b) A est composé direct d'un nombre fini de corps séparables sur k.

c) Quelle que soit l'extension K de k, l'ensemble $\mathcal{F}_{(K)}$ des opérateurs $u_{(K)}$ déduits des $u \in \mathcal{F}$ par extension à K du corps des scalaires engendre une K-algèbre semi-simple.

Soit Ω une extension algébriquement close de k. a) signifie que les $u_{(\Omega)}$ $(u \in \mathcal{F})$ sont semi-simples, donc (prop.15) que la Ω-algèbre qu'ils engendrent est semi-simple. Or cette dernière s'identifie à $\Omega \otimes_k A$, donc $\Omega \otimes_k A$ et à fortiori A n'a pas d'élément nilpotent non nul, donc A est composé d'un nombre fini de corps A_i. De plus, pour tout i, $\Omega \otimes_k A_i$ est semi-simple, c'est-à-dire (prop.4) Ω_i est une extension séparable de k. Donc a) $\Longrightarrow$ b). b) $\Longrightarrow$ c), car en vertu du th.1, si b) est satisfaite, $K \otimes_k A$ est semi-simple pour toute extension K de k. Enfin c) $\Longrightarrow$ a) comme on voit en prenant $K = \Omega$ et appliquant la prop.15 à l'ensemble des $u_{(\Omega)}$ $(u \in \mathcal{F})$.

COROLLAIRE 3. - Soit A une algèbre commutative de dimension finie sur un corps k. Si A est composée directe d'extensions séparables de k, il en est de même de toute sous-algèbre B de A. Réciproquement, si A est engendrée par des sous-algèbres B_i qui sont composées directes d'extensions séparables de k, alors A est aussi composée directe d'extensions séparables de k.

Identifions A à l'ensemble des homothéties du A-module A_s, donc toute sous-algèbre de A a une algèbre d'endomorphismes de l'espace vectoriel $V = A_s$. Alors le corollaire 3 résulte aussitôt du cor. 2.

PROPOSITION 16. - Avec les notations de la proposition 15, les propriétés suivantes sont équivalentes :

a) Il existe une base de V par rapport à laquelle tous les $u \in \mathfrak{F}$ sont diagonaux.

b) L'algèbre A est composée directe d'algèbres réduites à k.

c) Tout $u \in \mathfrak{F}$ est diagonalisable.

b) implique a), car A étant semi-simple, le A-module V est somme directe de A-modules simples V_i, isomorphes à des composantes simples de A, donc de dimension 1 sur k. Prenant un élément non nul dans chaque V_i, on obtient la base cherchée. a) implique c) trivialement. Prouvons que c) implique b). En vertu du corollaire 2, A est composé direct d'un nombre fini de corps A_i, prouvons que chaque A_i est réduit à k. Soit $u \in A_i$, soit P son polynôme minimal sur k, c'est aussi son polynôme minimal en tant qu'endomorphisme de V, donc (prop.11) toutes ses racines sont dans k, donc on a $x \in k$.

7. Décomposition canonique d'une algèbre commutative.

PROPOSITION 17. - Soient A une algèbre commutative de dimension finie sur un corps k, R son radical (identique à l'ensemble de ses éléments nilpotents), $B = A/R$, B_i $(1 \leq i \leq n)$ les extensions de k composantes simples de l'algèbre semi-simple B, B_{is} la plus grande sous-extension séparable de B_i. Soit S l'ensemble des $x \in A$ tels que l'endomorphisme $u_x : y \longrightarrow xy$ de l'espace vectoriel A soit absolument semi-simple. Alors S est une sous-algèbre semi-simple de A composée directe d'extensions séparables de k, et c'est la plus grande sous algèbre de A ayant ces propriétés. L'homomorphisme canonique de A sur $B = A/R$ induit un isomorphisme de S sur l'algèbre composée directe des corps B_{is}.

Le fait que S soit une sous-algèbre résulte de prop.15, cor.1, et du cor.2 à la même proposition, on conclut que les corps composants de S sont des extensions séparables de k. D'ailleurs, d'après ce même corollaire, si L est une sous-algèbre de A composée directe d'extensions séparables de k, alors pour tout $x \in L$, u_x est absolument semi-simple, d'où $L \subset S$. Comme S n'a pas d'éléments nilpotents, on a $R \cap S = \{0\}$ donc l'homomorphisme canonique φ de S dans B est injectif. Reste à prouver que son image est la somme des B_{is}. Soit $s \in S$, s' son image dans B. L'endomorphisme $b \longrightarrow s'b$ de l'espace vectoriel B est absolument semi-simple, donc ses restrictions aux B_i le sont aussi, donc si s'_i est la composante de s' sur B_i, l'endomorphisme $b \longrightarrow s'_i b$ de l'espace vectoriel B_i est absolument semi-simple, donc son polynôme minimal a toutes ses racines simples (prop.13). Comme ce polynôme est aussi le polynôme minimal sur k de l'élément s'_i de l'extension B_i, on voit que s'_i est séparable sur k, c'est-à-dire est dans B_{is}, d'où $\varphi(S) \subset \sum_i B_{is}$. Reste à prouver que $\sum_i B_{is} \subset \varphi(S)$. Il suffit de prouver que tout élément b du premier membre dont toutes les composantes $b_i \in B_i$ sauf une sont l'élément unité de B_i, est dans $\varphi(S)$. (En effet, l'espace vectoriel engendré par les éléments du type envisagé contient les B_{is} donc est identique à leur somme). Soit i l'indice tel que $b_i \neq 1$, soit P le polynôme minimal de $b_i \in B_{is}$ sur k, P a toutes ses racines distinctes, et distinctes de 1. Soit $Q(X) = (X-1)P(X)$, Q a toutes ses racines distinctes et on a $Q(b) = 0$. Tout revient à trouver un représentant a de b dans A tel que $Q(a) = 0$, car alors le polynôme minimal de $(x \longrightarrow ax)$ divise A et a donc toutes ses racines distinctes, ce qui signifie $a \in S$ en vertu de prop.13. Soit a_1 un représentant quelconque de b, on a évidemment $Q(a_1) \in R$, on va alors prouver par récurrence sur l'entier $k \geq 1$ qu'il existe un représentant a_k de b tel que $Q(a_k) \in R^k$ (ce qui achèvera la démonstration, puisque R est nilpotent). Supposons donc trouvé un représentant a_{k-1} de b tel que $Q(a_{k-1}) \in R^{k-1}$ $(k \geq 2)$, et cherchons un $r \in R$ tel que $Q(a_{k-1}+r) \in R^k$. Or on a

$$Q(a_{k-1}+r) \equiv Q(a_{k-1}) + r\,Q'(a_{k-1}) \mod R^{2(k-1)}$$

en vertu du développement du premier membre suivant les puissances croissantes de r. Comme $2(k-1) \leq k$, il suffit de choisir r de telle façon que le deuxième membre soit nul. Nous aurons prouvé que c'est possible si nous montrons que $Q'(a_{k-1})$ est inversible. Or dire qu'un $x \in A$ est inversible signifie que l'idéal qu'il engendre est identique à A, c'est-à-dire n'est contenu dans aucun idéal maximal, ou enfin que son image dans B satisfait à la même condition. Or l'image de $Q'(a_{k-1})$ est $Q'(b)$, et $Q'(X) = P(X) + (X-1)P'(X)$. La composante de $Q'(b)$ dans B_{js} est donc $P(1)$ si $j \neq 1$, $(b_i - 1)P'(b_i)$ dans le cas contraire, donc $\neq 0$ dans tous les cas puisque P est le polynôme minimal de b_i et que b_i est séparable et $\neq 1$. Donc $Q'(b)$ est inversible, ce qui achève la démonstration.

S s'appelle la <u>composante semi-simple</u> de A. Si k est parfait, toute extension de k est séparable donc $B_i = B_{is}$ et par suite :

COROLLAIRE 1. - <u>Soit</u> A <u>une algèbre commutative de dimension finie sur un corps parfait</u> k. <u>Alors</u> A <u>est somme directe de son radical et de sa</u>

partie semi-simple.

COROLLAIRE 2. - *Soit A une algèbre commutative de dimension finie sur un corps k. Si A est somme de son radical et de sa composante semi-simple, il en est de même de toute sous-algèbre de A. Réciproquement, si A est engendrée par des algèbres qui sont somme de leur radical et leur composante semi-simple, il en est de même de A.*

$R + S = A$ signifie que A/R est composée d'extensions séparables de k. Soit alors B une sous-algèbre de A, son radical $R(B)$ (ensemble de ses éléments nilpotents) est $R \cap B$, donc $B/R(B)$ s'identifie à une sous algèbre de A/R, donc est elle-même composée d'extensions séparables de k en vertu de prop.15, cor.3. Réciproquement, si A est engendrée par des sous-algèbres B_i telles que $B_i/R \cap B_i$ soit composée directe de corps extensions séparables de k, alors A/R, qui est engendrée par des sous-algèbres isomorphes aux $B/R \cap B_i$, est elle-même composée directe de corps extensions séparables de k, en vertu du même corollaire.

COROLLAIRE 3. - *Soient A une algèbre commutative de dimension finie sur un corps k, V un A-module fidèle, R le radical de A, S sa composante semi simple. Pour qu'un $x \in A$ soit dans R (resp. S) il faut et il suffit que l'homothétie x_V soit nilpotent (resp. absolument semi-simple).*

Le premier cas est trivial puisque R est l'ensemble des éléments nilpotents de A. Le deuxième résulte du critère c de la prop.13, si on note que le polynôme minimal de x_V est identique au polynôme minimal de l'endomorphisme $y \longrightarrow xy$ de l'espace vectoriel A. Ces deux polynômes sont en effet identiques au polynôme unitaire unique, générateur de l'idéal dans $k[X]$ formé des polynômes f tels que $f(x) = 0$.

COROLLAIRE 4. - Soit A une algèbre commutative de dimension finie sur un corps k, supposons A somme de son radical et de sa partie semi-simple (par exemple k parfait). Soit V un A-module, de dimension finie sur k. Alors V est somme directe de sous-espaces vectoriels V_i $(1 \leq i \leq n)$ tels que :

a) chaque V_i est un S-module simple ;

b) pour tout $1 \leq j \leq n$, $W_j = \sum_{i=1}^{j} V_i$ est un sous-A-module de V.

Comme V est un A-module de longueur finie, il existe une suite de Jordan-Hölder $W_0 = \{0\} \subset W_1 \subset \ldots . \subset W_n = V$ de V. Comme V est un S-module semi-simple, on peut trouver pour tout i tel que $1 \leq i \leq n$ un supplémentaire V_i de W_{i-1} dans W_i stable sous S. Tout revient à montrer que V_i est un S-module simple, or V_i est isomorphe au S-module W_i/W_{i-1}, donc on sait que c'est un A-module simple, donc un A/R-module simple, donc un S-module simple puisque A/R s'identifie à S.

PROPOSITION 18. - Soit u un endomorphisme d'un espace vectoriel V de dimension finie sur un corps k. Supposons que u soit de la forme $u = u_s + u_n$ où u_s est absolument semi-simple, u_n nilpotent et u_s et u_n commutent ; alors une telle décomposition est unique, et u_s et u_n s'expriment comme polynômes en u à coefficients dans k. Si k est parfait, une telle décomposition existe toujours.

Soient A l'algèbre d'endomorphismes de V engendrée par 1, u_s, u_n, R son radical, S sa composante semi-simple. On a $u_s \in S$ (prop.17, cor.3) et comme l'image de u_s dans A/R engendre évidemment l'algèbre A/R, il s'ensuit que A/R est identique à l'image de S, donc A = R + S. Soit A' la sous-algèbre de A engendrée par u, alors A' est aussi somme de son radical et de sa partie semi-simple (prop.18, cor.2) et comme la somme de R et S est directe, on en conclut $u_s \in A'$, $u_n \in A'$, d'où $A' = A$. D'où aussitôt l'unicité de la décomposition $u = u_s + u_n$ et le fait que u_s et u_n s'expriment comme polynômes par rapport à u. Réciproquement, supposons l'endomorphisme u tel que l'algèbre A engendrée par 1 et u soit somme de son radical R et de sa partie semi-simple S (ce qui est toujours le cas si k est parfait). Alors on a $u = u_s + u_n$ avec $u_s \in S$ et $u_n \in R$, et d'après la prop.18, cor.3 cette décomposition satisfait aux conditions de la prop.18. Cela achève la démonstration.

Les endomorphismes u_s et u_n de la prop 18, dans le cas où ils existent, sont appelés resp. la composante semi-simple et la composante nilpotente de u.

COROLLAIRE 1. - Soit A une algèbre commutative de dimension finie sur un corps k, V un A-module de dimension finie sur k, R le radical de A et S sa partie semi-simple. Si $x = s + r$ ($s \in S$, $r \in R$) est un élément de S + R, alors l'homothétie x_V admet s_V et r_V comme composantes semi simple et nilpotente. Supposons que V soit un A-module fidèle, et soit $x \in A$. Pour qu'on ait $x \in R$ (resp. $x \in S$, resp. $x \in R+S$) il faut et il suffit que l'homothétie x_V soit nilpotente (resp. absolument semi-simple, resp. admette une composante semi-simple).

Toutes les assertions sont évidentes, sauf que si x_V admet une partie semi-simple, alors $x \in R+S$. Or comme les parties semi-simple et nilpotente de x_V sont des polynômes en x_V, ce sont des homothéties s_V et r_V de V, et d'après ce qu'on a vu on a $s \in S$, $r \in R$, d'où $x = s + r \in S+R$ ce qui achève la démonstration.

COROLLAIRE 2. - Soit V un espace vectoriel de dimension finie sur un corps k, $\mathcal{F}$ une famille d'endomorphismes deux à deux permutables de

V, A l'algèbre d'endomorphismes engendrée par 1 et $\mathfrak{F}$. Pour que A soit somme directe de son radical et de sa partie semi-simple S il faut et il suffit que tout $u \in \mathfrak{F}$ admette une partie semi-simple. Alors S est l'algèbre engendrée par 1 et les parties semi-simples des $u \in \mathfrak{F}$.

Pour tout $u \in \mathfrak{F}$, soit A(u) l'algèbre engendrée par 1 et u. On a vu dans la démonstration de la proposition 18 que u admet une partie semi-simple si et seulement si A(u) est somme de son radical et de sa partie semi-simple ; d'autre part A est l'algèbre engendrée par les A(u). Donc la première assertion résulte du corollaire 2 de la prop. 17. La dernière assertion résulte du fait que l'application de projection de A sur sa partie semi-simple S est un homomorphisme d'algèbres, transformant les générateurs $u \in \mathfrak{F}$ de A en leur partie semi-simple u_s.

PROPOSITION 19.- Soient V un espace vectoriel de dimension finie sur un corps k, $\mathfrak{F}$ un ensemble d'endomorphismes de V deux à deux permutables, A l'algèbre d'endomorphismes engendrée par $\mathfrak{F}$ et 1. Les propriétés suivantes sont équivalentes, et toujours satisfaites si k est algèbriquement clos :

a) Il existe une base (e_i) de V telle que pour tout $u \in \mathfrak{F}$, la matrice de u par rapport à cette base n'ait que des zéros au dessous de la diagonale principale, et u admette une partie semi-simple diagonale par rapport à (e_i).

b) Tout $u \in \mathfrak{F}$ admet une partie semi-simple diagonalisable.

c) A est somme de son radical et d'une algèbre composée directe d'algèbres réduites à k.

a) implique b) trivialement. b) implique c), car en vertu du cor.2 à la proposition 18, A est somme de son radical et de sa partie semi-simple S, de plus cette dernière est engendrée par 1 et les u_s ($u \in \mathfrak{F}$) qui sont diagonalisables, donc S est composée directe d'algèbres réduites à k (prop.16). Enfin c) implique a), car avec les notations du cor.4 à la prop.17, il suffit de prouver que les V_i sont de dimension 1 (car alors, prenant dans chaque V_i un élément e_i non nul, on obtient la base cherchée). Or la partie semi-simple S de A étant isomorphe à la composée directe de corps réduits à k, et V_i étant un S-module simple donc isomorphe à une composante simple de S, la conclusion s'ensuit.

COROLLAIRE.- Soit $\mathfrak{F}$ un ensemble d'opérateurs nilpotents deux à deux permutables dans un espace vectoriel V de dimension finie sur un corps algébriquement clos k. Si V est non nul, il existe un élément non nul de V annulé par tous les $u \in \mathfrak{F}$.

En effet, les conditions de la proposition 19 sont satisfaites, et il suffit de remarquer (avec les notations de cette proposition) que pour tout $u \in \mathfrak{F}$, $u_n = u - u_s$ annule e_1, comme on voit par l'inspection de sa matrice.

8.- Décomposition canonique d'un automorphisme.

(N. B. Ce numéro, demandé par Borel, ne semble pas dans l'esprit de ce chapitre. Comme on ne s'en servira sans doute qu'au moment de parler de groupes algébriques, il semble raisonnable de le renvoyer à cet endroit).

DEFINITION 5. Soit V un espace vectoriel de dimension finie sur un corps k. Un endomorphisme u de V est dit unipotent si 1-u est nilpotent, autrement dit si u n'a d'autre valeur propre que 1.

Si u est unipotent, 0 n'est pas valeur propre de u, donc u est inversible. Si K est extension de k, et si $u_{(K)}$ désigne l'opérateur déduit de u par extension à K du corps des scalaires, u est unipotent si et seulement si $u_{(K)}$ l'est. Si u est unipotent et diagonalisable, u est réduit à l'identité ; donc si k est parfait et si u est unipotent et semi-simple, u est réduit à l'identité.

PROPOSITION 20. - Soient V un espace vectoriel de dimension finie sur un corps k, x un automorphisme de V. Pour que x puisse se mettre sous la forme $x = x_s x_u$, avec x_s absolument semi-simple, x_u unipotent et x_s cet x_u permutables, il faut et il suffit que x admette une décomposition en partie semi-simple et nilpotente (prop. 18), et alors cette x_s et x_u sont déterminés de façon unique : x_s est la partie semi-simple de x, et $x_u = 1 + x_s^{-1} x_n$, où x_n est la partie nilpotente de x. x_s et x_u peuvent s'exprimer comme polynômes en u à coefficients dans k. Une telle décomposition de u existe toujours si k est parfait.

Si on peut écrire $x = x_s x_u$ avec x_s absolument semi-simple et x_u unipotent, x_s et x_u permutables, posons $x_u = 1+v$, où v est nilpotent et permutable à x_s, on a donc $x = x_s + x_s v$ et ceci constitue une décomposition de x en somme d'un opérateur absolument semi-simple et d'un opérateur nilpotents permutables. Réciproquement, si x admet une telle décomposition $x = x_s + x_n$, alors x_s est inversible (sinon le noyau de x_s, qui est stable sous l'opérateur nilpotent x_n, contiendrait un élément non nul annulé par ce dernier, donc aussi par x, contrairement à l'hypothèse que u est un automorphisme) et posant $x_u = 1+x_s^{-1}x_n$ on trouve $x = x_s x_u$, où x_s est absolument semi-simple, x_u unipotent, et x_s permute à x_u. On sait déjà que x_s s'exprime comme polynôme par rapport à x ; il en est de même de $x_u = x_s^{-1}x$, car on voit aussitôt que x_s^{-1} donc aussi son produit par x appartient au bicommutant de x, donc on peut appliquer par.1, prop.6 au module associé à l'endomorphisme u. La dernière assertion de la prop.20 résulte de la prop.18.

§ 8. Radical et semi-simplicité d'un produit tensoriel

Modules séparables

1. Produit tensoriel avec un module simple.

Dans ce numéro et le suivant, nous considèrerons, comme dans par.7, N°1, deux algèbres A et B sur un corps k, et nous identifierons A et B aux sous-algèbres $A \otimes 1$ resp. $1 \otimes B$ de leur produit tensoriel $A \otimes_k B = C$. Pour tout A-module M et tout B-module N, $M \otimes_k N$ sera considéré comme un C-module de la façon naturelle déjà expliquée. Dans le présent paragraphe, nous allons surtout expliciter certaines conséquences utiles des résultats généraux donnés dans par.7 N°1.

Nous aurons besoin par la suite du

LEMME 1.- (Au chap. III, appendice ?). *Soient D un corps, P (resp. Q) un espace vectoriel à droite (resp. à gauche) sur D, $(P_i)_{i \in I}$ une famille de sous-espaces vectoriels de P, $(Q_j)_{j \in J}$ une famille de sous-espaces vectoriels de Q, identifions, pour tout sous-espace vectoriel V de P, et tout sous-espace vectoriel W de Q, $V \otimes_D W$ à un sous-groupe de $P \otimes_D Q$ par l'application du premier groupe dans le second, produit tensoriel des injections canoniques de V dans P et de W dans Q. Alors on a :*

$$\bigcap_{ij} (P_i \otimes_D Q_j) = (\bigcap_i P_i) \otimes_D (\bigcap_j Q_j) \tag{1}$$

Que l'application canonique $V \otimes_D W \to P \otimes_D Q$ soit injective résulte aussitôt du fait que V et W admettent des supplémentaires dans P et Q. Posons maintenant $V = \bigcap_i P_i$, $W = \bigcap_j Q_j$, tout revient à prouver que le premier membre de (1) est contenu dans $V \otimes_D W$. Or $V \otimes_D W$ est l'intersection de $P \otimes_D W$ et de $V \otimes_D Q$, comme on voit encore aussitôt en décomposant P et Q en sommes directes de V resp. W et d'un supplémentaire.

Par suite, il suffit de prouver que le premier membre de (1) est contenu dans $P \otimes_D W$ et dans $V \otimes_D Q$. Prouvons par exemple la première de ces inclusions, il suffit à fortiori de prouver $\bigcap_j (P \otimes_D Q_j) \subset P \otimes_D W$. Or, prenant une base $(e_t)_{t \in T}$ dans P, les deux membres de cette inclusion s'identifient respectivement aux sous-groupes $\bigcap_j (Q_j^{(T)})$ et $(\bigcap_j Q_j)^{(T)}$ du groupe $Q^{(T)}$, et sont donc manifestement identiques.

COROLLAIRE.- Soient D un corps, P (resp. Q) un espace vectoriel à droite (resp. à gauche) sur D, $(P_i)_{i \in I}$ (resp. $(Q_j)_{j \in J}$) une famille d'espaces vectoriels à droite (resp. à gauche) sur D. Soit pour tout $i \in I$ (resp. $j \in J$) u_i (resp. v_j) une application linéaire de P dans P_i (resp. de Q dans Q_j) et supposons que tout élément de P (resp. Q) annulé par tous les u_i (resp. v_j) soit nul. Alors l'application de $P \otimes_D Q$ dans $\prod_{i,j} P_i \otimes_D Q_j$, dont les composantes sont les applications $u_i \otimes_D v_j$ de $P \otimes_D Q$ dans $P_i \otimes_D Q_j$, est injective.

En factorisant l'application considérée en le produit des applications naturelles $P \otimes_D Q \longrightarrow \prod_i (P_i \otimes_D Q) \longrightarrow \prod_{i,j} (P_i \otimes_D Q_j)$, on est ramené au cas où l'un des deux ensembles I, J est réduit à un élément. Supposons que ce soit J. Comme le noyau de $u_i \otimes_D v$ s'identifie à $P_i' \otimes_D Q$, où P_i' désigne le noyau de u_i, notre assertion résulte alors du lemme 1.

PROPOSITION 1.- Soient A et B deux algèbres sur un corps k, M un A-module, N un B-module, Supposons N simple, soit D le corps commutant de N, Z son centre, D^o le corps opposé à D. Identifions le C-module $M \otimes_k N$ à $(M \otimes_k D) \otimes_D N$ ou à $(M \otimes_k Z) \otimes_Z N$. Alors on a :

(2) $\mathfrak{R}_C(M \;{}_k N) = \mathfrak{R}_{A \otimes_k D^o}(M \otimes_k D) \otimes_D N \subset \mathfrak{R}_{A \otimes_k Z}(M \otimes_k Z) \otimes_Z N$

En tant que B-module, $M \otimes_k N = (M \otimes_k D) \otimes_D N$ est isotypique de type N ; donc (par.4, prop.5, cor.1) ses sous-B-modules sont exactement les sous-groupes de la forme $V \otimes_D N$, où V est un sous-espace vectoriel de l'espace vectoriel à droite $M \otimes_k D$ sur D, qu'on peut considérer aussi comme un espace vectoriel à gauche sur D^o. Un tel sous-module est aussi un sous-A-module, donc un sous-C-module, si et seulement si V est un sous-A-module, donc un sous-$(A \otimes_k D^o)$-module. Donc les sous-modules L de $M \otimes_k N$ correspondent biunivoquement aux sous-modules V de $M \otimes_k D$ par la correspondance précédente. Cette correspondance respectant les relations d'inclusion, aux sous-modules V correspondent les sous-modules L maximaux, d'où, en désignant par I l'ensemble des sous-modules maximaux de $M \otimes_k D$: $\mathfrak{R}_C(M \otimes_k N) = \bigcap_{V \in I}(V \otimes_D N)$. En vertu du lemme 1, le deuxième membre est égal à $(\bigcap_{V \in I} V) \otimes_D N = \mathfrak{R}_{A \otimes_k D^o}(M \otimes_k D) \otimes_D N$, d'où la première relation dans (2). Posons $C' = A \otimes_k D^o$, et explicitons $\mathfrak{R}_{C'}(M \otimes_k D)$. Ecrivons $M \otimes_k D = (M \otimes_k Z) \otimes_Z D = (M \otimes_k Z) \otimes_Z D^o$; comme Z est le corps des invariants du groupe des automorphismes intérieurs du corps D^o, on peut appliquer le corollaire à la prop.2,a) du par.7, (où on remplace B par $A \otimes_k Z$, A par D^o, N par $M \otimes_k Z$ et M par D^o), ce qui donne $\mathfrak{R}_{C'}(M \otimes_k D) \subset \mathfrak{R}_{A \otimes_k Z}(M \cap_k Z) \otimes_Z D$. D'où $\mathfrak{R}_{C'}(M \otimes_k N) \otimes_D N \subset \mathfrak{R}_{A \otimes_k Z}(M \otimes_k Z) \otimes_Z D \otimes_D N$, ce qui (compte tenu de l'associativité du produit tensoriel) n'est autre que la dernière inclusion dans la formule (2).

COROLLAIRE 1. - <u>Sous les conditions de la prop.1, pour que $M \otimes_k N$ soit un C-module sans radical</u> (resp. <u>semi-simple</u>, resp. <u>simple</u>) <u>il faut et il suffit que $M \otimes_k D$ soit un</u> $(A \otimes_k D^o)$-<u>module sans radical</u> (resp.

semi-simple, resp. *simple*). *Pour que* $M \otimes_k N$ *soit un* C-*module sans radical*, *il suffit aussi que* $M \otimes_k Z$ *soit un* $A \otimes_k Z$-*module sans radical*.

Les assertions relatives au radical sont conséquence immédiate des formules (2). Les autres résultent de la définition, compte tenu de la correspondance biunivoque signalée plus haut entre sous-modules de $M \otimes_k N$ et sous-modules de $M \otimes_k D$.

Si on suppose que c'est M qui est simple (N étant un B-module quelconque) on vérifie aussitôt que la formule (2) se remplace par :

(2 bis) $\quad \mathcal{R}_C(M \otimes_k N) = M \otimes_{D'^o} \mathcal{R}_{D'^o \otimes_k B}(D'^o \otimes N) \subset M \otimes_{Z'} \mathcal{R}_{Z' \otimes_k B}(Z' \otimes_k N)$

où D' désigne le corps commutant de M, D'^o le corps opposé, Z' le centre de D'. Si M et N sont tous les deux simples, l'application successive de (2) et (2 bis), ou le raisonnement de la proposition 1 directement, donne aussitôt les résultats suivants :

COROLLAIRE 2. - *Soient* M *un* A-*module simple*, N *un* B-*module simple*, D' *le corps commutant de* M *et* Z' *le centre de* D', D *le corps commutant de* N *et* Z *le centre de* D, *considérons* $M \otimes_k N$ *comme un* C-*module* ($C = A \otimes_k B$) *et comme un* $D' \otimes_k D$-*module*. *Alors on a* $\mathcal{R}_C(M \otimes_k N) = \mathcal{R}(D' \otimes D).(M \otimes_k N)$. *De plus* $\mathcal{R}(D' \otimes_k D)$ *est l'idéal engendré par* $\mathcal{R}(Z' \otimes_k Z)$. *En particulier*, *pour que* $M \otimes_k N$ *soit sans radical*, *il faut et il suffit que* $D' \otimes_k D$ *soit un anneau sans radical*, *ou aussi que* $Z' \otimes_k Z$ *soit un anneau sans radical*.

Il faut seulement montrer encore que l'idéal engendré par $\mathcal{R}(Z' \otimes_k Z)$ dans l'anneau $D' \otimes_k D$ est contenu dans le radical de ce dernier. Or cela résulte du fait que les éléments de $\mathcal{R}(Z' \otimes_k Z)$ sont nilpotents (par.7, th.1, cor.4) et contenus dans le centre de $D' \otimes_k D$.

De même, une double application du corollaire 1 prouve :

COROLLAIRE 3. - Dans les conditions du corollaire précédent, pour que $M \otimes_k N$ soit un C-module semi-simple (resp. simple), il faut et il suffit que l'anneau $D' \otimes_k D$ soit semi-simple (resp. soit un corps).

(N.B.- Le rédacteur ignore si la deuxième inclusion dans (2) n'est pas nécessairement une égalité).

2. Modules et algèbres séparables : critères de séparabilité.

La prop.4 du par.7 conduit à poser la définition suivante :

DEFINITION 1. - Soient A une algèbre sur un corps k, M un A-module. On dit que M est séparable (sur k) si, quelle que soit l'extension K de k, $K \otimes_k M$ est un $(K \otimes_k A)$-module sans radical. L'algèbre A est dité séparable (sur k) si le A-module A_s l'est, c'est-à-dire si pour toute extension K de k, $K \otimes_k A$ est un anneau sans radical.

En vertu de la proposition citée, si A est une extension de k, cette définition coincide avec la définition donnée au Chap.V d'une extension séparable de k. Notons aussi que A est une k-algèbre séparable si et seulement si l'algèbre opposée A^o l'est. Si M est séparable sur k, M est sans radical, et si k' est parfait la réciproque est vraie en vertu de § 7, prop.3 b), cor. Enfin, pour que le A-module M soit séparable sur k, il faut et il suffit qu'il le soit en tant que module sur son anneau de homothéties A_M.

PROPOSITION 2. - Soient A une algèbre sur k, M un A-module, K une extension de k. Si M est séparable sur k, alors le $(K \otimes_k A)$-module $K \otimes_k M$ est séparable sur K.

Ceci résulte aussitôt de la définition, compte tenu de l'associativité du produit tensoriel.

PROPOSITION 3. - Soit A une algèbre sur un corps k. Si M est un

A-module séparable sur k, alors tout sous-module N de M est séparable. Soit $(M_i)_{i \in I}$ une famille de A-modules ; pour que son produit (resp. sa somme directe) soit un A-module séparable, il faut et il suffit que chaque M_i le soit.

Soit M un A-module, N un sous-module. Pour toute extension K de k, le $(K \otimes_k A)$-module $K \otimes_k N$ s'identifie à un sous-module de $K \otimes_k M$, donc est sans radical si ce dernier est sans radical (par.6, prop.2), d'où la première assertion de la proposition. Soit $(M_i)_{i \in I}$ une famille de A-modules. Les M_i s'identifient à des sous-modules de la somme directe et du produit de la famille (M_i), donc sont séparables sur k si $\sum M_i$ ou $\prod M_i$ l'est, d'après ce qui précède. Inversement, supposons les M_i séparables, prouvons que leur produit est un module séparable sur k, ce qui impliquera en même temps que la somme directe est séparable, puisqu'elle est un sous-module du produit. Soit K une extension de k. Les applications k-linéaires naturelles de $K \otimes_k \prod_i M_i$, produits tensoriels de l'identité dans K par les projections de $\prod_i M_i$ sur ses facteurs, définissent une application k-linéaire naturelle de $K \otimes_k \prod M_i$ dans $\prod_i (K \otimes_k M_i)$. Cette application est d'ailleurs A-linéaire, et elle est injective, en vertu du cor. du lemme 1. Donc $K \otimes_k \prod_i M_i$ est isomorphe à un sous-module de $\prod (K \otimes_k M_i)$, qui est sans radical puisque ses facteurs sont sans radical ; il s'ensuit que $K \otimes_k \prod M_i$ est sans radical, donc que $\prod_i M_i$ est séparable, ce qui achève la démonstration.

PROPOSITION 4 (Exercice 7). - Soient A une algèbre sur un corps k, M un A-module de type fini, K un corps parfait, extension algébrique de k. Si $K \otimes_k M$ est un $K \otimes_k A$-module sans radical, alors M est séparable *sur* k. *En particulier, si* $K \otimes_k A$ *est un anneau sans radical*, A *est une* k-*algèbre séparable*.

Soit L une extension quelconque de k, on doit prouver que le radical du $L \otimes_k A$-module $L \otimes_k M$ est nul. Soit Ω une clôture algébrique de L, on a $\Omega \otimes_k M = \Omega \otimes_L (L \otimes_k M)$, et $L \otimes_k M$ est un $(L \otimes_k A)$-module de type fini, donc en vertu de la proposition 2,a) du par.7 le radical de $L \otimes_k M$ est contenu dans celui du $(\Omega \otimes_k A)$-module $\Omega \otimes_k M$, il suffit de prouver que ce dernier est nul. Or K étant algébrique sur k, on peut supposer K contenu dans Ω, et on peut donc écrire $\Omega \otimes_k M =$ $= \Omega \otimes_K (K \otimes_k M)$. K étant parfait, Ω est une extension séparable de K, de plus $(K \otimes_k M)$ est un $(K \otimes_k A)$-module de type fini, on est donc dans les conditions d'application du cor. à la prop. 3 a) du par.7, qui implique que $\mathcal{R}_{\Omega \otimes_k A}(M \otimes_k A)$ est nul puisque $\mathcal{R}_{K \otimes_k A}(K \otimes_k M)$ est nul par hypothèse.

THEOREME 1. - *Soient* A *une algèbre sur un corps* k, M *un* A-*module simple*, D *son corps commutant*, Z *le centre de* D. *Les propriétés suivantes sont équivalentes* :

a) M *est séparable sur* k

b) D *est une* k-*algèbre séparable*

c) Z *est une extension séparable de* k.

Soit K une extension de k. En vertu du cor.2 à la prop.1 le radical de $K \otimes_k M$ est nul si et seulement si celui de l'anneau $K \otimes_k D$ est nul, d'ou l'équivalence de a) et b) ; et le radical de $K \ {}_k D$ est nul si et seulement si celui de $K \otimes_k Z$ l'est, d'où l'équivalence de b) et c).

Le th.1 conjugué avec la prop.3, donne des conditions nécessaires et suffisantes pour qu'un module semi-simple sur A soit séparable. Plus particulièrement :

COROLLAIRE 1. - *Soient A une algèbre d'Artin sur un corps k, M un A-module fidèle. Les propriétés suivantes sont équivalentes :*

a) *A est une k-algèbre séparable.*

b) *Tout A-module est séparable sur k.*

b') *M est un A-module séparable sur k.*

c) *A est semi-simple, et ses composantes simples sont des k-algèbres séparables.*

d) *A est semi-simple et son centre est une algèbre séparable sur k.*

b) implique trivialement a) et b'), prouvons que b') implique b), ce qui établira en même temps (en faisant $M = A_s$) que a) implique b), d'où l'équivalence de a), b), b'). M étant séparable, son radical est nul, comme ce radical contient $\mathfrak{r}(A).M$ et que M est un module fidèle, $\mathfrak{r}(A)$ est nul, donc A est semi-simple (par.6, th.4, cor.2). Donc M est somme directe de sous-modules simples M_i, qui sont séparables comme sous-module de M qui est séparable (prop.3). D'autre part, M étant un module fidèle sur l'anneau semi-simple A, tout A-module N est isomorphe à une somme directe de modules simples, isomorphes à des composantes simples M_i de M, donc N est séparable en vertu de prop.3, ce qui prouve b). Ainsi a), b), b') sont équivalentes. De plus a) implique, on l'a vu, que A est semi-simple, donc que chaque composante simple A_i est un A-module simple en vertu de b), donc A_i est séparable sur k comme module sur son anneau d'homothéties A_i, ce qui signifie que A_i est une k-algèbre séparable d'où c). Réciproquement, c) implique que les composantes simples A_i de A sont des A-modules séparables sur k. Il en est donc de même de leur somme directe A, d'où a).

Reste à montrer que la propriété d) est équivalente aux autres. Pour ceci, on est aussitôt ramené au cas où A est simple. Soit alors S un A-module simple (nécessairement fidèle), D son corps commutant, Z le centre de D. D'après ce qui a été vu, A est une k-algèbre séparable si et seulement si S est un A-module séparable sur k, ce qui a lieu si et seulement si Z est une k-algèbre séparable (th.1). Or identifiant A à l'anneau des homothéties de S, on sait (par.5, th.2 b) que A est le commutant de D, donc Z est aussi le centre de A, ce qui achève la démonstration.

COROLLAIRE 2. - Soient A une algèbre sur un corps k, M un A-module, A_M l'anneau des homothéties de M et B le commutant de M. On suppose que M et son contremodule sont de longueur finie (par exemple M de dimension finie sur k). Alors les propriétés suivantes sont équivalentes :

a) M est un A-module séparable sur k.

b) M est un B-module séparable sur k.

c) A_M est une k-algèbre séparable.

d) B est une k-algèbre séparable.

On peut supposer $A = A_M$. Alors A est le commutant de B en vertu de par.4, th.1, cor.1. D'ailleurs A et B sont des anneaux d'Artin (par.2, prop.8). Donc a) $\Longleftrightarrow$ c) et b) $\Longleftrightarrow$ d) en vertu de l'équivalence des propriétés a) et b') dans le cor.1. D'ailleurs l'intersection $A \cap B$ est le centre commun de A et B, donc c) $\Longleftrightarrow$ d) en vertu du cor.1

COROLLAIRE 3. - *Soient A une algèbre sur un corps k, M un A-module, de dimension finie sur k. Pour que M soit séparable sur k, il faut et il suffit que pour toute extension K de k, le $(K \otimes_k A)$-module $K \otimes_k M$ soit semi-simple. En particulier, si A est de dimension finie sur k, A est une k-algèbre séparable si et seulement si pour toute extension K de k, $K \otimes_k A$ est une K-algèbre semi-simple.*

Comme $K \otimes_k M$ est de dimension finie sur K, et à fortiori un $(K \otimes_k A)$-module de longueur finie, il revient au même de dire qu'il est semi-simple ou qu'il est sans radical (par.6, th.4) d'où la conclusion. - Nous dirons qu'un A-module de dimension finie sur k est *absolument semi-simple* (sur k) s'il est séparable sur k, en particulier nous dirons que la k-algèbre A est absolument semi-simple sur k, si elle est séparable et de dimension finie. En vertu de par.7 prop.13, un endomorphisme u d'un espace vectoriel V de dimension finie sur k est absolument semi-simple (par.7, déf.4) si et seulement si l'algèbre d'endomorphismes engendrée par u et 1 est absolument semi-simple, ou encore si et seulement si le module associé à u (chap.VII, par.5) est absolument semi-simple. Tout le monde est content.

3. *Produit tensoriel avec un module séparable.*

THEOREME (?) 2. - *Soient A et B deux algèbres sur un corps k, $C = A \otimes_k B$, M un A-module, N un B-module. Si M est séparable sur k* ($n^o 2$, déf.1) *et N sans radical, alors $M \otimes_k N$ est un C-module sans radical*

N étant sans radical est isomorphe à un sous-module d'un produit $\prod_i N_i$ de B-modules simples, donc $M \otimes_k N$ est isomorphe à un sous-module de $M \otimes_k \prod_i N_i$, qui lui-même s'identifie à un sous-module de $\prod_i (M \otimes_k N_i)$ ($n^o 1$, cor. au lemme 1). Il suffit donc de prouver que chaque $M \otimes_k N_i$ est un C-module sans radical, ce qui nous ramène au cas où N est un B-module simple. Soit alors D son corps commutant, Z le centre de D. M étant séparable, il s'ensuit par définition que $M \otimes_k Z$ est un $(A \otimes_k Z)$-module sans radical, d'où résulte (prop. 1, cor. 1) que $M \otimes_k N$ est un C-module sans radical, ce qui achève la démons.

COROLLAIRE 1. - *Soient A et B deux algèbres sur un corps k, $C = A \otimes_k B$, M un A-module séparable sur k, N un B-module quelconque. Alors on a* $\mathfrak{R}_{A \otimes_k B}(M \otimes_k N) \subset M \otimes_k \mathfrak{R}_B(N)$.

En vertu de par. 6 prop. cor. 1 il suffit de montrer que $(M \otimes_k N)/(M \otimes_k \mathfrak{R}_B(N))$ est un C-module sans radical, or ce module s'identifie à $M \otimes_k (N/\mathfrak{R}_B(N))$, qui est sans radical en vertu de th. 2, puisque $N/\mathfrak{R}_B(N)$ est sans radical.

COROLLAIRE 2. - *Soient A et B deux algèbres sur le corps k. Si A est séparable, on a* $\mathfrak{R}(A \otimes_k B) \subset A \otimes_k \mathfrak{R}(B)$.

Il suffit de faire $M = A_s$, $N = B_s$ dans le corollaire 1.

COROLLAIRE 3. - *Soient A et B deux algèbres sur un corps k, $C = A \otimes_k B$, M un A-module, N un B-module. Si M et N sont séparables sur k, il en est de même du C-module $M \otimes_k N$.*

Il faut montrer que pour toute extension K de k, $K \otimes_k (M \otimes_k N)$ est un $K \otimes_k (A \otimes_k B)$-module sans radical. Or ce module s'identifie au module $(K \otimes_k M) \otimes_k N$ sur $(K \otimes_k A) \otimes_k B$, dont le premier facteur est un $(K \otimes_k A)$-module sans radical puisque M est séparable, et le deuxième est séparable sur k, d'où la conclusion en vertu du th. 2 (où l'on échange le rôle des facteurs M et N).

4. *Semi-simplicité d'un produit tensoriel de modules.*

PROPOSITION 5. - *Soient* A *et* B *des algèbres sur un corps* k, $C = A \otimes_k B$, M *un* A-*module*, N *un* B-*module*, *on considère le* C-*module* $M \otimes_k N$

1°) *Si* M *et* N *sont semi-simples*, *l'un des deux étant séparable sur* k *et l'un des deux étant de dimension finie sur* k, *alors* $M \otimes_k N$ *est semi-simple*.

2°) *Si* $M \otimes_k N$ *est semi-simple* (resp. *simple*), $M \neq \{0\}$ et $N \neq \{0\}$, *alors* M *et* N *sont semi-simples* (resp, *simples*).

3°) *Si* k *est algébriquement clos*, M *et* N *simples*, *et* M *ou* N *de dimension finie*, *alors* $M \otimes_k N$ *est simple*.

Démontrons 1°). On peut se limiter au cas où M et N sont simples. Alors $M \otimes_k N$ est sans radical en vertu du th.2. Supposons par exemple M de dimension finie sur k, alors $M \otimes_k N$ est un B-module de longueur finie, donc à fortiori un C-module de longueur finie, donc semi-simple puisqu'un module d'Artin sans radical est semi-simple (par.6, th.4).

Supposons maintenant $M \otimes_k N$ semi-simple sur C. Soit N' un sous-B-module de N, alors $M \otimes_k N'$ est un sous-C-module de $M \otimes_k N$, il existe donc un projecteur e de $M \otimes_k N$ sur $M \otimes_k N'$. Comme $M \neq \{0\}$, on peut trouver un $m \in M$ et une forme k-linéaire h sur M tels que $h(m) = 1$. Alors $n \longrightarrow (h \otimes 1)(e(m \otimes n))$ est un B-homomorphisme de N dans $k \otimes_k N'$ qui transforme tout $n' \in N'$ en $1 \otimes n' \in k \otimes_k N'$. Composant avec l'isomorphisme canonique de $k \otimes_k N'$ sur N', on trouve donc un projecteur de N sur N', ce qui prouve que N est semi-simple. On voit de même que M est semi simple.

Plaçons nous maintenant dans les hypothèses de 3), supposons par exemple que M est de dimension finie, alors son commutant est réduit à k (par.4, lemme 3), et la conclusion résulte alors de prop.1, cor.3

COROLLAIRE 1. - Soient A une algèbre sur un corps k, M un A-module, K une extension de k.

1°) Supposons K ou M est séparable sur k, et K ou M de dimension finie sur k. Si M est semi-simple, alors $K \otimes_k M$ est un $(K \otimes_k A)$-module semi-simple.

2°) Si $K \otimes_k M$ est un $(K \otimes_k A)$-module semi-simple (resp. simple), alors M est un A-module semi-simple (resp. simple).

3°) Supposons k algébriquement clos, et K ou M de dimension finie sur k. Alors M est simple si et seulement si $K \otimes_k M$ est un $(K \otimes_k A)$-module simple.

COROLLAIRE 2. - Soient A et B deux algèbres sur un corps k.

1°) Supposons A ou B séparable sur k, et A ou B de dimension finie. Alors si A et B sont semi-simples, il en est de même de l'algèbre $A \otimes_k B$.

2°) Si $A \otimes_k B$ est semi-simple (resp. est un corps) alors A et B sont semi-simples (resp. sont des corps).

PROPOSITION 6 (à renvoyer au par.9 ?). - Soient A et B deux algèbres simples sur un corps k, supposons A ou B de dimension finie sur k, et A ou B de centre k. Alors $A \otimes_k B$ est une algèbre simple.

Une algèbre simple sur k de centre k étant séparable sur k en vertu de th.1, cor.1, il résulte du corollaire 2, 1°) que $A \otimes_k B$ est semi-simple. Pour prouver qu'elle est simple il suffit donc de prouver que son centre est un corps, ce qui résulte aussitôt du

LEMME 2. - Soient A et B deux algèbres sur un corps k, Z et Z' leurs centres, alors le centre de $A \otimes_k B$ est $Z \otimes_k Z'$.

Soit $u = \sum_i a_i \otimes b_i$ un élément du centre de $A \otimes_k B$, il suffit de montrer qu'il est contenu dans $Z \otimes_k B$ et dans $A \otimes_k Z'$, prouvons par exemple la deuxième inclusion. On peut supposer les a_i linéairement indépendants. Pour tout $b \in B$, on a $ub = bu$ c'est-à-dire $\sum a_i \otimes (bb_i - b_i b) = 0$, d'où $bb_i - b_i b = 0$ pour tout i, et par suite $b_i \in Z'$ pour tout i, d'où $u \in A \otimes_k Z'$.

5. <u>Modules simples sur un produit tensoriel d'algèbres.</u>

LEMME 3. - <u>Soient</u> A <u>et</u> B <u>deux algèbres sur un corps</u> k, P <u>un module simple sur</u> $A \otimes_k B$, <u>de dimension finie sur</u> k. <u>Alors</u> P <u>est isomorphe à un quotient d'un module</u> $M \otimes_k N$, <u>où</u> M (resp. N) <u>est un module simple sur</u> A (resp. B) <u>de dimension finie sur</u> k. <u>Les classes des modules simples</u> M <u>et</u> N <u>sont bien déterminées par la classe de</u> P.

Soit M un sous-A-module non nul minimal de P. Munissons $\mathcal{L}_A(M,P)$ de la structure de B-module provenant de la structure de B-module de P (ce qui est possible, les opérations de B dans P étant des homomorphismes pour la structure de A-module de P). L'application naturelle φ de $M \otimes_k \mathcal{L}_A(M,P)$ dans P est $(A \otimes_k B)$-linéaire, comme on vérifie aussitôt. Soit N un sous-B-module non nul minimal de $\mathcal{L}_A(M,P)$ (un tel N existe car $\mathcal{L}_A(M,P)$ est de dimension finie sur k et non réduit à $\{0\}$). Alors φ induit un $(A \otimes_k B)$-homomorphisme non nul de $M \otimes_k N$ dans P, donc <u>sur</u> P puisque P est simple, ce qui achève la démonstration de la première assertion. De plus comme $M \otimes_k N$ est en tant que A-module, isotypique de type M, on voit que la classe de M est bien déterminée par celle de P. Il en est de même de celle de N, pour la même raison.

PROPOSITION 7. - <u>Soient</u> A <u>et</u> B <u>deux algèbres sur un corps algébriquement clos</u>, C(A) (resp. C(B), C(A $\times$ B)) <u>l'ensemble des classes modules simples sur</u> A (resp. B, resp. $A \otimes_k B$) <u>qui sont de dimension finie sur</u> k. <u>Pour tout</u> $S_i \in C(A)$ <u>et tout</u> $T_j \in C(B)$, $S_i \otimes_k T_j$ <u>est un</u> $(A \otimes_k B)$-<u>module</u>

<u>simple de dimension finie sur</u> k (prop. 5, 3°) <u>dont on désigne la classe par</u> p(i,j). <u>L'application</u> p <u>de</u> $C(A) \times C(B)$ <u>dans</u> $C(A \otimes_k B)$ <u>ainsi définie est bijective</u>.

Elle est surjective, car en vertu du lemme 3, tout module simple P sur $A \otimes_k B$, de dimension finie sur k, est isomorphe à un quotient d'un module $S_i \otimes_k T_j$, donc à $S_i \otimes_k T_j$ lui-même puisque ce module est simple. p est injective en vertu de la dernière assertion du lemme 3.

PROJET D'ADDITION AU CHAPITRE VIII D'ALGEBRE

On propose d'ajouter au §5 (Anneaux simples et semi-simples) un nouveau numéro intitulé "Duals et produits tensoriels de modules sur un anneau semi-simple", qui pourrait par exemple se placer entre les actuels n^os 4 et 5. Voici la rédaction proposée de ce numéro.

On désigne par A un anneau semi-simple.

PROPOSITION 1. - <u>Soit</u> E <u>un</u> A-<u>module</u> (<u>à gauche ou à droite</u>) <u>de type fini. L'application canonique de</u> E <u>dans son bidual est alors un isomorphisme</u>.

Décomposant E en somme directe de modules simples E_i, on voit immédiatement qu'une condition nécessaire et suffisante pour que l'assertion soit vraie pour E est qu'elle le soit pour chaque E_i. Or, chaque E_i est isomorphe à un sous-module de A, considéré comme module à gauche ou à droite sur lui-même. Le même raisonnement que ci-dessus, appliqué à A au lieu de E, montre alors qu'il suffit de démontrer la proposition dans le cas où E = A ; or elle est vraie dans ce cas parce que A est un module monogène libre.

PROPOSITION 2. - <u>Soient</u> E <u>un module à droite de type fini sur</u> A et F un module à gauche de type fini sur A. Soit Γ un sous-anneau du centre de A. L'application canonique de $E \otimes_A F$ dans le module des applications doublement linéaires de $E^* \otimes_\Gamma F^*$ dans A (où E^* et F^* sont les duals de E et de F ; cf. Appendice II au chap.III) est alors un isomorphisme.

Représentons E comme somme directe de modules simples E_i et F comme somme directe de modules simples F_j ; on voit tout de suite que, pour que l'assertion soit vraie de $E \otimes_A F$, il faut et suffit qu'elle le soit pour chaque $E_i \otimes_A F_j$. Or un module simple à gauche (resp. à droite) est isomorphe à un idéal à gauche (resp. à droite de A). On voit donc qu'il suffit de démontrer la proposition dans le cas où $E = A_d$, $F = A_g$. Or, elle est vraie dans ce cas, puisque E et F ont alors chacun une base de un élément.

Nous allons maintenant déterminer la structure de $E \otimes_A F$ dans le cas où E et F sont des modules simples. Soit $A = A_1 + \dots + A_n$ la décomposition de A en somme directe d'idéaux bilatères qui sont des anneaux simples ; soit e_i l'élément unité de A_i. On sait qu'il y a des indices i et j tels que $EA_k = 0$ si $k \neq i$, $A_k F = 0$ si $k \neq j$: on a alors $xe_i = x$ si $x \in E$, $e_j y = y$ si $y \in F$. Si $i \neq j$, on a $x \otimes_A y = xe_i \otimes_A y = x \otimes_A e_i y = 0$ quels que soient $x \in E$ et $y \in F$, d'où $E \otimes_A F = \{0\}$. Supposons donc à partir de maintenant que $i = j$. Soit K le commutant de E, qui est un corps : alors E admet une structure de module sur K, et les opérations de K commutant par définition à celles de A ; pour tout A-module à gauche G, $E \otimes_A G$ admet par suite une structure d'espace vectoriel sur K. Soit D l'espace vectoriel $E \otimes_A F$; F est isomorphe à un idéal à gauche minimal de A_i, et A_i est somme directe d'un certain nombre, soit n, de modules isomorphes à F ; par ailleurs, $E \otimes_A A_j = 0$ si $j \neq i$; il en résulte que $E \otimes_A A$ est somme directe de n espaces isomorphes à D. Mais $E \otimes_A A$ s'identifie à E, et la structure d'espace vectoriel de $E \otimes_A A$ sur K s'identifie alors à la structure de module sur K de E. Or la dimension de E sur K est égale à la longueur du A-module à droite A_i considéré comme module sur son commutant (prop.5, §4), donc à la longueur de A_i considéré comme module à gauche sur lui-même, c'est-à-dire à n. On en conclut que D est un espace vectoriel de dimension 1 sur K. Donc, si i = j, et si Γ est un sous-anneau du centre de A, $E \otimes_A F$ est un Γ-module isomorphe au commutant de E.

PROJET D'ADDITION A L'APPENDICE I DU CHAPITRE III

p.7, l.7 du bas. Remplacer "Soit Γ le centre..." par "Soit Γ un sous-anneau du centre..."

p.8. Avant la formule de la l.4, insérer : " Λ : ".

Entre la fin du passage en retrait de la p.8 et le début de l'alinéa suivant, ("Lorsque A est commutatif..."), insérer ce qui suit.

Posons $U = \mathcal{L}_A(E,E')$, $V = \mathcal{L}_A(F,F')$; si $w \in U \otimes_\Gamma V$, désignons par Λ_w l'image de w par Λ. Si $z \in E \otimes_A F$, l'application $w \longrightarrow \Lambda_w(z)$ de $U \otimes_\Gamma V$ dans $E' \otimes_A F'$ est évidemment Γ-linéaire. On déduit donc de Λ une application Λ', que l'on appelle encore canonique, de $E \otimes_A F$ dans $\mathcal{L}_\Gamma(U \otimes_\Gamma V, E' \otimes_A F')$. Nous allons considérer plus particulièrement le cas où $E' = A_d$, $F' = A_g$; dans ce cas, U et V ne sont autres que les duals E^* et F^* de E et F, et $E' \otimes_A F'$ s'identifie à A. Observons maintenant que E^* (resp. F^*) possède une structure de A-module à gauche (resp. à droite) ; les opérations de Γ dans E^* et dans F^* sont certaines des opérations de A et commutent avec toutes les opérations de A. Donc $E^* \otimes_{\Gamma} F^*$ est muni de structures de module à gauche et à droite sur A, les opérations de Γ étant certaines des opérations de A. Une application Γ-linéaire ζ de $E^* \otimes_{\Gamma} F^*$ est dite *doublement linéaire* si $\zeta(aw) = a\,\zeta(w)$, $\zeta(wa) = \zeta(w)a$ pour tout $w \in E^* \otimes F^*$ et tout $a \in A$. Les applications doublement linéaires de $E^* \otimes_{\Gamma} F^*$ dans A forment évidemment un sous-module de $\mathcal{L}_{\Gamma}(E^* \otimes_{\Gamma} F^*, A)$, que nous désignerons par $\mathcal{L}_{A,A}(E^* \otimes_{\Gamma} F^*, A)$. Nous allons montrer que Λ' applique $E \otimes_A F$ dans $\mathcal{L}_{A,A}(E^* \otimes F^*, A)$. Il suffit de montrer que, si $x \in E$, $y \in F$, $z = x \otimes_A y$, $w \in E^* \otimes F^*$, on a $\Lambda_{aw}(z) = a\Lambda_w(z)$, $\Lambda_{wa}(z) = \Lambda_w(z)a$. Il suffit de faire la vérification dans le cas où w est le produit tensoriel dans $E^* \otimes F^*$ d'un élément u de E^* et d'un élément v de F^* ; dans ce cas, Λ_w est l'application $(au) \otimes v$, $\Lambda_{wa} = u \otimes (va)$, $\Lambda_w = u \otimes v$. On a donc $\Lambda_{aw}(z) = (au)(x)v(y) = au(x)v(y) = a\Lambda_w(z)$, et de même $\Lambda_{wa}(z) = \Lambda_w(z)a$. On a donc une application linéaire

$$\Lambda' : E \otimes_A F \longrightarrow \mathcal{L}_{A,A}(E^* \otimes_{\Gamma} F^*, A)$$

que l'on appelle encore canonique. Si $z = x \otimes_A y$, $\Lambda'(z)$ applique le produit tensoriel dans $E^* \otimes_A F^*$ d'un élément $u \in E^*$ et d'un élément $v \in F^*$ sur l'élément $u(x)v(y)$ de A.

Supposons que E (resp. F) soit somme directe de modules E_i $(1 \leq i \leq h)$ (resp. F_j, $1 \leq j \leq k$); $E \otimes_A F$ est alors somme directe des $E_i \otimes_A F_j$; E^* (resp. F^*) est somme directe des duals E_i^* (resp. F_j^*) des E_i (resp. F_j), et $E^* \otimes F^*$ est somme directe des $E_i^* \otimes F_j^*$; il est clair que, pour tout (i,j), la restriction de Λ' à $E_i \otimes_A F_j$ est l'application canonique de ce module dans $\mathcal{L}_{A,A}(E_i^* \otimes F_j^*, A)$.

Si chacun des modules E, F *admet une base finie*, *l'application*

<u>canonique</u> Λ' <u>est un isomorphisme de</u> $E \otimes_A F$ <u>sur</u> $\mathcal{L}_{A,A}(E^* \otimes_\Gamma F^*, A)$. Tenant compte de ce qu'on vient de dire, on voit qu'il suffit de le montrer dans le cas où E et F sont des modules libres monogènes, donc encore quand $E = A_d$, $F = A_g$. Dans ce cas, on a $E \otimes_A F = A$, l'élément $a \otimes_A b$ s'identifiant à ab. Par ailleurs, E^* et F^* s'identifient à A_g et A_d respectivement (en identifiant toute forme linéaire sur A_d ou A_g à sa valeur en 1). Une application doublement linéaire θ de $E^* \otimes F^*$ est déterminée par sa valeur en l'élément $1 \otimes_\Gamma 1$, qui est un élément a de A. Or $\Lambda'(a \otimes_A 1)$ applique $1 \otimes_\Gamma 1$ sur a ; il en résulte immédiatement que Λ' est un isomorphisme.