RÉDACTION N° 165

COTE : NBR 066

TITRE : ANNEAUX PRIMITIFS (ÉTAT 3)

ASSOCIATION DES COLLABORATEURS DE NICOLAS BOURBAKI

NOMBRE DE PAGES : 75

NOMBRE DE FEUILLES : 75

ANNEAUX PRIMITIFS (Etat 3)

Sommaire

§ 1. Modules semi-simples.

1. Modules simples. 2. Modules semi-simples. 3. Modules semi-simples homogènes. 4. Commutant et bicommutant. 5. Commutant et bicommutant. Cas des modules semi-simples.

§ 2. Radical. Représentations linéaires.

1. Définitions. 2. Détermination du radical. 3. Généralités sur les représentations linéaires. 4. Extension du corps de base dans les représentations linéaires. 5. Effet d'une extension du corps de base sur le radical d'une algèbre.

§ 3. Anneaux d'Artin.

1. Anneaux d'Artin. 2. Le radical d'un anneau d'Artin. 3. Anneaux d'Artin primitifs. 4. Anneaux d'Artin semi-primitifs. 5. Modules sur un anneau d'Artin simple. 6. Modules sur un anneau d'Artin semi-simple. 7. Algèbres semi-simples. 8. Algèbres simples et semi-simples sur un corps algébriquement clos.

§ 4. Produits tensoriels d'algèbres semi-simples.

1. Un lemme sur les produits tensoriels. 2. Produit tensoriel d'une algèbre séparable et d'une algèbre semi-primitive. 3. Extension du corps de base. 4. Isomorphismes d'algèbres simples. 5. Commutation dans les algèbres simples. 6. Groupe de Brauer. 7. Extension du corps de base, corps de décomposition. 8. Le critère de décomposition. 9. Existence de corps de décomposition galoisiens. 10. Classes d'algèbres simples décomposées par une extension galoisienne du corps de base (Remarques).

§ 5. Représentations des groupes.

1. Norme et trace d'une représentation. 2. Représentations linéaires des groupes. 3. Théorème de Maschke.

Appendice. Le radical d'une algèbre quelconque.

1. Modules sur une algèbre. 2. Le radical d'une algèbre. 3. Adjonction d'un élément unité.

Commentaires du rédacteur.

La rédaction est vaguement essentiellement conforme aux ordres de la Tribu (n°19, nov. 1949). Principales différences :

Le §1 (modules semi-simples, représentations, radical) a été coupé en deux : modules semi-simples d'un côté, et radical et représentations de l'autre.

Dans le §2 (radical, représentations), on a inséré un n° assez long (n°4) sur l'extension du corps de base dans les rep. linéaires (cf. le bouquin de Chevalley sur les groupes algèbriques, p.64). Ces résultats ne sont pas utilisés par la suite ; on pourrait peut être les vider ?

Pour égayer un peu sa rédaction, le rédacteur a essayé de faire les produits tensoriels d'algèbres semi-simples avec le minimum de conditions de finitude. D'où le n°5 du § 2 .

Dans le § 4, il a réintroduit le groupe de Brauer, non pas parce que "c'est de la cohomologie", mais justement parce que ca n'en est pas ! Plus précisément, la cohomologie fournit une interprétation du groupe $\mathcal{B}_{K/k}$ des classes d'algèbres sur k décomposées par K , lorsque K/k est galoisienne finie ; mais pour pouvoir le démontrer, il faut avoir en mains certains résultats purement algébriques (tel le critère de décomposition) ; ce sont ces résultats qu'il a donnés dans les n°s 7,8,9 .

Le théorème de Maschke a été réintroduit au § 5, pour des raisons analogues : même quand on aura fait les groupes compacts, on ne l'obtiendra pas. Il faut donc le faire ici même. (En fait, le th. de Maschke pourrait aussi bien venir avec la cohomologie des groupes, puisque ce n'est qu'un cas particulier du fait que $h.x = 0$, si x appartient à un groupe de cohomologie d'un groupe fini à h éléments).

Pour le reste du § , le rédacteur s'est conformé aux ordres de la tribu, autrement dit a rédigé l'ensemble vide

Les anneaux sans élément unité ont été relégués en Appendice. Le rédacteur a trouve fort agréable d'en être débarrassé ainsi. Il signale cependant un léger canular ; si l'on ajoute un élément unité à un anneau d'Artin semi-primitif, on ne trouve plus un anneau d'Artin. Conséquence loufoque : on ne peut plus démontrer (sinon directement !) qu'un anneau d'Artin semi-primitif a un élément unité. Ce n'est d'ailleurs pas bien grave, et il propose de laisser les choses en l'état.

Enfin, le rédacteur signale qu'il lui a été très difficile de placer en marge des points d'exclamation pour indiquer les démonstrations nonasinitrottantes.

ANNEAUX PRIMITIFS.

Sauf mention expresse du contraire, tous les anneaux considérés dans ce Chapitre (Appendice exclu) sont supposés possèder un élément unité ; tous les modules considérés sont des modules unitaires à gauche.

§ 1. Modules semi-simples.

1. Modules simples.

DEFINITION 1.- Un A-module unitaire E est dit simple s'il vérifie les deux conditions suivantes :

a). $E \neq (0)$.

b). Considéré comme groupe abélien à opérateurs, E est un groupe simple (au sens de Alg.I, § 6, déf. 14).

La condition b) équivaut à dire que E n'admet pas d'autre sous-module que (0) et E . S'il en est ainsi, tout élément de E différent de 0 engendre E (E est donc un module monogène) et réciproquement cette dernière propriété entraîne b) .

Exemples.

1. Lorsque A = Z, anneau des entiers, les modules simples ne sont autres que les groupes abéliens simples distincts de (0), autrement dit les groupes $Z/(p)$, où p est premier.

2. Soit E un espace vectoriel sur un corps k , et soit $A = L(E)$ l'anneau des endomorphismes de E . L'application $(a,x) \longrightarrow a(x)$ de $A \times E$ dans E définit sur E une structure de A-module unitaire simple si $E \neq (0)$. En effet si x et y sont deux éléments de E ; $x \neq 0$, il existe un endomorphisme a de E tel que $a(x)=y$; ceci signifie que le sous-A-module engendré par x est E tout entier, et E est bien un A-module simple.

Soit E un A-module simple. Puisque E est monogène, E est isomorphe à $A_s/\mathfrak{a}$; où $\mathfrak{a}$ est un idéal à gauche de A (Chap.II, § 1, Prop.11).

Comme les sous-modules de $A_s/\mathfrak{a}$ correspondent biunivoquement aux idéaux à gauche $\mathfrak{b}$ de A tels que $\mathfrak{a} \subset \mathfrak{b} \subset A$, on voit que $\mathfrak{a}$ est un idéal maximal de A. Le même raisonnement montre que, réciproquement, si $\mathfrak{m}$ est un idéal maximal de A, le A-module $A_s/\mathfrak{m}$ est simple. Donc :

PROPOSITION 1.- Pour qu'un A-module soit simple il faut et il suffit qu'il soit isomorphe à un module $A_s/\mathfrak{m}$, où $\mathfrak{m}$ est un idéal à gauche maximal de A.

2. Modules semi-simples.

DÉFINITION 2. Un A-module unitaire E est dit semi-simple s'il existe une famille de sous-modules simples de E dont E soit somme directe.

A la différence de Alg. I, § 6, déf. 15, on ne suppose pas que la famille en question est finie.

Exemples.

1. Le A-module réduit à (0) est semi-simple, car il est somme directe de la famille vide de sous-modules simples.

2. Si A est un corps, il y a identité entre A-modules et espaces vectoriels sur A ; un module simple est un espace vectoriel à une dimension, et puisque tout espace vectoriel admet une base, on voit que tout A-module est semi-simple.

3. On verra plus loin que, si A est un anneau d'Artin semi-simple, tout A-module est semi-simple.

4. Le groupe Z, considéré comme Z-module, n'est pas semi-simple.

PROPOSITION 2.- Soit E un A-module somme (non nécessairement directe) d'une famille de sous-modules simples E_λ, $\lambda \in L$. Si F est un sous-module de E, il existe une partie M de L telle que la somme de la famille E_λ, $\lambda \in M$, soit directe et constitue un supplémentaire de F dans E.

Soit Φ l'ensemble des parties N de L telles que la somme $G_N = \sum_{\lambda \in N} E_\lambda$

soit directe et que $G_M \cap F = (0)$. Puisque Φ est de caractère fini, Φ possède un élément maximal M . Il reste à voir que G_M est un supplémentaire de F dans E . Puisque $G_M \cap F = (0)$, cela revient à montrer que $G_M + F = E$, ou encore que tout E_λ , $\lambda \in L$, est contenu dans $G_M + F$. Ceci est évident si $\lambda \in M$; supposons donc $\lambda \in \complement M$, et $E_\lambda \not\subset G_M + F$. Puisque $E_\lambda \cap (G_M + F)$ est un sous-module de E_λ , distinct de E_λ , c'est (0) et la somme $E_\lambda + G_M + F$ est directe. Il s'ensuit que $M \cup \{\lambda\} \in \Phi$, contrairement au caractère maximal de M : Ceci achève la démonstration.

COROLLAIRE 1. Dans les hypothèses précédentes E est somme directe d'une sous-famille de la famille des E et est donc semi-simple.

On applique la proposition avec $F = (0)$.

COROLLAIRE 2. Tout sous-module F d'un module semi-simple E est semi-simple et admet un supplémentaire.

D'après la proposition précédente F admet un supplémentaire semi-simple G . Appliquant ceci à G , on voit que G admet un supplémentaire semi-simple H . Puisque deux supplémentaires quelconques de G sont isomorphes, F est isomorphe à H et est donc bien semi-simple.

COROLLAIRE 3. Tout module quotient E/F d'un module semi-simple E est semi-simple.

En effet, F admet un supplémentaire semi-simple G , et E/F est isomorphe à G .

COROLLAIRE 4. Soit E un module somme directe d'une famille E_λ, $\lambda \in L$, de sous-modules simples. Tout sous-module simple F de E est isomorphe à l'un des E_λ .

D'après la proposition précédente il existe $M \subset L$ tel que $\sum_{\lambda \in M} E_\lambda$ soit supplémentaire de F . Comme $\sum_{\lambda \in \complement M} E_\lambda$ est supplémentaire de $\sum_{\lambda \in M} E_\lambda$, il s'ensuit que F est isomorphe à $\sum_{\lambda \in \complement M} E_\lambda$, et puisque F est simple $\complement M$ est réduit à un seul élément.

Remarques. 1. Lorsque A est un corps, le cor.1 redonne l'existence d'une base dans tout espace vectoriel.

2. Lorsqu'un module E est somme directe de deux familles E_λ et F_μ de sous-modules simples, tout élément de l'une de ces familles est isomorphe à un élément de l'autre d'après le cor.4 .

Nous allons maintenant montrer que le cor.2 à la prop.2 admet une réciproque. De façon plus précise :

PROPOSITION 3. Si tout sous-module d'un module E admet un supplémentaire dans E , E est semi-simple.

Soit R(E) la propriété "tout sous-module de E admet un supplémentaire" Si F est un sous-module de E , R(E) $\Rightarrow$ R(F). En effet, soit F' un sous-module de F ; puisque R(E) est vrai, F' admet un supplémentaire G dans E , et $G \cap F$ est un supplémentaire de F' dans F .

Montrons maintenant que R(E) et $E \neq (0)$ entraînent que E contient un sous-module simple. D'après ce qui précède on peut supposer E monogène donc de la forme $A_s/\mathfrak{a}$, où $\mathfrak{a}$ est un idéal à gauche de A distinct de A . (puisque $E \neq (0)$). D'après le théorème de Krull $\mathfrak{a}$ est contenu dans un idéal à gauche maximal $\mathfrak{m}$; puisque R(E) est vrai, le sous-module $\mathfrak{m}/\mathfrak{a}$ de $E = A_s/\mathfrak{a}$ admet un supplémentaire. Ce supplémentaire est isomorphe à $(A_s/\mathfrak{a})/(\mathfrak{m}/\mathfrak{a})$, donc à $A_s/\mathfrak{m}$ et c'est un module simple d'après la prop.1. Nous avons donc bien montré que E contient un sous-module simple.

Démontrons maintenant la proposition 3. Soit E un module tel que R(E) soit vrai ; soit E_0 le module somme de tous les sous-modules simples de E ; soit F un supplémentaire de E_0 dans E. Puisque R(F) est vrai, il résulte de ce qu'on vient de voir que ou bien F contient un sous-module simple, ou bien F = (0). Le premier cas étant exclu par définition même de F, on a donc F = (0) et $E = E_0$, ce qui montre que E est semi-simple (cor. 1 de la prop. 2).

La Tribu enjoignait au rédacteur de montrer que si tout sous-module monogène de E admet un supplémentaire, E est semi-simple. Le rédacteur n'a été foutu de trouver, ni démonstration, ni contre-exemple.

3. Modules semi-simples homogènes.

DÉFINITION 3. Un module semi-simple est dit homogène s'il est somme directe de sous-modules simples isomorphes.

Exemples.

1. Le module (0), tout module simple, sont des modules homogènes.
2. Tout espace vectoriel est un module homogène sur son corps des scalaires.

PROPOSITION 4. Soient E un module semi-simple, S_α un module simple. La somme E_α des sous-modules de E isomorphes à S_α est un sous-module homogène de E, appelé composant homogène de E d'espèce S_α. Le module E est somme directe des sous-modules E_α relatifs aux divers modules simples S_α.

Ecrivons E comme somme directe de modules simples : $E = \sum_{\iota \in I} N_\iota$, et soit J_α l'ensemble des $\iota \in I$ tels que N_ι soit isomorphe à S_α. Posons $F_\alpha = \sum_{\iota \in J_\alpha} N_\iota$. Il est clair que F_α est un module homogène et que E est somme directe des différents F_α. Il nous suffit donc de prouver que $E_\alpha = F_\alpha$. On a évidemment $F_\alpha \subset E_\alpha$. D'autre part, soit G

un sous-module de E isomorphe à S_α , et soit G' l'image canonique de G dans E/F_α ; puisque G est simple, le noyau de l'homomorphisme $G \to G'$ et soit (0), soit (G), et G' est donc soit isomorphe à G , soit réduit à (0). Mais E/F_α est isomorphe à $\sum_{\iota \in \complement J_\alpha} N_\iota$; si G' était isomorphe à G , d'après la prop.2, cor.4, G' serait isomorphe à l'un des N_ι , $\iota \in \complement J_\alpha$, ce qui n'est pas. Le module G' est donc réduit à (0), ce qui signifie que $G \subset F_\alpha$. On a donc $E_\alpha \subset F_\alpha$, d'où $E_\alpha = F_\alpha$, ce qui achève la démonstration.

Remarque.

Les résultats des n° 2 et 3 sont valables, non seulement pour les A-modules unitaires, mais pour tous les groupes abéliens à opérateurs. Ceci peut se voir, soit en examinant les démonstrations, soit en remarquant que l'on peut associer canoniquement un A-module unitaire à tout groupe abélien à opérateurs par le procédé décrit dans Alg.II, § 7, n°9 (où l'on a d'ailleurs oublié de préciser que le A-module obtenu était unitaire !).

4. Commutant et bicommutant.

Soient E un groupe abélien, Ω l'anneau des endomorphismes de E . On sait que l'application $(u,x) \to u(x)$ de $\Omega \times E$ dans E définit sur E une structure de Ω-module unitaire à gauche. Si A est un anneau à élément unité, tout homomorphisme $\varphi : A \to \Omega$ définit donc sur E une structure de A-module à gauche, qui est unitaire si $\varphi(1)=1$. Réciproquement, il est clair que toute structure de A-module unitaire sur E définit un tel homomorphisme φ et un seul. On a :

$$(\varphi(a))(x) = a.x \quad , \quad a \in A \quad , \quad x \in E .$$

En particulier tout sous-anneau B de Ω , contenant 1 , définit sur E une structure de B-module unitaire.

DEFINITION 4. Soient E un A-module unitaire, $\varphi : A \to \Omega$ l'homomorphisme associé à E . On appelle commutant de A vis à vis de E (ou simplement commutant de A) l'ensemble A' des éléments de Ω qui commutent avec tous les éléments de $\varphi(A)$.

En d'autres termes, on a $u \in A' \iff (u(a.x) = a.u(x)$ quels que soient $a \in A$ et $x \in E)$; A' n'est autre que l'anneau des endomorphismes de E considéré comme A-module.

La définition précédente s'applique notamment lorsque A est un sous-anneau de Ω et que $\varphi : A \to \Omega$ est l'injection de A dans Ω . On peut donc l'appliquer à A' lui-même, et on obtient ainsi un sous-anneau A" de Ω , appelé bicommutant de A . Il est clair que $A'' \supset \varphi(A)$, mais, en général, on a $A'' \neq \varphi(A)$.

Remarques.

1. On a $(\varphi(A))' = A'$. On pourrait donc se borner à étudier les commutants des sous-anneaux de Ω . Cela reviendrait à n'envisager que des A-modules fidèles.
2. Si A est un sous-anneau de Ω , $A \cap A'$ est le centre de A et est contenu dans le centre de A'. En particulier, si A est commutatif, on a $A \subset A'$, d'où $A' \supset A''$, et A" est le centre de A' ; donc le bicommutant d'un anneau commutatif est commutatif.

PROPOSITION 5. Soit E un A-module unitaire dont le groupe abélien sous-jacent est somme directe d'une famille de sous-groupes E_λ . Soient p_λ les projecteurs attachés canoniquement à cette décomposition en somme directe. Les trois propriétés suivantes sont équivalentes :

(a) Les E_λ sont des sous-A-modules de E .

(b) Les projecteurs p_λ appartiennent au commutant A' de A .

(c) Les E_λ sont des sous-A"-modules de E , A" désignant le bicommutant de A .

(a) $\Rightarrow$ (b) résulte de Alg.II, § 1, prop.7 .

(b) $\Rightarrow$ (c) car si l'on a $b \in A''$, on a $b.p_\lambda = p_\lambda.b$ d'où

$b(E_\lambda) = b(p_\lambda(E)) = p_\lambda(b(E)) \subset p_\lambda(E) = E_\lambda$, ce qui montre bien que E_λ est stable par les opérations de A" .

(c) $\Rightarrow$ (a) car $A'' \supset A$.

Soit $E = \sum E_\lambda$ un A-module vérifiant les conditions (a), (b) et (c). Nous désignerons par A'_λ et A''_λ le commutant et le bicommutant de A vis à vis du A-module E_λ .

PROPOSITION 6. Soit E un A-module unitaire, somme directe de sous-modules E_λ . La restriction b_λ de tout élément $b \in A''$ à E_λ appartient à A''_λ .

Soit $u \in A'_\lambda$, et soit $\underline{u}$ l'endomorphisme de E qui est nul sur les E_μ , $\mu \neq \lambda$, et coïncide avec u sur E_λ . Il est clair que $\underline{u} \in A'$, et on a donc $\underline{u}.b = b.\underline{u}$, d'où pour tout $x_\lambda \in E_\lambda$, $u(b_\lambda(x_\lambda)) = b_\lambda(u(x_\lambda))$, ce qui montre que b_λ commute avec u , donc que l'on a bien $b_\lambda \in A''_\lambda$.

COROLLAIRE 1. Supposons que toute application A-linéaire de E_λ dans E_μ soit nulle quels que soient λ et μ avec $\lambda \neq \mu$. Pour qu'un endomorphisme b de E appartienne à A" , il faut et il suffit qu'il existe des éléments $b_\lambda \in A''_\lambda$ tels que $b(x_\lambda) = b_\lambda(x_\lambda)$ pour tout $x_\lambda \in E_\lambda$.

La nécessité a été démontrée dans la proposition précédente. Pour prouver la suffisance, remarquons d'abord que, d'après Alg.II, § 2 et 6, tout endomorphisme u de E est défini par une matrice $(u_{\lambda\mu})$, où $u_{\lambda\mu}$ est une application A-linéaire de E_λ dans E_μ . Vu l'hypothèse faite on a donc $u_{\lambda\mu} = 0$ si $\lambda \neq \mu$, ce qui signifie que les E_λ sont stables par tout $u \in A'$. Il est alors clair que tout endomorphisme de E de la forme : $(x_\lambda) \to (b_\lambda(x_\lambda))$, avec $b_\lambda \in A''$, commute aux éléments de A', ce qui démontre le corollaire.

COROLLAIRE 2. Supposons que tous les modules E_λ soient isomorphes à un même module F, et désignons par A'_F et A''_F le commutant et le bicommutant de A vis à vis de F. Pour qu'un endomorphisme b de E appartienne à A" il faut et il suffit qu'il existe un élément $b_F \in A''_F$ tel que $b(x_\lambda) = b_F(x_\lambda)$ pour tout $x_\lambda \in E_\lambda$ (identifié à F par abus de langage).

Comme précédemment, le commutant A' est formé des matrices $(u_{\lambda\mu})$ où $u_{\lambda\mu} \in A'_F$. Il s'ensuit d'abord que la condition de l'énoncé est suffisante (produits de matrices !). Montrons qu'elle est nécessaire. D'après la prop.6, tout $b \in A''$ est de la forme $(x_\lambda) \to (b_\lambda(x_\lambda))$ avec $b_\lambda \in A''_F$. Soit $c_{\mu\nu}$ l'endomorphisme de E défini par :

$(x_\lambda) \to (y_\lambda)$, avec $y_\lambda = 0$ si $\lambda \neq \mu$, $y_\mu = x_\nu$.

Si l'on écrit que b et $c_{\mu\nu}$ commutent, on obtient aussitôt que $b_\mu = b_\nu$, ce qui montre que tous les b_λ sont égaux, et achève la démonstration.

Remarques.

1. Les deux corollaires précédents déterminent les bicommutants de A dans les cas les plus importants. On remarquera que le cor.2 contient comme cas particulier la détermination du centre de l'anneau des endomorphismes d'un module libre, faite au Chap.II, § 2, n°5.
2. Le contenu de ce n° n'a aucune espèce de rapport avec les modules semi-simples ; le rédacteur l'a fourré là parce qu'il allait en avoir besoin, mais on pourrait tout aussi bien le mettre dans le Chap.II. Bourbaki demerdetur !

5. Commutant et bicommutant. Cas des modules semi-simples.

Nous allons appliquer aux modules semi-simples les résultats du n° précédent. Cette application est basée sur le résultat suivant :

THÉORÈME 1 (Lemme de Schur). Soient S et T deux modules simples. Toute application linéaire f de S dans T est, soit nulle, soit un isomorphisme de S sur T .

Soient N et I le noyau et l'image de f , respectivement. Puisque N est un sous-module du module simple S , on a N = (0) ou N = S . Dans le premier cas I est isomorphe à S , donc distinct de (0), et comme T est simple ceci entraîne I = T ; f est alors un isomorphisme de S sur T . Dans le second cas f est évidemment nulle.

COROLLAIRE. L'anneau des endomorphismes d'un module simple est un corps.

En effet, d'après le théorème précédent, tout élément de cet anneau est, soit nul, soit inversible.

Démontrons maintenant un résultat auxiliaire :

LEMME 1. Soit E un A-module semi-simple, b un élément du bicommutant A" de A vis à vis de E . Pour tout $x \in E$ il existe $a \in A$ tel que $a.x = b(x)$.

Soit V le sous-module A.x de E ; puisque E est semi-simple, V admet un supplémentaire et est donc stable par b , d'après la prop.5. Comme $x \in V$, on a aussi $b(x) \in V$, C.Q.F.D.

Nous allons généraliser le résultat précédent au cas de n éléments $x_1, \ldots, x_n$ de E :

THEOREME 2. (Théorème de densité). Soient E un A-module semi-simple et b un élément du bicommutant de A vis à vis de E . Pour toute suite finie x_i, $1 \leqslant i \leqslant n$, d'éléments de E il existe $a \in A$ tel que

$$a.x_i = b(x_i) \quad \text{pour} \quad 1 \leqslant i \leqslant n .$$

Soit E^n la somme directe de n modules isomorphes à E . L'élément b définit un endomorphisme b' de E^n par la formule :

$$b'(y_i) = (b(y_i)) \quad , \quad 1 \leqslant i \leqslant n \quad ,$$

et d'après le cor.2 à la prop.6 b' appartient au bicommutant de A vis à vis de E^n . Appliquant alors à E^n le lemme précédent on voit qu'il existe $a \in A$ tel que $a.x_i = b(x_i)$ pour $1 \leqslant i \leqslant n$, C.Q.F.D.

COROLLAIRE. Soient E un A-module simple, K le commutant de A vis à vis de E . Etant donnés n éléments $x_1,\dots,x_n$ de E , linéairement indépendants sur K , et n éléments arbitraires $y_1,\dots,y_n$ de E , il existe $a \in A$ tel que $a.x_i = y_i$ pour tout i .

Puisque le bicommutant de A est l'ensemble de tous les endomorphismes du K-espace vectoriel E , il existe un élément b de ce bicommutant tel que $b(x_i)=y_i$ pour tout i , d'où , d'après le th.2 un élément $a \in A$ tel que $a.x_i = y_i$ pour tout i .

Remarque.

Si l'on munit E de la topologie discrète et Ω de la topologie de la convergence simple, le th.2 exprime que $\varphi(A)$ est dense dans A", d'où le nom de "théorème de densité" (φ et Ω ayant le signification expliquée au n°4). On notera que A" est fermé dans Ω (car défini par des équations), donc que A" est l'adhérence de $\varphi(A)$ dans Ω .

Il faut se garder de croire que le théorème de densité soit spécial aux modules semi-simples. On a en effet le résultat suivant :

PROPOSITION 7. Soient A un anneau commutatif principal, et E un A-module de type fini. Le bicommutant A" de A vis à vis de E est égal à l'ensemble $\varphi(A)$ des homothéties de E .

On sait (Alg.VII, § 4, th.2) que E est somme directe de modules monogènes E_i , i=1,...,m , isomorphes à $A/\mathfrak{a}_i$ où les $\mathfrak{a}_i$ sont des idéaux de A tels que $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \dots \subset \mathfrak{a}_m$. On désignera par e_i un générateur de E_i ; $\mathfrak{a}_i$ est donc l'annulateur de e_i .

D'après la prop.5 tout élément $b \in A''$ laisse stable les E_i ; il existe donc des éléments $x_i \in A$, $i = 1,\dots,m$, tels que $b(e_i) = x_i \cdot e_i$ pour tout i . Comme b commute avec les homothéties, il s'ensuit que $b(e) = x_i \cdot e$ pour tout $e \in E_i$.

Soit maintenant C_i l'endomorphisme de E défini par :

$$C_i(e_1) = e_i \quad \text{et} \quad C_i(e_j) = 0 \quad \text{si} \quad j \neq 1 .$$

Cette définition est licite puisque $\mathfrak{a}_1 \subset \mathfrak{a}_i$. Si l'on écrit que b commute avec C_i ,on obtient :

$$C_i(b(e_1)) = C_i(x_1 \cdot e_1) = x_1 \cdot e_1 = b(C_i(e_1)) = b(e_i) = x_i \cdot e_i ,$$

d'où en comparant, $x_1 \equiv x_i \mod \mathfrak{a}_i$. Il en résulte immédiatement que b coïncide avec l'homothétie de rapport x_1 .

COROLLAIRE. Soient E un espace vectoriel de dimension finie sur un corps commutatif k , u un endomorphisme de E . Pour qu'un endomorphisme v commute avec tous les endomorphismes qui commutent avec u , il faut et il suffit que v soit un polynome en u .

Soit $A = k[X]$ l'anneau des polynomes sur k ; on munit E d'une structure de A-module en posant $P.e = P(u)(e)$ pour $P \in A$ (cf. Alg.VII, § 5,n°1), et l'on applique la prop.7 au module ainsi obtenu.

La prop.7 n'a évidemment rien à voir avec les anneaux primitifs, et elle ne sera pas utilisée dans la suite de la rédaction. Le rédacteur ne l'a fourrée ici que parce que son corollaire est utile dans les algèbres de Lie (théorie des héritiers).

§ 2. Radical. Représentations linéaires.

1. Définitions.

Soient A un anneau, E un A-module unitaire. Rappelons (Alg.II, § 1) que l'on appelle annulateur d'une partie D de E l'ensemble $\mathfrak{a}(D)$ des $a \in A$ tels que $a.x = 0$ pour tout $x \in D$. Lorsque D est réduit à un élément x, on écrit $\mathfrak{a}(x)$ au lieu de $\mathfrak{a}(\{x\})$.

Pour tout D, $\mathfrak{a}(D)$ est un idéal à gauche de A ; si D est un sous-module de E, $\mathfrak{a}(D)$ est un idéal bilatère de A. En particulier l'annulateur $\mathfrak{a}(E)$ de E lui-même est un idéal bilatère de A, qui n'est autre que le noyau de l'homomorphisme canonique $\varphi : A \longrightarrow \Omega$, Ω désignant, comme au § 1, l'anneau des endomorphismes du groupe abélien sous-jacent de E. Lorsque $\mathfrak{a}(E) = (0)$, le module E est dit fidèle. On observera que $\mathfrak{a}(E) = \bigcap_{x \in E} \mathfrak{a}(x)$.

Le but de ce paragraphe est d'étudier certains anneaux au moyen des modules sur ces anneaux.

DEFINITION 1. Un anneau A est dit primitif s'il existe un A-module simple et fidèle.

Un anneau A est dit semi-primitif s'il existe un A-module semi-simple et fidèle.

DEFINITION 2. On appelle radical d'un anneau A l'intersection des annulateurs de tous les A-modules simples.

PROPOSITION 1. Le radical d'un anneau A est le plus petit idéal bilatère $\mathfrak{a}$ tel que l'anneau quotient $A/\mathfrak{a}$ soit semi-primitif.

Soit $\mathfrak{r}$ le radical de A, intersection des annulateurs des A-modules simples E_λ ; il est clair que $E = \sum E_\lambda$ est un module semi-simple d'annulateur $\mathfrak{r}$, et peut donc être considéré comme un $A/\mathfrak{r}$-module semi-simple. Il s'ensuit que le quotient $A/\mathfrak{r}$ est un anneau semi-primitif.

Réciproquement, soit $\mathfrak{a}$ un idéal bilatère tel que $A/\mathfrak{a}$ soit un anneau semi-primitif, et soit $E = \sum E_\lambda$ un $A/\mathfrak{a}$ -module semi-simple et fidèle, somme directe de modules simples E_λ . On peut munir E d'une structure de A-module, et on aura alors $\mathfrak{a}(E) = \mathfrak{a}$. Mais on a $\mathfrak{a}(E) = \bigcap \mathfrak{a}(E_\lambda)$, et les E_λ sont des A-modules simples. D'après la définition du radical on a donc $\mathfrak{a} = \mathfrak{a}(E) \supset \mathfrak{r}$, C.Q.F.D.

COROLLAIRE. Pour qu'un anneau soit semi-primitif il faut et il suffit que son radical soit nul.

Exemples d'anneaux primitifs et semi-primitifs.

1. Soit A un anneau "simple", c'est-à-dire n'ayant pas d'autres idéaux bilatères que (0) et A ; si $\mathfrak{m}$ est un idéal à gauche maximal de A (un tel idéal existe d'après le th. de Krull), $E = A_s/\mathfrak{m}$ est un A-module simple (§ 1, prop.1) ; puisque l'annulateur de E est un idéal bilatère de A qui ne contient pas 1, il est réduit à (0) et E est un module fidèle. Il s'ensuit que tout anneau simple est primitif (et en particulier tout corps est primitif).

2. Si E est un espace vectoriel sur un corps K , l'anneau $\mathfrak{L}(E)$ des endomorphismes de E admet évidemment E comme module simple et fidèle (cf. § 1, n°1) ; ainsi $\mathfrak{L}(E)$ est un anneau primitif. On notera que, si E est de dimension infinie sur K , $\mathfrak{L}(E)$ n'est pas un anneau simple car l'ensemble des endomorphismes de rang fini de E forme un idéal bilatère de $\mathfrak{L}(E)$ distinct de (0) et de $\mathfrak{L}(E)$.

3. D'après le th. de densité (§ 1, th.2) tout anneau primitif est sous-anneau partout dense d'un anneau obtenu comme précédemment et réciproquement il est clair qu'un tel sous-anneau est primitif.

4. L'anneau Z des entiers est semi-primitif, car les Z-modules simples sont les groupes $Z/(p)$, p premier, et l'intersection de leurs annulateurs est (0).

Les propositions suivantes fournissent d'autres exemples d'anneaux semi-primitifs :

PROPOSITION 2. Tout produit direct d'anneaux semi-primitifs est semi-primitif.

Si les A_λ sont des anneaux semi-primitifs, de modules semi-simples et fidèles E_λ, la somme directe $E = \sum E_\lambda$ est un module semi-simple et fidèle sur l'anneau produit $\prod A_\lambda$, la structure de module étant définie par :

$$(a_\lambda).(x_\lambda) = (a_\lambda . x_\lambda) \quad , \qquad a_\lambda \in A_\lambda \quad , \quad x_\lambda \in E_\lambda \ .$$

Il s'ensuit que $\prod A_\lambda$ est un anneau semi-primitif.

PROPOSITION 3. Soit A un anneau primitif (resp. semi-primitif). L'anneau $M_n(A)$ des matrices carrées d'ordre n sur A est un anneau primitif (resp. semi-primitif).

Si E est un A-module, nous munirons E^n d'une structure de $M_n(A)$-module en posant $(a_{ij})(x_i) = (\sum_{j=1}^{j=n} a_{ij} . x_j)$. On a les propriétés suivantes :

a) Si E est fidèle, E^n est fidèle.

b) Si E est simple, E^n est simple.

Soient (x_i) et (y_i) deux éléments de E^n, le premier n'étant pas nul. Il existe donc un indice k tel que $x_k \neq 0$, et, puisque E est simple, il existe des $a_i \in A$, $i=1,\ldots,n$, tels que $a_i . x_k = y_i$. La matrice (a_{ij}) définie par : $a_{ij}=0$ si $j \neq k$, $a_{ik}=a_i$, est donc telle que $(a_{ij}).(x_i)=(y_i)$, ce qui prouve bien que E^n est simple.

c) Si E est semi-simple, E^n est semi-simple.

Si $E = \sum E_i$, où chaque E_i est simple, on a $E^n = \sum E_i^n$ et comme E_i^n est simple d'après b), E^n est bien semi-simple.

La prop.3 résulte évidemment de ces trois propriétés.

2. Détermination du radical.

Démontrons tout d'abord le résultat suivant :

PROPOSITION 4. Le radical $\mathscr{r}$ d'un anneau A est identique à l'intersection des idéaux à gauche maximaux de A .

Par définition, on a $\mathscr{r} = \bigcap \mathscr{a}(E_\lambda)$, où E_λ parcourt l'ensemble des A-modules simples (ce n'est d'ailleurs pas un ensemble ! cf. Livre I où le lecteur trouvera les formules d'exorcisation canoniques...). On a d'autre part $\mathscr{a}(E_\lambda) = \bigcap_{x \in E_\lambda} \mathscr{a}(x)$, et d'après la prop.1 du § 1, les $\mathscr{a}(x)$, $x \neq 0$, sont des idéaux à gauche maximaux de A et réciproquement tout idéal à gauche maximal de A est l'un des $\mathscr{a}(x)$. La proposition résulte immédiatement de là.

THÉORÈME 1. Soient A un anneau, $\mathscr{r}$ le radical de A . Pour qu'un élément $a \in A$ appartienne à $\mathscr{r}$, il faut et il suffit que pour tout $x \in A$ $1 - xa$ soit inversible à gauche dans A .

Soit $\{m_\iota\}$ l'ensemble des idéaux à gauche maximaux de A . D'après la prop.3, $a \in \mathscr{r} \iff a \in m_\iota$ quel que soit ι . Soit $\mathscr{a}$ l'idéal A.a . Les relations :

$a \in m_\iota$

$\mathscr{a} \subset m_\iota$

$\mathscr{a} + m_\iota = m_\iota$

$1 \notin \mathscr{a} + m_\iota$

$(1-\mathscr{a}) \cap m_\iota = \emptyset$

sont visiblement équivalentes (l'équivalence de la 3ème et de la 4ème résulte de ce que m_ι est maximal). Il s'ensuit que $a \in \mathscr{r}$ équivaut à ce que aucun élément de la forme $1-xa$, $x \in A$, ne soit contenu dans aucun idéal à gauche maximal m_ι ; d'après le th. de Krull,

ceci équivaut à dire que tout élément de la forme précédente est inversible à gauche, C.Q.F.D.

COROLLAIRE 1. Quels que soient $x \in A$ et $a \in \mathfrak{r}$, $1-xa$ et $1-ax$ sont inversibles.

Puisque $\mathfrak{r}$ est un idéal bilatère, il suffit de vérifier que pour tout $a \in \mathfrak{r}$, $1-a$ est inversible. D'après le th.1, $1-a$ a un inverse à gauche ; si on écrit un tel élément sous la forme $1-b$, il vient $-a-b+ba = 0$ d'où $b = ba-a$ et $b \in \mathfrak{r}$. Il s'ensuit en appliquant à nouveau le th.1 que $1-b$ est inversible à gauche, et comme il est inversible à droite, il est inversible et son inverse est $1-a$ qui est donc lui aussi inversible

COROLLAIRE 2. Le radical d'un anneau A est identique au radical de l'anneau opposé A^0.

Soient $\mathfrak{r}_1$ et $\mathfrak{r}_2$ le radical de A et de A^0 respectivement. Le th.1 joint au cor.1 montre que $\mathfrak{r}_1 \subset \mathfrak{r}_2$; en échangeant les rôles de A et de A^0 on obtient $\mathfrak{r}_2 \subset \mathfrak{r}_1$, d'où $\mathfrak{r}_1 = \mathfrak{r}_2$.

COROLLAIRE 3. Le radical d'un anneau A est identique à l'intersection des idéaux à droite maximaux de A.

Résulte immédiatement du cor.2 et de la prop.3.

Remarque. D'après le cor.2 ci-dessus, l'anneau opposé d'un anneau semi-primitif est semi-primitif. Par contre on ignore si l'anneau opposé d'un anneau primitif est primitif.

Exemples.

Le th.1 permet de déterminer le radical de nombreux anneaux. Par exemple, si l'on prend $A = K[[X_1,\dots,X_s]]$, algèbre des séries formelles en s indéterminées, on voit tout de suite (en utilisant la détermination des éléments inversibles de A faite dans Alg.IV, § 5) que $\mathfrak{r}$ est

l'ensemble des séries formelles sans terme constant. *Plus généralement, le radical d'un anneau local est évidemment l'unique idéal maximal de cet anneau .*

On voit de la même manière que le radical de l'algèbre de polynomes $K[X_1,\ldots,X_s]$ est réduit à (0). Il en est de même pour une algèbre extérieure, *ainsi que pour l'algèbre enveloppante d'une algèbre de Lie*.

3. Généralités sur les représentations linéaires.

Soient A une algèbre sur un corps K , E un espace vectoriel sur K , E un espace vectoriel sur K , $\mathcal{L}(E)$ l'algèbre des endomorphismes de E . On appelle représentation linéaire de A dans E tout homomorphisme M de l'algèbre A dans l'algèbre $\mathcal{L}(E)$ qui transforme l'élément unité de A en l'élément unité de $\mathcal{L}(E)$. On a donc :

$$M(1) = 1$$
$$M(x+y) = M(x) + M(y)$$
$$M(x.y) = M(x).M(y)$$
$$M(\lambda.x) = \lambda.M(x) \quad , \quad \lambda \in K \ .$$

Puisque $\mathcal{L}(E)$ est un sous-anneau de l'anneau Ω des endomorphismes du groupe abélien sous-jacent à E , toute représentation linéaire M de A dans E définit sur E une structure de A-module unitaire à gauche ; le produit d'un élément $a \in A$ et d'un élément $e \in E$ est alors par définition $M(a)(e)$.

Réciproquement, soit E un A-module (unitaire à gauche), et soit $\varphi : A \longrightarrow \Omega$, l'homomorphisme qui définit cette structure de A-module. Puisque A est une algèbre sur K et possède un élément unité, on peut identifier K à la sous-algèbre de A formée des multiples de l'élément unité 1 . Il s'ensuit que E est muni d'une structure d'espace vectoriel sur K .

Puisque les éléments de K commutent avec ceux de A , les éléments de $\varphi(A)$ commutent avec les homothéties de E , et sont donc des endomorphismes du K-espace vectoriel E . L'homomorphisme φ prend alors ses valeurs dans $\mathcal{L}(E)$ et définit donc une représentation linéaire de A dans E .

On voit ainsi qu'il y a une correspondance biunivoque entre les A-modules et les représentations linéaires de A . On peut donc traduire dans le langage des représentations linéaires les notions et résultats de la théorie des modules :

Une représentation linéaire est dite <u>irréductible</u> si le module associé est <u>simple</u>.

Une représentation linéaire est dite <u>complètement réductible</u> si le module associé est <u>semi-simple</u>.

On appelle <u>noyau</u> d'une représentation linéaire l'<u>annulateur</u> du modul associé ; c'est également le noyau de l'homomorphisme $M : A \longrightarrow \mathcal{L}(E)$.

Une représentation linéaire est dite <u>fidèle</u> si le module associé est <u>fidèle</u>, autrement dit si son noyau est réduit à (0).

Deux représentations linéaires sont dites <u>semblables</u> si les modules associés sont <u>isomorphes</u>. On dit aussi qu'elles appartiennent à la même <u>classe</u>.

Un cas particulier important de représentation linéaire est celui où $E = K^n$, $\mathcal{L}(E)$ étant alors l'algèbre des matrices carrées d'ordre n . Une telle représentation est dite <u>matricielle</u>. Toute représentation linéaire de A dans un espace E de dimension n sur K est évidemment semblable à une représentation matricielle ; n est dit le <u>degré</u> de la représentation. Pour que deux représentations

matricielles M et M' soient semblables il faut et il suffit qu'il existe une matrice inversible P telle que

$M'(x) = P.M(x).P^{-1}$.

4. Extension du corps de base dans les représentations linéaires.

Soient A une algèbre sur un corps K , E un espace vectoriel sur K , $M : A \to \mathcal{L}(E)$ une représentation linéaire de A dans E . D'autre part, soit L un corps commutatif, extension de K . On pose, comme d'ordinaire :

$$A_{(L)} = A \otimes L \quad , \quad E_{(L)} = E \otimes L \ ,$$

le produit tensoriel étant pris sur le corps K .

$A_{(L)}$ est une algèbre sur L , $E_{(L)}$ un espace vectoriel sur L . Nous allons définir une représentation $M_{(L)} : A_{(L)} \to \mathcal{L}(E_{(L)})$.

Soit $u \in \mathcal{L}(E)$ un K-endomorphisme de E ; u définit un L-endomorphisme $\overline{u}$ de $E_{(L)}$ par la formule :

$$\overline{u}(e \otimes \lambda) = u(e) \otimes \lambda \quad , \quad e \in E \quad , \quad \lambda \in L .$$

L'application $\psi : u \to \overline{u}$ est un homomorphisme de $\mathcal{L}(E)$ dans $\mathcal{L}(E_{(L)})$ (pour la structure de K-algèbres), et se prolonge donc de façon unique en un homomorphisme (de L-algèbres) :

$$\vartheta : \mathcal{L}(E) \otimes L \longrightarrow \mathcal{L}(E_{(L)}) .$$

De même, l'homomorphisme M se prolonge de façon unique en un L-homomorphisme $\overline{M} : A \otimes L \longrightarrow \mathcal{L}(E) \otimes L$. On peut alors poser :

DEFINITION 3. On appelle représentation obtenue à partir de M par extension à L du corps des scalaires la représentation :

$$M_{(L)} = \vartheta \circ \overline{M} .$$

On a donc par définition :

$$M_{(L)}(x \otimes \lambda)(e \otimes \mu) = M(x)(e) \otimes \lambda\mu \ , \quad x \in A, \ e \in E \ , \lambda, \mu \in L .$$

Remarque. Lorsque M est une représentation matricielle, il résulte de la formule précédente que la matrice $M_{(L)}(x \otimes \lambda)$ est le produit de la matrice $M(x)$ par la matrice diagonale dont les termes diagonaux sont tous égaux à λ. En particulier si l'on identifie A à un sous-anneau de $A \otimes L$ par l'application $x \to x \otimes 1$, on voit que la matrice $M_{(L)}(x)$, $x \in A$, est identique à la matrice $M(x)$.

PROPOSITION 5. Si $\mathfrak{a}$ est le noyau de la représentation M, le noyau de la représentation $M_{(L)}$ est $\mathfrak{a}_{(L)} = \mathfrak{a} \otimes L$.

Par définition, $M_{(L)}$ s'obtient par composition :

$$A \otimes L \xrightarrow{\overline{M}} \mathcal{L}(E) \otimes L \xrightarrow{\vartheta} \mathcal{L}(E_{(L)}) .$$

Il résulte immédiatement des propriétés du produit tensoriel de deux espaces vectoriels (voir Alg.III, ou Alg.II, 2ème éd.) que le noyau de $\overline{M}$ est $\mathfrak{a} \otimes L$. Notre proposition est donc une conséquence du lemme suivant :

LEMME 1. L'homomorphisme canonique $\vartheta : \mathcal{L}(E) \otimes L \to \mathcal{L}(E_{(L)})$ est biunivoque.

Soient $\{e_i\}_{i \in I}$ une base de E sur K, donc de $E_{(L)}$ sur L, et $\{\lambda_\alpha\}_{\alpha \in J}$ une base de L sur K. Soient $u^1, \ldots, u^k$ des éléments linéairement indépendants de $\mathcal{L}(E)$, $\mu^1, \ldots, \mu^k$ des éléments de L. Nous devons montrer que si $\mu^1 . \bar{u}^1 + \mu^2 . \bar{u}^2 + \ldots + \mu^k . \bar{u}^k = 0$, alors $\mu^1 = \ldots = \mu^k = 0$.

Soit (c^r_{ij}) la matrice (éventuellement infinie) de u^r relativement à $\{e_i\}$, et soit $\mu^r = \sum_\alpha \gamma^r_\alpha \lambda_\alpha$, $\gamma^r_\alpha \in K$, le développement de μ^r comme combinaison linéaire (à coefficients dans K) des λ_α. La matrice de $\mu^r . \bar{u}^r$ par rapport à la base $\{e_i\}$ de $E_{(L)}$ étant $(\mu^r . c^r_{ij})$, la relation $\sum_r \mu^r u^r = 0$ équivaut à $\sum_r \mu^r . c^r_{ij} = 0$ pour tout couple $i, j \in I$,

ou encore à $\sum_{r,\alpha} \gamma_\alpha^r . c_{ij}^r . \lambda_\alpha = 0$ pour tout couple $i,j \in I$.

Comme les λ_α sont linéairement indépendants sur K , cette dernière relation équivaut à $\sum_r \gamma_\alpha^r . c_{ij}^r = 0$ pour tout couple $i,j \in I$ et tout $\alpha \in J$, ou encore à :

$$\gamma_\alpha^1 . u^1 + \gamma_\alpha^2 . u^2 + \ldots + \gamma_\alpha^k . u^k = 0 \quad \text{pour tout} \quad \alpha \in J .$$

Puisque les u^r sont linéairement indépendants ceci entraîne $\gamma_\alpha^r = 0$ d'où $\mu^r = 0$, C.Q.F.D.

Note. Le rédacteur trouve scandaleux d'avoir à faire une pareille démonstration dans le Chap.X ou XI d'Algèbre ! Il propose un blâme et une réduction d'Armagnac à tous les salauds qui ont rédigé ou lu le chap.III, et l'ont ainsi réduit à cette triste nécessité.

Il profite également de l'occasion pour signaler qu'il a utilisé sans vergogne des matrices à une infinité de lignes et de colonnes espérant qu'elles ont été définies dans une édition ultérieure.

Nous allons maintenant étudier les rapports qui existent entre la complète réductibilité de M et celle de $M_{(L)}$.

PROPOSITION 6. (a) Si $M_{(L)}$ est irréductible, M est irréductible.
(b) Si $M_{(L)}$ est complètement réductible, M est complètement réductible.

Si $M_{(L)}$ est irréductible, on a $E_{(L)} \neq (0)$ d'où $E \neq (0)$. En outre si N est un sous-espace stable de E , $N_{(L)}$ est un sous-espace stable de $E_{(L)}$ et l'on a donc, soit $N_{(L)} = (0)$, soit $N_{(L)} = E_{(L)}$. Il en résulte que N est égal à (0) ou à E , ce qui démontre (a).

Pour prouver (b), soit N un sous-espace stable de E , et soit $F = E/N$ l'espace quotient qui est également un A-module. Soient $\{e_\lambda\}$ et $\{f_\mu\}$ une base de E et de F respectivement, et soit P la matrice de la projection canonique $p : E \to F$. D'après Alg.II, 2° éd., la recherche

d'un supplémentaire de N est équivalente à la recherche d'un A-homomorphisme $q : F \to E$ tel que $p \circ q = 1$. Si $\underline{Q}$ est la matrice de q , on doit donc avoir :

(1) $\underline{P}.\underline{Q} = \underline{I}$ ($\underline{I}$ étant la matrice unité)

(2) $\underline{M}(x).\underline{Q} = \underline{Q}.\underline{N}(x)$ ($\underline{M}(x)$ étant la matrice de l'opérateur $M(x)$, $x \in A$, et $\underline{N}(x)$ la matrice de l'opérateur de F déduit de $M(x)$ par passage au quotient) .

Réciproquement, toute matrice $\underline{Q}$ à coefficients dans K , dont chaque ligne ne comprend qu'un nombre fini de termes non nuls et qui vérifie (1) et (2), définit un supplémentaire de N .

Etendons maintenant le corps de base de K à L ; $N_{(L)}$ est encore un sous-espace stable de $E_{(L)}$, l'espace quotient étant canoniquement isomorphe à $F_{(L)}$. Puisque $E_{(L)}$ est complètement réductible, il existe un $A_{(L)}$-homomorphisme $q' : F_{(L)} \longrightarrow E_{(L)}$ tel que $p' \circ q' = 1$, p' désignant la projection canonique $E_{(L)} \longrightarrow F_{(L)}$. Il s'ensuit que la matrice $\underline{Q'}$ de q' est une matrice à coefficients dans L qui vérifie les équations (1) et (2). Or les équations en question sont des équations linéaires à coefficients dans K (les inconnues étant les coefficients de $\underline{Q}$) ; puisque ce système linéaire a une solution dans L (à savoir les coefficients de $\underline{Q'}$) il en a une dans K (Alg.II, § 5, Th.1), C.Q.F.D.

Note. Il y a ici un léger canular : le système linéaire en question n'est pas du type envisagé dans Alg.II . En effet les inconnues q_{ij} ; i fixé, sont assujetties à être nulles pour tout j sauf un nombre fini, et (grâce à cette restriction) chaque équation linéaire que doit satisfaire les q_{ij} a une infinité de termes. On vérifie cependant immédiatement que le Th.1 du § 5 s'applique encore (on peut par exemple ajouter des équations $q_{ij}=0$, et se ramener à un système du type usuel).

Conclusion pratique : soit mettre une remarque dans Alg.II, § 5 disant que le th. s'étend au cas étudié ici, soit remplacer la fin de la démonstration précédente par :

Variante. Soit $\psi : L \to K$ un projecteur de L, considéré comme K-espace vectoriel, sur K ; pour toute matrice $\underline{B}$ à coefficients dans L , désignons par $\psi(\underline{B})$ la matrice obtenue en appliquant l'opération ψ aux coefficients de $\underline{B}$. Si $\underline{C}$ est une matrice à coefficients dans K , on a évidemment $\psi(\underline{B}.\underline{C}) = \psi(\underline{B}).\underline{C}$ et $\psi(\underline{C}.\underline{B}) = \underline{C}.\psi(\underline{B})$. Posons alors $\underline{Q} = \psi(\underline{Q}')$; puisque $\underline{Q}'$ vérifie (1) et (2) il résulte des formules précédentes que $\underline{Q}$ les vérifie aussi, et comme les coefficients de $\underline{Q}$ appartiennent à K , la démonstration est achevée.

PROPOSITION 7. Si M est complètement réductible et de degré fini et si L est une extension algébrique séparable de K , $M_{(L)}$ est complètement réductible.

Soit L' une extension galoisienne de K contenant L . Puisque $M_{(L')}$ se déduit de $M_{(L)}$ par extension du corps de base à L', il suffit, d'après la prop.5, de prouver que $M_{(L')}$ est complètement réductible. En outre on peut évidemment supposer M irréductible.

Cela étant, soit G le groupe de Galois de L' sur K ; tout élément $\sigma \in G$ définit un automorphisme de $E_{(L')}$ que nous noterons encore σ , au moyen de la formule :

$$\sigma(\sum e_i \otimes \lambda_i) = \sum e_i \otimes \sigma(\lambda_i) \quad , \quad e_i \in E \quad , \quad \lambda_i \in L' \ .$$

Les automorphismes ainsi obtenus vérifient les propriétés suivantes :

(1) $\sigma(\lambda . e) = \sigma(\lambda).\sigma(e)$ si $\lambda \in L'$ et $e \in E_{(L')}$,

(2) $\sigma(\tau(e)) = \sigma\tau(e)$, si $\sigma , \tau \in G$, $e \in E_{(L')}$,

(3) $M_{L')}(x) \circ \sigma = \sigma \circ M_{(L')}(x)$ pour $x \in A$.

Ces définitions étant posées, soit V un sous-espace de $E_{(L')}$, stable par les opérations de A (donc de $A_{(L')}$), différent de (0), et de dimension minimum parmi tous ceux jouissant des propriétés précédentes. Un tel sous-espace existe, car $E_{(L')}$ est de dimension finie (nous supposons que $E \neq (0)$, ce qui est licite), et c'est évidemment un sous-module simple de $E_{(L')}$. Soit V^σ le sous-espace transformé de V par l'opération σ, $\sigma \in G$; il résulte de (1) que V^σ est un sous-espace vectoriel de $E_{(L')}$, et de (3) que V^σ est stable par les opérations $M_{(L')}(x)$, $x \in A$. Soit $W = \sum_{\sigma \in G} V^\sigma$ la somme des V^σ. Comme les V^σ sont simples, W est semi-simple, et, d'après (2), on a $W^\sigma = W$ pour tout $\sigma \in G$; soit $\{e_i\}$ une base de E sur K, donc aussi de $E_{(L')}$ sur L' ; d'après le cor. à la prop.10 d'Alg.II, § 5 le sous-corps de L' attaché à W relativement à la base $\{e_i\}$ est contenu dans l'ensemble des points fixes du groupe G, c'est-à-dire dans K. D'après le th.2 d'Alg.II, § 5, il s'ensuit que W est engendré (sur L') par son intersection avec E, et comme $W \cap E$ est un sous-espace stable de E, on a $W \cap E = (0)$, ou $W \cap E = E$; le premier cas conduit à $W = (0)$ ce qui est absurde, et le second cas à $W = E_{(L')}$, ce qui montre que $E_{(L')}$ est semi-simple.

Remarques. 1. Il ne faudrait pas croire que si M est irréductible, $M_{(L)}$ est irréductible.

2. Le rédacteur ignore si la proposition est vraie pour toute extension séparable (algèbrique ou pas) L de K ; si L est de type fini sur K c'est le cas, à cause de l'existence d'une base séparante.

3. Lorsque $[L:K] = 2$ (cas fréquent dans la pratique), l'hypothèse "M est de degré fini" est superflue, comme on le voit aussitôt. Le rédacteur ignore si ce résultat s'étend au cas où $[L:K] > 2$.

5. Effet d'une extension du corps de base sur le radical d'une algèbre.

(Dans ce n° nous notons $r(B)$ le radical d'un anneau B.)

Soient A une algèbre à élément unité sur un corps K, et L une extension de K. Nous nous proposons de comparer $r(A)$ et $r(A \otimes L)$.

THÉORÈME 2. *Si* $[L:K]$ *est fini,* $r(A) \otimes L \subset r(A \otimes L)$.

Nous démontrerons le résulta-t plus général suivant :

PROPOSITION 8. *Soient* A *et* B *deux algèbres à élément unité sur un corps* K. *Si* $[B:K]$ *est fini,* $r(A) \otimes B \subset r(A \otimes B)$.

Il est clair que $r(A) \otimes B$ est un idéal de $A \otimes B$; pour montrer qu'il est contenu dans $r(A \otimes B)$ il suffit, d'après le th.1, de prouver que $1-z$ est inversible à gauche pour tout $z \in r(A) \otimes B$.

Soit (ε_i), $1 \leqslant i \leqslant n$, une base de B sur K, avec $\varepsilon_i \cdot \varepsilon_j = \sum_{k=1}^{k=n} c_{ij}^k \varepsilon_k$, les c_{ij}^k étant des éléments de K (les "constantes de structure" de B). On a $z = \sum_{i=1}^{i=n} a_i \otimes \varepsilon_i$, $a_i \in r(A)$. Nous allons maintenant déterminer des éléments (x_i) de A, $1 \leqslant i \leqslant n$, tels que $1 - \sum_{i=1}^{i=n} x_i \otimes \varepsilon_i$ soit un inverse à gauche de $1-z$. Ceci conduit à l'équation :

$$\sum_i x_i \otimes \varepsilon_i + \sum_j a_j \otimes \varepsilon_j - \sum_{i,j} x_i \cdot a_j \otimes \varepsilon_i \cdot \varepsilon_j = 0 \text{ , ou encore :}$$

$$\sum_k (x_k + a_k - \sum_{i,j} c_{ij}^k \cdot x_i \cdot a_j) \otimes \varepsilon_k = 0 \text{ ,}$$

et comme les (ε_k), $1 \leqslant k \leqslant n$, forment une base de B sur K, l'équation précédente équivaut au système de n équations linéaires suivant :

$$x_k = -a_k + \sum_{i,j} c_{ij}^k \cdot x_i \cdot a_j \qquad (k = 1, \ldots, n) \text{ .}$$

Si nous montrons que ce système linéaire a une solution (x_k) la proposition sera démontrée. Or cela résulte du lemme plus général suivant :

LEMME 2. *Soit* A *un anneau à élément unité. Le système linéaire :*

$$x_k = u_k + \sum_{i=1}^{i=n} x_i \cdot v_k^i \qquad (k = 1, \ldots, n) \text{ , } u_k \in A \text{ ,}$$

a une solution $(x_1,\dots,x_n)$ avec $x_k \in A$ si tous les v_k^i appartiennent à $r(A)$.

On raisonne par récurrence sur n , nombre d'inconnues et d'équations du système. Si $n=1$, on a $x_1 = u_1 + x_1 \cdot v_1^1$, et puisque $v_1^1 \in r(A)$, $1-v_1^1$ est inversible (th.1) et on trouve $x_1 = u_1 \cdot (1-v_1^1)^{-1}$.

Si $n>1$, on tire x_1 de la première équation. Cela donne :

$$x_1 = u_1 \cdot (1-v_1^1)^{-1} + \sum_{i=2}^{i=n} x_i \cdot v_1^i \cdot (1-v_1^1)^{-1} ,$$

et en portant cette valeur dans les (n-1) équations restantes on trouve un système linéaire du même type, système qui est résoluble d'après l'hypothèse de récurrence.

La démonstration de la proposition 7 est donc achevée.

Remarques.

1. La conclusion du th.2 ne subsiste pas nécessairement si on ne fait pas de restriction sur $[L:K]$. Cf. Exerc.1 .

2. La démonstration du Lemme 2 montre en fait ceci : si V est une matrice carrée à coefficients dans $r(A)$, la matrice $I-V$ est inversible. Cf.Exer.2 .

Soit maintenant L un corps gauche contenant le corps K dans son centre. Nous dirons que L est une extension galoisienne de K s'il existe un groupe G d'automorphismes de L dont l'ensemble des points fixes soit K . Cette définition est une généralisation de celle introduite dans Alg.V, § 10, pour les corps commutatifs. On notera que tout corps gauche est extension galoisienne de son centre, le groupe G étant le groupe des automorphismes intérieurs.

THÉORÈME 3. Si L est une extension galoisienne (commutative ou non) de K , $r(A \otimes L)$ est engendré (en tant qu'espace vectoriel à droite sur L) par son intersection avec A .

Soit G le groupe des automorphismes de L laissant les éléments de K invariants ; tout élément $\sigma \in G$ s'étend en un automorphisme σ de $A \otimes L$ par la formule $\sigma(a \otimes \lambda) = a \otimes \sigma(\lambda)$, $a \in A, \lambda \in L$. Il est clair que l'on a $\sigma(r(A \otimes L)) = r(A \otimes L)$ pour tout $\sigma \in G$ (transfert de structure !). Le raisonnement fait plus haut (dans la démonstration de la prop.6) s'applique alors, et montre que $r(A \otimes L)$ est engendré par son intersection avec A .

Le fait que $r(A \otimes L)$ soit engendré par son intersection avec A peut s'exprimer par la formule :

$$r(A \otimes L) = (r(A \otimes L) \cap A) \otimes L .$$

THÉORÈME 4. Soient A une algèbre à élément unité sur un corps commutatif K et L une extension galoisienne finie (commutative ou non) de K . On a $r(A \otimes L) = r(A) \otimes L$.

D'après ce qui précède il nous suffit de montrer que $r(A \otimes L) \cap A = r(A)$ Comme $r(A) \subset r(A \otimes L)$ d'après la prop.7, tout revient à prouver que $r(A \otimes L) \cap A \subset r(A)$.

Soit donc $x \in A \cap r(A \otimes L)$; nous devons montrer que $1-ax$ est inversible à gauche dans A pour tout $a \in A$; puisque $x \in r(A \otimes L)$ il existe $y \in A \otimes L$ tel que $y.(1-ax)=1$. Si ψ est un projecteur de L , considéré comme K-espace vectoriel, sur K , étendons ψ à $A \otimes L$ en posant $\psi(t \otimes \lambda) = t \otimes \psi(\lambda) = \psi(\lambda).t$, $t \in A$, $\lambda \in L$. On vérifie immédiatement que $\psi(t.b) = \psi(t).b$ si $t \in A \otimes L$ et $b \in A$, et que $\psi(b) = b$ si $b \in A$. Appliquant alors ψ à l'équation $y.(1-ax)=1$, on trouve $\psi(y).(1-ax)=1$, et comme $\psi(y) \in A$, ceci montre que $1-ax$ est inversible à gauche dans A et achève la démonstration.

COROLLAIRE. Si L est une extension commutative finie et séparable du corps K , on a $r(A \otimes L) = r(A) \otimes L$.

Soit M une extension galoisienne de K contenant L . Nous conviendrons, pour éviter toute confusion, de noter $\otimes_K$ un produit tensoriel pris sur K , et $\otimes_L$ un produit tensoriel pris sur L . On a :

$r(A \otimes_K M) = r(A) \otimes_K M$ d'après le th.4, ce qui peut encore s'écrire :

$r(A \otimes_K M) = (r(A) \otimes_K L) \otimes_L M$ d'après la transitivité de l'opération d'extension du corps de base (cf.Alg.III, § 3,n°4).

Soit d'autre part $B = A \otimes_K L$; comme M est une extension galoisienne de L , on peut appliquer à B et à l'extension M/L le th.4 ; cela donne : $r(B \otimes_L M) = r(B) \otimes_L M$. Mais $B \otimes_L M = (A \otimes_K L) \otimes_L M = A \otimes_K M$. Comparant alors les deux expressions obtenues pour $r(A \otimes_K M)$ on voit que :

$$r(A \otimes_K M) = (r(A) \otimes_K L) \otimes_L M = (r(A \otimes_K L)) \otimes_L M .$$

Il s'ensuit que $r(A) \otimes_K L$ et $r(A \otimes_K L)$ sont deux sous-espaces vectoriels de $A \otimes_K L$ qui deviennent égaux par extension du corps de base à M . Ils sont donc égaux, C.Q.F.D.

Exercices à ajouter à ceux de l'Etat 2 .

(Les exercices 2 à 6 sont empruntés à un cours de Jacobson à Paris).

1. Soit A une algèbre à élément unité sur un corps K , et soit $L = K(t)$, t étant une indéterminée.

a). Soit $x \in r(A)$ et $y = 1-x \otimes t \in A \otimes L$. Montrer que, pour que y soit inversible dans $A \otimes L$, il faut et il suffit que x soit algébrique sur K .

b). Tirer de là un exemple où $r(A)$ n'est pas contenu dans $r(A \otimes L)$. (On prendra $A = K[[X]]$, et on appliquera a) à $x = X$) .

2. Soit A un anneau, A_n l'anneau des matrices d'ordre n à coefficients dans A . Montrer que $r(A_n)=(r(A))_n$ (utiliser le lemme 2 et la prop.3).

En particulier, l'anneau des matrices à coefficients entiers est semi-primitif.

3. *Soit A un anneau sans nilidéal $\neq (0)$. Montrer que $A[X]$ est semi-primitif (Amitsur).*

4. Montrer que l'algèbre engendrée par deux éléments u,v vérifiant la seule relation $u.v = 1$ est primitive.

5. Montrer que l'algèbre engendrée par deux éléments u,v vérifiant la seule relation $u.v-v.u = u$ *(alg. enveloppante de l'algèbre de Lie du groupe $x \longrightarrow ax+b$)* est primitive.

6. Soit G un groupe abélien sans torsion et $K^{(G)}$ l'algèbre du groupe G sur un corps commutatif K . Montrer que $K^{(G)}$ est semi-primitive (on commencera par munir G d'une structure d'ordre total compatible avec sa structure de groupe - cf. Alg. VI, § 1, Exerc. 20).

Généraliser, si possible, au cas d'un groupe non abélien.

7. Montrer que le corollaire du th.4 est valable lorsqu'on suppose que L est une extension algébrique séparable (finie ou non) de K .

8. Montrer que l'exercice 14 de l'Etat 2bis est faux.

9. Soient A et B deux algèbres sur un corps k . Montrer que $\mathscr{R}(A \otimes B) \cap A \subset \mathscr{R}(A)$. (Utiliser un projecteur k-linéaire de B sur k).

§ 3. Anneaux d'Artin.

1. Anneaux d'Artin.

DÉFINITION 1. Un anneau A est appelé anneau d'Artin (à gauche) s'il vérifie les deux conditions équivalentes suivantes :

(A) - Tout ensemble non vide d'idéaux à gauche de A, ordonné par inclusion, possède un élément minimal.

(A') - Si $(\mathfrak{a}_n)$ est une suite décroissante d'idéaux à gauche de A, il existe un entier i tel que $\mathfrak{a}_n = \mathfrak{a}_i$ pour tout $n \geqslant i$ (autrement dit, la suite des $\mathfrak{a}_n$ est stationnaire, au sens de Ens.III, § 6, déf.1).

L'équivalence des conditions (A) et (A') résulte de la prop.4 de Ens.III, § 6.

Exemples. 1. Tout anneau fini est un anneau d'Artin.

2. Toute algèbre de dimension finie sur un corps commutatif k est un anneau d'Artin, car tout idéal de A est un sous-espace vectoriel.

3. Plus généralement, tout anneau contenant un corps k (commutatif ou non) et de dimension finie (à gauche) sur k, est un anneau d'Artin.

4. L'anneau Z des entiers n'est pas un anneau d'Artin.

PROPOSITION 1. Soient A un anneau et $\mathfrak{m}$ un idéal bilatère de A. Si A est un anneau d'Artin, l'anneau quotient $A/\mathfrak{m}$ est un anneau d'Artin. Réciproquement, si $A/\mathfrak{m}$ est un anneau d'Artin, et si toute suite décroissante d'idéaux à gauche de A contenus dans $\mathfrak{m}$ est stationnaire, A est un anneau d'Artin.

La première partie de la proposition résulte de ce que les idéaux à gauche de $A/\mathfrak{m}$ correspondent biunivoquement aux idéaux à gauche de A contenant $\mathfrak{m}$.

Pour démontrer la seconde partie, considérons une suite décroissante $(\mathfrak{a}_n)$ d'Idéaux à gauche de A , et posons $\mathfrak{b}_n = \mathfrak{a}_n \cap \mathfrak{m}$ ainsi que $\mathfrak{x}_n = \mathfrak{a}_n + \mathfrak{m}$. Les $\mathfrak{b}_n$ sont contenus dans $\mathfrak{m}$, et les $\mathfrak{x}_n$ correspondent biunivoquement à des idéaux de $A/\mathfrak{m}$. D'après les hypothèses faites, il existe donc un entier i tel que $\mathfrak{b}_n = \mathfrak{b}_i$ et $\mathfrak{x}_n = \mathfrak{x}_i$ pour tout $n \geqslant i$.

On a alors :

$$(0) = \mathfrak{b}_i / \mathfrak{b}_n = (\mathfrak{a}_i + \mathfrak{m})/(\mathfrak{a}_n + \mathfrak{m}) = \mathfrak{a}_i/(\mathfrak{a}_n + \mathfrak{a}_i \cap \mathfrak{m}) = \mathfrak{a}_i/(\mathfrak{a}_n + \mathfrak{a}_n \cap \mathfrak{m}) = \mathfrak{a}_i/\mathfrak{a}_n$$

ce qui montre bien que $\mathfrak{a}_n = \mathfrak{a}_i$ pour $n \geqslant i$.

COROLLAIRE. Tout produit direct d'un nombre fini d'anneaux d'Artin est un anneau d'Artin.

Il suffit de prouver que si B et C sont deux anneaux d'Artin, $A = B \times C$ est un anneau d'Artin. Or cela résulte de la proposition précédente si l'on pose $\mathfrak{m} = B \times \{0\}$, et si l'on remarque que $A/\mathfrak{m}$ est isomorphe à C .

2 Par contre un sous-anneau d'un anneau d'Artin n'est pas nécessairement un anneau d'Artin.

2. Le radical d'un anneau d'Artin.

Soit A un anneau et soient B et C deux parties de A . Rappelons (Alg...) que l'on note B.C le sous-groupe additif de A engendré par les produits $b.c$, où b parcourt B et c parcourt C . Si B (resp.C) est un idéal à gauche (resp. à droite), B.C est un idéal à gauche (resp. à droite). En particulier, le produit B.C de deux idéaux bilatères B et C est un idéal bilatère.

Si b est un idéal, nous noterons b^n le produit de n idéaux égaux à b . S'il existe un entier n 0 tel que $b^n=(0)$, on dit que b est un idéal nilpotent. Pour tout $x \in b$, on a alors $x^n=0$, ce qui montre que tous les éléments de b sont nilpotents. En général, cette dernière propriété ne suffit pas à caractériser les idéaux nilpotents. On a cependant :

PROPOSITION 2. Soient A un anneau d'Artin à gauche, b un idéal à gauche de A dont tous les éléments soient nilpotents. Alors b est nilpotent.

La suite des idéaux (b^n) étant décroissante, il existe un entier i tel que $b^n = b^i$ pour tout $n \geqslant i$. Posons $c = b^i$; il nous faut montrer que $c=(0)$. Pour cela, raisonnons par l'absurde et supposons $c \neq (0)$. Soit Φ la famille des idéaux à gauche d tels que $d \subset c$ et que $c.d \neq (0)$; Φ n'est pas vide car $c^2 = c \neq (0)$; soit d un élément minimal de Φ ; puisque $c.d \neq (0)$ il existe $x \in d$ avec $c.x \neq (0)$; la relation $c^2.x = c.x \neq (0)$ montre que l'idéal à gauche c.x appartient à Φ , et comme $c.x \subset d$, on a $c.x = d$. Il existe donc $y \in c$ tel que $y.x = x$, d'où $x = y.x = y^2.x = \ldots = y^n.x$. D'après l'hypothèse faite sur c on a $y^n=0$ pour n assez grand, d'où $x=0$, ce qui contredit la relation $c.x \neq (0)$ et achève la démonstration.

THEOREME 1. 1) Dans un anneau quelconque, tout idéal (à gauche ou à droite) dont tous les éléments sont nilpotents est contenu dans le radical.

2) Dans un anneau d'Artin, le radical est un idéal nilpotent (c'est donc le plus grand idéal nilpotent).

Soit $\mathfrak{a}$ un idéal à gauche d'un anneau A ; si tous les éléments de $\mathfrak{a}$ sont nilpotents, il existe pour tout $x \in A$ et tout $a \in \mathfrak{a}$ un entier n tel que $(x.a)^n=0$, et $1-x.a$ admet pour inverse l'élément $1 + x.a + (x.a)^2 + \ldots + (x.a)^{n-1}$, comme on le vérifie aussitôt.

D'après le th.1 du § 2, ceci entraîne que a est contenu dans le radical de A , ce qui démontre 1).

Soit maintenant A un anneau d'Artin et soit r le radical de A . Pour montrer que r est nilpotent, il suffit, d'après la prop.2, de montrer que tout élément $a \in r$ est nilpotent. La suite d'idéaux à gauche $(A.a^n)$ étant décroissante, il existe $n > 0$ tel que $A.a^{n+1} = A.a^n$; il existe donc $x \in A$ tel que $x.a^{n+1} = a^n$, d'où $(1-x.a).a^n=0$, et comme $1-x.a$ est inversible (§ 2,th.1), on a bien $a^n=0$.

COROLLAIRE. Dans un anneau d'Artin commutatif A , le radical est identique à l'ensemble de tous les éléments nilpotents.

Soit r l'ensemble des éléments nilpotents de A . Si $a \in r$ et $x \in A$, il existe un entier $n > 0$ tel que $a^n = 0$, d'où $(x.a)^n = x^n.a^n = 0$, ce qui montre que $x.a \in r$; si a et b sont deux éléments de r , il existe un entier $n > 0$ tel que $a^n=b^n=0$, d'où $(a+b)^{2n-1} = 0$ d'après la formule du binôme, et $(a+b) \in r$. Ainsi r est un idéal de A .

Si r' désigne le radical de A ; on a donc $r \subset r'$ d'après la première partie du th.1, et $r' \subset r$ d'après la seconde partie. D'où $r=r'$, C.Q.F.D.

3. Anneaux d'Artin primitifs.

THEOREME 2. Si A est un anneau d'Artin, les propriétés suivantes sont équivalentes :

1) A est un anneau primitif.

2) A est isomorphe à l'anneau des endomorphismes d'un espace vectoriel de dimension finie.

3) A est isomorphe à un anneau de matrices $M_n(K)$ sur un corps K .

4) A est un anneau simple.

Montrons que 1) $\Rightarrow$ 2). Soit E un A-module simple et fidèle, K^0 le commutant de A vis à vis de E . D'après le § 1, th. 1, cor. , K^0 est un corps (commutattf ou non), et E est un espace vectoriel à gauche sur K^0. Montrons d'abord que E est de dimension finie sur K^0. Sinon, il existerait une suite d'éléments $(x_1,\dots,x_n,\dots)$ de E , linéairement indépendants sur K^0, et d'après le cor. au th. de densité, il existerait pour tout n un élément $a_n \in A$ tel que $a_n \cdot x_i = 0$ pour $i \leqslant n$, et $a_n \cdot x_{n+1} \neq 0$; si l'on désigne par $\mathfrak{a}_n$ l'ensemble des éléments $a \in A$ tels que $a.x_i = 0$ pour $i \leqslant n$, on aurait donc $a_n \in \mathfrak{a}_n$ et $a_n \notin \mathfrak{a}_{n+1}$, d'où $\mathfrak{a}_n \neq \mathfrak{a}_{n+1}$ pour tout n . La suite des $\mathfrak{a}_n$ serait alors une suite strictement décroissante d'idéaux à gauche de A , ce qui est impossible puisque A est un anneau d'Artin. Ainsi E est de dimension finie sur K^0, et le théorème de densité montre que A est identique à l'anneau de tous les endomorphismes de E , considéré comme espace vectoriel sur K^0.

On sait (Alg. II, § 6) que 2) $\Rightarrow$ 3). Plus précisément, si l'espace vectoriel E est de dimension n sur K^0, alors A est isomorphe à $\underline{M}_n(K)$ où K désigne le corps gauche opposé du corps K^0.

Montrons que 3) $\Rightarrow$ 4) . Soit (E_{ij}) la base canonique de $\underline{M}_n(K)$, considéré comme espace vectoriel sur K (à droite ou à gauche). Si $\mathfrak{m}$ est un idéal bilatère non réduit à (0) de $\underline{M}_n(K)$, choisissons un élément non nul $x = \sum x_{ij}E_{ij}$ de $\mathfrak{m}$; il existe donc un couple d'entiers (i,j) tel que $x_{ij} \neq 0$; si (k,m) est un couple d'entiers arbitraire, l'élément $E_{ki}.x.E_{jm}$ appartient à $\mathfrak{m}$; d'après la table de multiplication des (E_{ij}) cet élément est égal à $x_{ij}.E_{km}$, d'où , puisque $x_{ij} \neq 0$, $E_{km} \in \mathfrak{m}$, et, ceci ayant lieu quels que soient k et m , on a $\mathfrak{m} = \underline{M}_n(K)$ ce qui prouve bien que $\underline{M}_n(K)$ est simple.

Enfin, l'implication 4) $\Rightarrow$ 1) a été démontrée au n°1 du § 2 .

COROLLAIRE 1. Le centre d'un anneau d'Artin simple est un corps.

En effet, on sait que le centre de $M_n(K)$ est isomorphe au centre de K (Alg.II, § 2, prop.5, cor.1) qui est un corps (Alg.I, § 9, prop.1, cor.).

COROLLAIRE 2. L'anneau opposé d'un anneau d'Artin simple est un anneau d'Artin simple.

En effet, si A est isomorphe à l'anneau des endomorphismes d'un espace vectoriel E de dimension finie, l'anneau opposé A^0 est isomorphe à l'anneau des endomorphismes du dual E^* de E et est donc un anneau d'Artin simple.

4. Anneaux d'Artin semi-primitifs.

Si E est un A-module, rappelons que $\mathfrak{a}(E)$ désigne l'annulateur de E , c'est-à-dire l'ensemble des $a \in A$ tels que $a.x = 0$ pour tout $x \in E$. L'annulateur $\mathfrak{a}(E)$ est un idéal bilatère de A .

LEMME 1. Si A est un anneau d'Artin semi-primitif, il existe une famille finie de A-modules simples E_i telle que $\bigcap \mathfrak{a}(E_i) = (0)$.

Puisque A est semi-primitif, il existe une famille (finie ou infinie) de A-modules simples E_i , $i \in L$, telle que $\bigcap_{i \in L} \mathfrak{a}(E_i) = (0)$. Pour toute partie finie $J \subset L$, posons $\mathfrak{a}_J = \bigcap_{i \in J} \mathfrak{a}(E_i)$. D'après l'axiome (A) la famille des $\mathfrak{a}_J$ possède un élément minimal, soit $\mathfrak{a}_I$; comme la famille des $\mathfrak{a}_J$ est filtrante décroissante, $\mathfrak{a}_I$ est égal à l'intersection de tous les $\mathfrak{a}_J$, c'est-à-dire à (0), ce qui démontre le lemme.

THEOREME 3. Si A est un anneau d'Artin, les propriétés suivantes sont équivalentes :

1) A est un anneau semi-primitif.

2) A est produit direct d'anneaux simples en nombre fini.

2) $\Rightarrow$ 1) car si un anneau d'Artin A est produit direct d'anneaux simples A_i , chaque A_i est un anneau d'Artin (prop.1) donc est un anneau primitif d'après le th.2, et A est semi-primitif d'après la prop.2 du §2.

Montrons que 1) $\Rightarrow$ 2). D'après le lemme 1 il existe une famille finie de A-modules simples E_i telle que, si l'on pose $r_i = \mathfrak{a}(E_i)$, on ait $\bigcap r_i = (0)$. On peut évidemment supposer que les r_i sont tous distincts, auquel cas les modules E_i ne sont pas isomorphes, puisqu'ils ont des annulateurs distincts. Formons le module E somme directe des E_i . C'est un A-module semi-simple et fidèle. D'après le cor.1 à la prop.6 du §1 (qui s'applique, grâce au lemme de Schur), le bicommutant A" de A vis à vis de E est isomorphe au produit direct des bicommutants A_i'' de A vis à vis des E_i . Soit $A_i = A/r_i$; E_i est un A_i-module simple et fidèle, et comme A_i est un anneau d'Artin, il résulte de la démonstration du th.2 que $A_i = A_i''$ et que E_i est de dimension finie sur le corps K_i^0 , commutant de A_i vis à vis de E_i . Puisque les E_i sont en nombre fini, E , considéré comme module sur le commutant A' de A vis à vis de E , est engendré par un nombre fini d'éléments (x_α) ; il suit de là que $A = A''$. En effet, pour tout $b \in A''$ il existe $a \in A$, d'après le th. de densité, tel que $a.x_\alpha = b(x_\alpha)$ pour tout α , d'où $a.(\sum v_\alpha(x_\alpha)) = b(\sum v_\alpha(x_\alpha))$ lorsque $v_\alpha \in A'$, et puisque les (x_α) engendrent E , on a $a.x = b(x)$ pour tout $x \in E$, d'où $a = b$, et $A = A''$. Comme $A'' = \prod A_i'' = \prod A_i$, et que chaque A_i est un anneau d'Artin primitif, ceci achève la démonstration.

Un anneau qui vérifie la propriété 2) du th.3 est dit semi-simple. Ainsi, pour qu'un anneau d'Artin soit semi-simple, il faut et il suffit qu'il soit semi-primitif. On notera que si $A = \prod A_i$, où les A_i sont simples, tout idéal bilatère de A est produit d'une sous-famille des A_i ,

d'après Alg.I, § 8, prop.6 ; en particulier les A_i sont déterminés de façon unique par A (à une permutation des indices près) : ce sont les idéaux bilatères non nuls minimaux de A .

COROLLAIRE 1. Soit $A = \prod A_i$ un anneau d'Artin semi-simple, produit direct d'anneaux simples A_i . Le centre C de A est le produit direct des centres C_i des A_i (qui sont des corps commutatifs d'après le corollaire au th.2).

En effet, il est immédiat que le centre d'un produit direct d'anneaux est le produit direct des centres de ces anneaux.

COROLLAIRE 2. Un anneau d'Artin commutatif semi-simple est produit direct d'un nombre fini de corps commutatifs.

C'est un cas particulier du corollaire 1 .

5. Modules sur un anneau d'Artin simple.

Soit A un anneau d'Artin simple, isomorphe à l'anneau des endomorphismes d'un espace vectoriel E de dimension finie n sur un corps K^o . Nous allons étudier la structure des A-modules à gauche. Remarquons que parmi ces modules figurent E et A_s .

THÉORÈME 4. 1) A_s est un A-module semi-simple, somme directe de n sous-modules isomorphes à E .

2) Tout A-module est semi-simple.

3) Tout A-module simple est isomorphe à E .

Etudions d'abord A_s . Soit $e_1, \ldots, e_n$ une base de E sur K^o, et soit $\mathfrak{a}_i$ $(1 \leqslant i \leqslant n)$ l'idéal à gauche des $a \in A$ tels que $a(e_j)=0$ pour $j \neq i$; l'application $a \to a(e_i)$ est une application biunivoque de $\mathfrak{a}_i$ sur E , et est un homomorphisme pour les structures de A-modules de $\mathfrak{a}_i$ et de E . Il s'ensuit que $\mathfrak{a}_i$, en tant que A-module, est isomorphe à E , et comme A est somme directe des $\mathfrak{a}_i$ pour $1 \leqslant i \leqslant n$, la partie 1) est démon-trée.

Considérons maintenant un A-module monogène M ; un tel module est isomorphe à un module quotient de A_s , donc à un sous-module de A_s puisque A_s est semi-simple ; comme A_s est somme directe de n modules isomorphes à E , il s'ensuit que M est somme directe d'un certain nombre (inférieur à n) de modules isomorphes à E. En particulier, si M est simple il est isomorphe à E , ce qui démontre 3). D'autre part, tout module étant somme de sous-modules monogènes est somme de sous-modules semi-simples, donc est semi-simple d'après la prop.2 du § 1, ce qui démontre 2).

COROLLAIRE. Si A est un anneau d'Artin simple, deux A-modules simples sont isomorphes.

6. Modules sur un anneau d'Artin semi-simple.

Soit A un anneau d'Artin semi-simple. D'après le th.3 A est isomorphe à $\prod_i A_i$, où chaque A_i est un anneau simple. Pour tout i, désignons par E_i un A_i-module simple (le th.4 montre qu'un tel module est bien déterminé, à un isomorphisme près) ; la projection canonique $A \longrightarrow A_i$ munit E_i d'une structure de A-module simple dont l'annulateur est $\prod_{j \neq i} A_j$. Les E_i sont donc des A-modules non isomorphes.

THÉORÈME 5. 1) Tout A-module est semi-simple.

2) Tout A-module simple est isomorphe à l'un des E_i .

Identifions A_i à un idéal bilatère de $A = \prod A_i$ comme il est dit dans Alg.I, § 8 . Le module A_s est somme directe des sous-A-modules A_i, et, d'après le th.4, chaque module A_i est somme directe de sous-modules simples tous isomorphes à E_i (en tant que A_i-modules, donc aussi en tant que A-module). Ceci démontre que A_s est semi-simple. On en déduit 1) et 2) par un raisonnement tout analogue à celui du th.4 .

COROLLAIRE. Soient A un anneau d'Artin semi-simple, $\mathfrak{a}$ un idéal à gauche de A . Il existe deux éléments e,e' de A tels que $\mathfrak{a} = A.e$, que l'idéal $\mathfrak{a}' = A.e'$ soit un supplémentaire de $\mathfrak{a}$ dans A , et que :

$$e^2 = e \ , \quad e'^2 = e' \ , \quad ee' = e'e = 0 \ , \quad e+e' = 1 \ .$$

Puisque A_s est un A-module semi-simple, il existe un idéal à gauche $\mathfrak{a}'$ supplémentaire de $\mathfrak{a}$ dans A . Soit $1 = e+e'$ la décomposition de l'élément unité 1 suivant $\mathfrak{a}$ et $\mathfrak{a}'$. Si $x \in A$, on a $x = x.e + x.e'$ et comme $x.e \in \mathfrak{a}$ et $x.e' \in \mathfrak{a}'$, on en conclut que x.e et x.e' sont les composants de x dans $\mathfrak{a}$ et dans $\mathfrak{a}'$ respectivement. D'où $\mathfrak{a} = A.e$, $\mathfrak{a}' = A.e'$, ainsi que les relations $e^2 = e$, ... etc.

Réciproquement :

PROPOSITION 3. Soit A un anneau tel que le A-module A_s soit semi-simple. Alors A est un anneau d'Artin semi-simple.

Soit $A_s = \sum_{i \in I} \mathfrak{a}_i$ une décomposition de A_s en somme de A-modules simples. Chaque $\mathfrak{a}_i$ est donc un idéal à gauche $\neq (0)$ de A . Montrons d'abord que l'ensemble d'indices I est fini. Pour cela, soit $1 = \sum_{i \in I} e_i$ la décomposition de l'élément unité de l'anneau A suivant les composants $\mathfrak{a}_i$; soit J l'ensemble fini des $i \in I$ tels que $e_i \neq 0$. Si $x \in A$, on a $x = x.1 = \sum_{i \in I} x.e_i = \sum_{i \in J} x.e_i$; et comme $x.e_i \in \mathfrak{a}_i$, $\mathfrak{a}_i$ étant un idéal à gauche, on en conclut que $x \in \sum_{i \in J} \mathfrak{a}_i$, ce qui prouve que $A = \sum_{i \in J} \mathfrak{a}_i$, d'où $J = I$ et I est bien fini.

Il résulte alors du théorème de Jordan-Hölder pour les groupes à opérateurs que toute suite strictement décroissante de sous-modules de A_s, c'est-à-dire d'idéaux à gauche de A , est de longueur $\leqslant n$, n étant le nombre d'éléments de I . Donc A est un anneau d'Artin, et comme le

le module A_s est semi-simple et fidèle, A est semi-primitif donc semi-simple.

Le fait que A_s semi-simple $\Rightarrow$ A d'Artin est une pure curiosité que l'on pourrait rejeter en exercice. La démonstration précédente se réduirait alors à ses deux dernières lignes.

PROPOSITION 4. Soient A un anneau d'Artin semi-simple, M un A-module semi-simple, somme directe d'un nombre fini de modules simples. Le commutant A' de A vis à vis de M est un anneau d'Artin semi-simple.

Supposons d'abord que M soit un module homogène (§ 1, déf.3), somme directe de n modules isomorphes à un même module simple E . On sait que dans ce cas l'anneau A' commutant de A vis à vis de M n'est autre que l'anneau des matrices carrées d'ordre n sur le commutant K^0 de A vis à vis de E ; A' est donc isomorphe à $M_n(K^0)$ qui est un anneau d'Artin simple

Venons-en au cas général, et soit $M = \sum M_i$ la décomposition de M en somme directe de composants homogènes, M_i étant d'espèce E_i . Tout élément $a' \in A'$ est défini par une matrice u_{ij} , où u_{ij} est un homomorphisme de E_i dans E_j . Mais si $i \neq j$ un tel homomorphisme est forcément nul (cela résulte par exemple du lemme de Schur), ce qui montre que a' est simplement défini par une matrice diagonale u_{ii} où u_{ii} appartient au commutant A'_i de A vis à vis de M_i . Il s'ensuit que A' est isomorphe au produit direct des anneaux A'_i , et est donc bien un anneau d'Artin semi-simple d'après la première partie de la démonstration.

7. Algèbres semi-simples.

DEFINITION 2. Une algèbre A sur un corps commutatif k est dite semi-simple (resp. simple) si :

a) $[A : k]$ est fini ,

b) A est un anneau semi-primitif (resp. primitif).

Puisque la condition a) entraîne que A est un anneau d'Artin, cette terminologie est cohérente avec celle introduite plus haut.

Les résultats démontrés dans les n^os précédents s'appliquent aux algèbres simples et semi-simples. Vu l'importance de ce cas particulier, nous allons les répéter brièvement, tout en traduisant deux relatifs aux modules dans le langage des représentations linéaires. La représentation de A associée au module A_s sera appelée <u>représentation régulière</u> (gauche) de A .

<u>Une algèbre simple</u> A <u>sur</u> k <u>est isomorphe à une algèbre de matrices</u> $M_n(K)$; <u>on a</u> $k \subset K \subset A$, <u>ce qui montre que K contient k dans son centre et que</u> $[A:k] = [A:K] \cdot [K:k] = n^2 \cdot [K:k]$. <u>Toute représentation irréductible de</u> A <u>est semblable à la représentation matricielle</u> $A \to M_n(K)$ <u>et son degré est</u> $n \cdot [K:k]$. <u>Toute représentation linéaire de</u> A <u>est complètement réductible.</u>

<u>Une algèbre semi-simple</u> A <u>sur</u> k <u>est isomorphe à un produit</u> $\prod_{i=1}^{z} M_{n_i}(K_i)$ <u>d'algèbres de matrices sur des corps gauches</u> K_i ; $[A:k] = \sum_{i=1}^{z} n_i^2 \cdot [K_i:k]$. <u>Le centre de</u> A <u>est</u> $\prod C_i$, C_i <u>désignant le centre de</u> K_i . <u>Toute représentation linéaire de</u> A <u>est complètement réductible ; toute représentation irréductible de</u> A <u>est semblable à l'une des représentations matricielles</u> $A \to M_{n_i}(K_i)$ <u>et est de degré</u> $n_i \cdot [K_i:k]$. <u>Une telle représentation est contenue</u> n_i <u>fois dans la représentation régulière</u> .

8. <u>Algèbres simples et semi-simples sur un corps algébriquement clos.</u>

Lorsque le corps de base est algébriquement clos, la théorie se simplifie, grâce au résultat suivant :

PROPOSITION 3. Soient K un corps gauche, k un sous-corps de K contenu dans le centre de K et tel que $[K:k] < +\infty$. Si k est algébriquement clos on a $K = k$.

Soit $x \in K$, et soit $k(x)$ le sous-corps de K engendré par k et x . Le corps $k(x)$ est commutatif puisque x commute avec les éléments de k , et c'est une extension finie de k . On a donc $k(x)=k$, d'où $x \in k$, et $K=k$ d'après Ens.II, A.1 .

Combinant la proposition précédente et les résultats du n°7 on obtient:

THEOREME 6. Soit A une algèbre semi-simple sur un corps algébriquement clos k . L'algèbre A est isomorphe à un produit $\prod_{i=1}^{i=r} M_{n_i}(k)$ d'algèbres de matrices sur k . Les représentations matricielles $A \longrightarrow M_{n_i}(k)$ sont, à un isomorphisme près, les seules représentations irréductibles de A ; chacune d'elles est contenue dans la représentation régulière un nombre de fois égal à son degré (i.e. n_i fois). Le centre de A est isomorphe au produit direct de r corps isomorphes à k .

Nous expliciterons deux cas particuliers importants du théorème précédent (à force de descendre du général au particulier dans quel abysme allons-nous tomber !) :

COROLLAIRE 1. Toute représentation irréductible d'une algèbre commutative de dimension finie sur un corps k algébriquement clos est de degré 1 .

En effet, on peut toujours supposer que la représentation est fidèle, auquel cas l'algèbre est semi-simple, et, puisqu'elle est commutative les nombres n_i de l'énoncé du th.6 sont tous égaux à 1 .

COROLLAIRE 2. Soient E un espace vectoriel de dimension finie sur un corps algébriquement clos k , A une sous-algèbre de $\mathcal{L}(E)$ telle que l'injection de A dans $\mathcal{L}(E)$ définisse une représentation irréductible de A . Alors $A = \mathcal{L}(E)$.

Exercices à ajouter à ceux de l'état précédent.

(Les exerc. 1, 5 et 6 figuraient dans l'état 2 comme propositions).

1. Si un anneau primitif A possède un idéal à gauche minimal $\mathfrak{l}$, tout A-module simple et fidèle est isomorphe à $\mathfrak{l}$.

2. Montrer que tout idéal bilatère d'un anneau d'Artin semi-simple est engendré par son intersection avec le centre.

3. Soit E un espace vectoriel de dimension finie sur un corps k algébriquement clos, u un endomorphisme de E. On munit E d'une structure de $k[X]$-module en posant comme à l'ordinaire $P.e = P(u)(e)$ si P est un polynome sur k et si $e \in E$. Montrer que pour que E soit un module semi-simple il faut et il suffit que u soit réductible à la forme diagonale.

4. Un A-module est dit module d'Artin si ses sous-modules vérifient la condition de chaîne descendante.

a) Si on a une suite exacte de modules $M \to N \to P$, où M et P sont des modules d'Artin, alors N est un module d'Artin.

b) Montrer que, pour qu'un groupe abélien soit un module d'Artin sur Z, il faut et il suffit qu'il soit somme directe d'un groupe fini et d'une famille finie de groupes isomorphes au groupe U_p défini dans Alg.VII, § 2, ex.3 (groupe "de type p^∞" de Prufer).

5. Soit E un A-module, et soit A' le commutant de A vis à vis de E. Si F est un sous-A-module de E, on désignera par F° (resp. ${}^\circ F$) l'ensemble des $u \in A'$ tels que $u(E) \subset F$ (resp. tels que $u(F)=0$). F° (resp. ${}^\circ F$) est un idéal à droite (resp. à gauche) de A'.

Inversement, si $\mathfrak{a}$ (resp. $\mathfrak{b}$) est un idéal à droite (resp. à gauche) de A', on désignera par $\mathfrak{a}^\circ$ (resp. ${}^\circ\mathfrak{b}$) le sous-module $\sum_{u \in \mathfrak{a}} u(E)$ (resp. $\bigcap_{u \in \mathfrak{b}} u^{-1}(0)$).

a) Montrer que, si F est facteur direct dans E , on a $(F^0)^0 = F$ et ${}^0({}^0F) = F$ (si p désigne un projecteur de E sur F , on montrera d'abord que $F^0 = p.A$ et que ${}^0F = A.(1-p)$).

b) Si A est un anneau d'Artin semi-simple et si E est de type fini, montrer que l'application $F \longrightarrow F^0$ (resp. $F \longrightarrow {}^0F$) est une application biunivoque de l'ensemble des sous-modules de E sur l'ensemble des idéaux à droite (resp. à gauche) de A' dont l'application réciproque est $\mathfrak{a} \longrightarrow \mathfrak{a}^\circ$ (resp. $\mathfrak{b} \longrightarrow {}^\circ\mathfrak{b}$).

c) Application au cas de l'anneau des endomorphismes d'un espace vectoriel de dimension finie ; détermination des idéaux, nouvelle démonstration de simplicité, etc.

6. Soient A un anneau d'Artin, E un A-module semi-simple. Montrer que, avec les notations du § 1, n°4, on a $A'' = \varphi(A)$.

§ 4. Produits tensoriels d'algèbres semi-simples.

1. Un lemme sur les produits tensoriels.

Soient A et B deux algèbres à élément unité sur un corps commutatif k. On rappelle que l'on peut munir le produit tensoriel $A \otimes B$ d'une structure d'algèbre sur k. L'application $a \to a \otimes 1$ est un isomorphisme de A sur une sous-algèbre de $A \otimes B$, et en général nous identifierons A avec son image par cet isomorphisme. Identification analogue de B avec la sous-algèbre de $A \otimes B$ formée des éléments $1 \otimes b$. Les algèbres A et B sont donc des sous-algèbres de $A \otimes B$.

Si A est une algèbre sur k, et si E est une sous-algèbre de A, on notera E' le commutant de E dans A, c'est-à-dire la sous-algèbre de A formée des a tels que $a.x = x.a$ pour tout $x \in E$.

Ces notations étant posées, on a le lemme suivant (qui aurait avantageusement pu venir au Chap.III) :

LEMME 1. *Soient A et B deux algèbres à élément unité sur un corps commutatif k, C et D des sous-algèbres de A et B respectivement, C' et D' les commutants de C et D dans A et B. Le commutant de $C \otimes D$ dans $A \otimes B$ est $C' \otimes D'$.*

Cherchons d'abord le commutant de C dans $A \otimes B$; soit (b_i) une base de B ; tout élément de $A \otimes B$ s'écrit d'une façon et d'une seule sous la forme $x = \sum a_i \otimes b_i$, avec $a_i \in A$; si l'on exprime que x commute avec tous les éléments de la forme $c \otimes 1$, $c \in C$, on trouve $a_i.c = c.a_i$ pour tout i, ce qui signifie que l'on a $x \in C' \otimes B$. De même le commutant de D est $A \otimes D'$.

Le commutant de $C \otimes D$ est égal à l'intersection des commutants de C et de D, c'est-à-dire à $(C' \otimes B) \cap (A \otimes D')$, et on constate immédiatement que cette dernière sous-algèbre est égale à $C' \otimes D'$.

COROLLAIRE. Le centre de $A \otimes B$ est égal au produit tensoriel des centres de A et de B .

2. Produit tensoriel d'une algèbre séparable et d'une algèbre semi-primitive.

DÉFINITION 1. Une algèbre A sur un corps commutatif k est dite séparable si :

a) A est une algèbre semi-simple (§ 3, n°7),

b) Le centre de A est produit direct de corps commutatifs qui sont des extensions séparables de k .

Il résulte de la condition a) qu'une algèbre séparable est de dimension finie sur k . On notera d'autre part que, si le corps de base k est parfait, toute algèbre semi-simple est séparable.

La principale propriété des algèbres séparables est la suivante :

THEOREME 1. Soient A une algèbre séparable sur un corps k , B une algèbre semi-primitive sur k (de dimension finie ou infinie). L'algèbre $A \otimes B$ est alors semi-primitive.

Si A est produit d'algèbres simples A_i , $A \otimes B$ est produit des algèbres $A_i \otimes B$ et on sait qu'un produit d'algèbres semi-primitives est une algèbre semi-primitive (§ 2, prop.2) ; il suffit donc de prouver le théorème lorsque A est simple.

On a alors $A = M_n(K)$, K étant un corps gauche ; or on sait que $M_n(K) \approx M_n(k) \otimes K$. On a donc $A \otimes B \approx M_n(k) \otimes K \otimes B \approx M_n(K \otimes B)$ et si on sait que $K \otimes B$ est semi-primitive, il en sera donc de même de $A \otimes B$ d'après la prop.3 du § 2 . On est donc ramené au cas où A est un corps K dont le centre C est séparable sur k .

L'algèbre $C \otimes B$ est alors semi-primitive d'après le cor. au th.4 du § 2 ; désignons cette algèbre par B_0 ; l'algèbre $A \otimes B$ est isomorphe à $K \otimes B_0$, le produit tensoriel étant pris sur C (transitivité du produit tensoriel - sera faite en long et en large dans la 2è édition des chap.II,III). Appliquant alors le th.4 du § 2, on voit que $K \otimes B_0$ est semi-primitive, ce qui achève la démonstration.

COROLLAIRE 1. Le produit tensoriel d'une algèbre semi-simple et d'une algèbre séparable est une algèbre semi-simple.

En effet on sait que "semi-simple" équivaut à "semi-primitif" pour une algèbre de dimension finie.

COROLLAIRE 2. Soient A et B deux algèbres simples sur k , A ayant k pour centre. Le produit tensoriel $A \otimes B$ est une algèbre simple.

Puisque k est le centre de A , A est séparable sur k , et $A \otimes B$ est semi-simple d'après le cor.1 ; reste à voir que $A \otimes B$ est simple, ou, ce qui revient au même, que son centre est réduit à un corps commutatif. Or le centre de B est un corps K , et, d'après le cor. au lemme 1, le centre de $A \otimes B$ est $k \otimes K \approx K$. C.Q.F.D.

COROLLAIRE 3. Soit A une algèbre simple sur k , de rang n , et ayant k pour centre. Si A^0 est l'algèbre opposée de A , $A \otimes A^0$ est isomorphe à l'algèbre de matrices $M_n(k)$.

Désignons par E l'algèbre A , munie de sa seule structure d'espace vectoriel sur k . Pour tout $a \in A$, les applications $x \to a.x$ et $x \to x.a$ sont des k-endomorphismes de E , que nous noterons G_a et R_a respectivement. L'application $a \to G_a$ (resp. $a \to R_a$) est un isomorphisme de l'algèbre A (resp.A^0) dans l'algèbre $\mathcal{L}(E)$ de tous les endomorphismes de E ; comme $G_a.R_b = R_b.G_a$ pour tout couple (a,b) d'éléments de A ,

ces isomorphismes définissent un homomorphisme $\varphi : A \otimes A^0 \longrightarrow \mathcal{L}(E)$ tel que $\varphi(a \otimes b) = G_a . R_b$, donc non nul. Or $\mathcal{L}(E)$ est simple (§ 3, th.2) ainsi que $A \otimes A^0$ (cor.2), et ces deux algèbres ont même dimension sur k , à savoir n^2 . Il s'ensuit que φ est un isomorphisme de $A \otimes A^0$ sur $\mathcal{L}(E) \approx \underline{M}_n(k)$. C.Q.F.D.

3. Extension du corps de base.

Soient A une algèbre sur k , K une extension du corps k . On sait qu'on peut munir le produit tensoriel $A \otimes K$ d'une structure d'algèbre sur K . Nous désignerons $A \otimes K$ muni de cette structure par $A_{(K)}$. On a $[A_{(K)} : K] = [A : k]$.

THEOREME 2. Si A est une algèbre de dimension finie sur un corps commutatif k , les deux propriétés suivantes sont équivalentes :

a) A est une algèbre séparable.

b) $A_{(K)}$ est semi-simple quelle que soit l'extension K de k .

Si A est séparable, A_K est un anneau semi-primitif d'après le th.1 ; l'algèbre $A_{(K)}$ étant à la fois de dimension finie sur K , et semi-primitive, est une algèbre semi-simple, ce qui montre que a) $\Rightarrow$ b) .

Réciproquement soit A une algèbre vérifiant b) ; prenant K=k on voit d'abord que A est semi-simple sur k ; soit $\prod C_i$ le centre de A , chaque C_i étant une extension finie de k . Si K est une extension arbitraire de k , le centre de $A \otimes K$ est $\prod (C_i \otimes K)$, et il s'ensuit que chaque $C_i \otimes K$ est une algèbre semi-simple sur K . Il nous suffit donc de prouver :

LEMME 2. Soit C une extension finie d'un corps k . Si $C \otimes C$ est une algèbre semi-simple, C est séparable sur k .

Posons $E = C \otimes C$, et soit C_o la plus grande extension séparable de k contenue dans C ; soit F le produit tensoriel de C avec lui-même pris sur C_o .

L'application $x \otimes_k y \longrightarrow x \otimes_{C_o} y$ étant un homomorphisme de E sur F il s'ensuit que F est une algèbre semi-simple (en effet, d'après les résultats du § 3,n°4, toute algèbre quotient d'une algèbre semi-simple est semi-simple), et comme F est commutative, cela signifie que le seul élément nilpotent de F est 0 (§ 3,cor. au th.1).

Soit alors $x \in C$; on sait que x est radiciel sur C_o, autrement dit qu'il existe une puissance p^f de la caractéristique telle que $x^{p^f} = a$ appartienne à C_o . Soit $y = x \otimes 1 - 1 \otimes x$ dans $C \otimes C = F$. On a d'après la formule du binôme $y^{p^f} = a \otimes 1 - 1 \otimes a = 0$. Il s'ensuit que $y=0$, ce qui entraîne $x \in C_o$, d'où $C=C_o$ et C est bien séparable sur k .

(Le rédacteur serait assez d'avis de vider en exer. la partie b) $\Rightarrow$ a) du th.2 ; cela n'a pas un bien grand intérêt de savoir que les seules "bonnes" algèbres sont celles qui sont séparables).

COROLLAIRE 1. Si A est une algèbre simple de centre k , $A_{(K)}$ est une algèbre simple de centre K quelle que soit l'extension K de k .

Il résulte du th.2 que $A_{(K)}$ est une algèbre semi-simple. Comme son centre est K c'est une algèbre simple.

COROLLAIRE 2. Si A est une algèbre simple de centre k , son rang est un carré parfait r^2 . En particulier, le rang d'un corps gauche sur son centre est soit infini, soit un carré parfait.

Soit Ω la clôture algébrique de k . D'après le cor.1 ci-dessus $A_{(\Omega)}$ est une algèbre simple de centre Ω , et d'après le th.6 du § 3 , $A_{(\Omega)}$ est donc isomorphe à une algèbre de matrices $M_r(\Omega)$. On a donc

$$[A:k] = [A_{(\Omega)} : \Omega] = r^2 .$$

COROLLAIRE 3. Soient K et L deux corps commutatifs, extensions d'un corps k . Si L est une extension séparable finie de k , le produit tensoriel $L \otimes K$ (sur k) est produit direct de corps commutatifs M_i . Chaque M_i contient des sous-corps isomorphes à L et K qui l'engendrent, et réciproquement tout corps M jouissant de cette propriété est isomorphe à l'un des M_i .

D'après le th.2, $L \otimes K$ est une algèbre semi-simple sur K , donc est produit direct de corps commutatifs M_i ; soit $r_i : L \otimes K \to M_i$ la projection canonique de $L \otimes K$ sur son i-ème facteur. Les images L' et K' de L et de K dans M_i sont des sous-corps de M_i qui l'engendrent et L' est isomorphe à L ainsi que K' à K . Réciproquement s'il existe deux isomorphismes de K et L dans un corps M dont les images engendrent M , cela définit un homomorphisme de $L \otimes K$ sur M , et M est isomorphe à l'un des M_i .

Remarque. D'après le théorème de l'élément primitif, L est isomorphe à $k[X]/(f)$, où f est un polynome irréductible sur k et séparable. Il s'ensuit que $L \otimes K$ est isomorphe à $K[X]/(f)$; soit $f_1, \ldots, f_r$ les facteurs de la décomposition de f en polynomes irréductibles sur K ; les f_i sont tous distincts puisque f est séparable. Ils sont donc premiers entre eux, et $K[X]/(f)$ est isomorphe au produit direct des corps $K[X]/(f_i)$. On retrouve ainsi directement la décomposition de $L \otimes K$, avec en plus la détermination des K_i : $K_i = K[X]/(f_i)$.

*Exemple. Soit k un corps valué par une valuation φ , $K = \hat{k}_\varphi$ le complété de k , L une extension finie et séparable de k . Le produit tensoriel $L \otimes \hat{k}_\varphi$ est isomorphe au produit direct des complétés de L relativement aux diverses valuations qui prolongent φ :

$$L \hat{\otimes} \hat{k}_{\mathfrak{p}} = \prod_{\mathfrak{q}|\mathfrak{p}} \hat{L}_{\mathfrak{q}} . \quad *$$

4. Isomorphismes d'algèbres simples.

THÉORÈME 3. Soit A une algèbre simple sur un corps k , de centre réduit à k . Soient f et g deux isomorphismes d'une algèbre simple B dans l'algèbre A tels que $f(1) = g(1) = 1$. Il existe alors un élément inversible $a \in A$ tel que $f(x) = a.g(x).a^{-1}$ pour tout $x \in B$.

Si A est une algèbre de matrices sur k , le théorème 3 revient à affirmer que deux représentations matricielles de même degré de l'algèbre B sont semblables, ce qui est évident puisque ces deux représentations contiennent le même nombre de fois l'unique représentation irréductible de B .

Dans le cas général, soit A^0 l'algèbre opposée de A , et prolongeons f et g en des isomorphismes f' et g' de $B \otimes A^0$ dans $A \otimes A^0$ en posant :

$$f'(x \otimes y) = f'(x) \otimes y \quad \text{et} \quad g'(x \otimes y) = g(x) \otimes y , \quad \text{si } x \in B \text{ et } y \in A^0 .$$

D'après le cor.3 au th.1, $A \otimes A^0$ est une algèbre de matrices sur k , et il existe donc $c \in A \otimes A^0$ tel que $f'(x \otimes y) = c.g'(x \otimes y).c^{-1}$. En particulier, prenant $x=1$, on a $1 \otimes y = c.(1 \otimes y).c^{-1}$, ce qui signifie que c appartient au commutant de $k \otimes A^0$ dans $A \otimes A^0$. D'après le lemme 1, ce commutant est $A \otimes k$, et on a donc $c = a \otimes 1$, $a \in A$. On tire de là :

$$(f(x) - a.g(x).a^{-1}) \otimes y = 0 \quad \text{pour tout } y , \text{ d'où } f(x) = a.g(x).a^{-1} ,$$

C.Q.F.D.

COROLLAIRE (Skolem-Noether). Si A est une algèbre simple sur un corps k , de centre réduit à k , tout automorphisme de A est intérieur.

5. Commutation dans les algèbres simples.

THEOREME 4. Soit A une algèbre simple sur un corps k , de centre réduit à k . Soit B une sous-algèbre simple de A , contenant 1 , et soit C le commutant de B dans A . L'algèbre C est simple, on a :

$$[A:k] = [B:k] \cdot [C:k] ,$$

et B est le commutant de C dans A .

Désignons par E l'algèbre B munie de sa seule structure de k-espace vectoriel, et plongeons B dans l'algèbre $\mathcal{L}(E)$ des endomorphismes de E en faisant correspondre à tout b l'homothétie $x \to b.x$. On sait que le commutant de B dans $\mathcal{L}(E)$ est l'algèbre des homothéties $x \to x.b$, $b \in B$, isomorphe à l'algèbre opposée B^0 de B .

Considérons l'algèbre $A \otimes \mathcal{L}(E)$; c'est une algèbre simple d'après le cor.2 au th.1 et son centre est k ; $A \otimes \mathcal{L}(E)$ contient deux sous-algèbres isomorphes à B : $B \otimes k$ et $k \otimes B$. D'après le th.3 il existe un automorphisme intérieur qui transforme l'une en l'autre ces deux sous-algèbres, donc aussi leurs commutants. Or le commutant de $B \otimes k$ est $C \otimes \mathcal{L}(E)$, et celui de $k \otimes B$ est $A \otimes B^0$ (Lemme 1) ; il s'ensuit que $C \otimes \mathcal{L}(E)$ est isomorphe à $A \otimes B^0$.

D'après le cor.2 au th.1, $A \otimes B^0$ est une algèbre simple ; il en est donc de même de $C \otimes \mathcal{L}(E)$, donc aussi de C. On a en outre :

$[C \otimes \mathcal{L}(E) : k] = [C:k] \cdot [B:k]^2$ et $[A \otimes B^0 : k] = [A:k] \cdot [B:k]$, d'où en comparant : $[A:k] = [B:k] \cdot [C:k]$.

Enfin, si B' désigne le commutant de C dans A , on a évidemment $B' \supset B$, et, d'après ce qui précède : $[A:k] = [C:k] \cdot [B':k]$, d'où $[B':k] = [B:k]$, et $B' = B$.

COROLLAIRE 1. Si le centre de B est réduit à k , B et C sont linéairement disjoints sur k , et $A \approx B \otimes C$.

Le centre de B et le centre de C sont égaux à $B \cap C$, donc réduits à k , ce qui montre que $B \otimes C$ est une algèbre simple de centre k (cor.2 au th.1). Il s'ensuit que l'homomorphisme canonique de $B \otimes C$ sur la sous-algèbre de A engendre par B et C est biunivoque, et comme $B \otimes C$ et A ont même rang, c'est un isomorphisme de $B \otimes C$ sur A .

COROLLAIRE 2. *Soient A une algèbre simple sur un corps k , de centre réduit à k , et soit L un sous-corps commutatif de A , contenant k . Les trois propriétés suivantes sont équivalentes :*

a) $[A:k] = [L:k]^2$,

b) *L coïncide avec son commutant dans A ,*

c) *L est un sous-anneau commutatif maximal de A .*

Soit L' le commutant de L dans A ; puisque L est commutatif, $L' \supset L$, ce qui montre l'équivalence de a) et de b), compte tenu du th.4 . L'équivalence de b) et de c) est évidente.

COROLLAIRE 3. *Soit D un corps gauche, de rang fini sur son centre k . Pour qu'un sous-corps commutatif L de D , contenant k , soit sous-corps commutatif maximal de D , il faut et il suffit que* $[D:k] = [L:k]^2$.

Cela résulte du cor.2 et du fait que tout sous-anneau de D contenant k est un corps (chap.V, référence ?).

Comme D possède au moins un sous-corps commutatif maximal, on retrouve le fait que $[D:k]$ est un carré parfait.

COROLLAIRE 4. (prime au lecteur). *Tout corps fini est commutatif.*

Soit D un corps fini, k son centre ; deux sous-corps commutatifs maximaux de D ont même degré sur k (cor.3), donc sont isomorphes (Alg.V, § 11, prop.3) et transformés l'un en l'autre par un automorphisme intérieur de D (th.3). Comme tout élément de D appartient à un sous-corps commutatif contenant k , donc aussi à un sous-corps commutatif maximal,

il suit de là que D est réunion des xLx^{-1} , $x \in D^*$, L étant un sous-corps commutatif maximal fixe de D . Il s'ensuit que le groupe multiplicatif D^* est réunion des conjugués xL^*x^{-1} de son sous-groupe L^* . Si $x'=xt$, $t \in L^*$, on a $x'L^*x'^{-1} = xtL^*t^{-1}x^{-1} = xL^*x^{-1}$; le nombre des conjugués xL^*x^{-1} est donc au plus égal à l'indice $(D^*:L^*)$; comme chaque conjugué a même nombre d'éléments que L^* , D^* ne peut être réunion des xL^*x^{-1} que si ces ensembles forment une partition de D^* ; puisqu'ils ont en commun l'élément unité, c'est que leur nombre est 1, d'où $D^*=L^*$ et $D = L$, ce qui montre que D est commutatif.

6. Groupe de Brauer.

Soit k un corps commutatif. Tout algèbre A simple sur k , et de centre k , est isomorphe à $\underline{M}_n(k) \otimes K$, où K est un corps gauche de centre k . En outre, le corps K est déterminé par A de façon unique, puisque le corps opposé K^0 est le commutant de A vis-à-vis d'une représentation irréductible de A et que deux telles représentations sont semblables. On peut donc parler du corps gauche K attaché à A .

On dit que deux algèbres simples A et A', de centre réduit à k , sont semblables si le corps K attaché à A est k-isomorphe au corps K' attaché à A'. Cela définit une relation d'équivalence entre algèbres simples de centre k dont les classes (appelées classes d'algèbres simples) correspondent biunivoquement aux corps gauches de centre k et finis sur k .

Si A appartient à la classe $\mathcal{A}$, le produit tensoriel $A \otimes \underline{M}_r(k)$ appartient aussi à $\mathcal{A}$, car $A \otimes \underline{M}_r(k) \approx \underline{M}_n(k) \otimes D \otimes \underline{M}_r(k) \approx \underline{M}_{nr}(k) \otimes D$.

Soient $\mathcal{A}$ et $\mathcal{B}$ deux classes correspondant aux corps gauches D et D'. La classe du produit tensoriel $D \otimes D'$ est dite classe produit des classes $\mathcal{A}$ et $\mathcal{B}$ et est désignée par $\mathcal{A}.\mathcal{B}$; si on a $A \in \mathcal{A}$ et $B \in \mathcal{B}$,

on a $A \otimes B \in \mathcal{A}.\mathcal{B}$; en effet, on a $A = M_n(k) \otimes D$, $B = M_m(k) \otimes D'$, d'où $A \otimes B = M_{mn}(k) \otimes D \otimes D'$ ce qui entraîne $A \otimes B \in \mathcal{A}.\mathcal{B}$, comme nous venons de le voir. Réciproquement, il est évident que cette propriété caractérise le produit de deux classes. L'associativité et la commutativité du produit tensoriel montrent alors que le produit des classes d'algèbres est associatif et commutatif. La classe formée des algèbres $M_n(k)$, $n \geqslant 1$, est élément neutre pour ce produit. Si A parcourt une classe $\mathcal{A}$, correspondant au corps gauche D , les algèbres opposées A^0 parcourent une classe $\mathcal{A}^0$ qui correspond au corps gauche D^0 opposé de D , et qui est l'inverse de la classe $\mathcal{A}$ d'après le cor.3 du th.1 .

Ainsi l'ensemble $\mathcal{G}_k$ des classes d'algèbres simples de centre k , muni de la loi de composition précédente, forme un groupe abélien.

DEFINITION 2. Soit k un corps commutatif. Le groupe abélien $\mathcal{G}_k$ des classes d'algèbres simples sur k , de centre réduit à k , muni de la loi de composition du produit tensoriel, est appelé groupe de Brauer de k .

Exemples . 1. Si k est algébriquement clos, $\mathcal{G}_k = \{e\}$, d'après la prop.3 du § 3 .

2. Si k est un corps fini, $\mathcal{G}_k = \{e\}$, d'après le cor.4 du th.4 .

3. Si k est ordonné maximal, $\mathcal{G}_k \approx \mathbb{Z}/(2)$, cf. exerc.2 .

* 4. Si k est un corps localement compact, pour la topologie définie par une valuation (non archimédienne), $\mathcal{G}_k \approx \mathbb{Q}/\mathbb{Z}$ ("rationnels modulo 1"). Cf.Alg. Unid., I .

*

7. Extension du corps de base, corps de décomposition.

Soient k un corps commutatif, K une extension de k. A toute algèbre simple sur k , de centre réduit à k , soit A , faisons correspondre l'algèbre $A_{(K)}$ obtenue par extension du corps de base à K .

D'après le cor.1 au th.2 $A_{(K)}$ est une algèbre simple de centre K . En outre il est clair que si A et B sont deux algèbres semblables, les algèbres $A_{(K)}$ et $B_{(K)}$ sont semblables. Il s'ensuit que $A \to A_{(K)}$ définit par passage au quotient une application $\varphi_{K/k}$ du groupe de Brauer $\mathcal{G}_k$ dans le groupe de Brauer $\mathcal{G}_K$.

PROPOSITION 1. L'application $\varphi_{K/k}: \mathcal{G}_k \to \mathcal{G}_K$ est un homomorphisme.

Cela résulte de la formule :

$$A_{(K)} \otimes_K B_{(K)} \approx (A \otimes_k B)_{(K)} ,$$

où A et B désignent des algèbres sur k . Cette formule se démontre immédiatement en prenant une base, ou par tout autre moyen.

Le noyau $\mathcal{H}_{K/k}$ de $\varphi_{K/k}$ est donc un sous-groupe de $\mathcal{G}_k$; ses éléments sont appelés classes d'algèbres décomposées par K . Par abus de langage, on dit qu'une algèbre simple de centre k , A , est décomposée par K si la classe $\mathcal{A}$ de A appartient à $\mathcal{H}_{K/k}$. Pour cela il faut et il suffit que $A_{(K)}$ soit isomorphe à $M_n(K)$ pour un certain n . Le corps K est alors dit corps de décomposition de A (et aussi de $\mathcal{A}$).

8. Critère de décomposition.

THEOREME 5. Soient k un corps commutatif, $\mathcal{G}_k$ le groupe de Brauer de k , $\mathcal{A}$ un élément de $\mathcal{G}_k$, et K une extension finie de k . Les deux propriétés suivantes sont équivalentes :

a) K est corps de décomposition de $\mathcal{A}$,

b) La classe $\mathcal{A}$ contient une algèbre A telle que $K \subset A$ et que $[A:k] = [K:k]^2$.

Montrons que a) $\Rightarrow$ b) . Soit D le corps gauche attaché à la classe $\mathcal{A}$; puisque K est corps de décomposition de $\mathcal{A}$, il l'est aussi de la classe opposée $\mathcal{A}^0$ et en particulier de D^0 ; $D^0 \otimes K$ est isomorphe

à une algèbre de matrices sur K , ou, ce qui revient au même, à l'algèbre $\mathcal{L}_K(E)$ des K-endomorphismes d'un K-espace vectoriel E de dimension finie. Soit $\mathcal{L}_k(E)$ l'algèbre des k-endomorphismes de l'espace vectoriel E ; l'algèbre $D^0 \otimes K \approx \mathcal{L}_K(E)$ est plongée dans $\mathcal{L}_k(E)$ et son commutant est K , identifié aux homothéties de E . Soit A le commutant de D^0 dans $\mathcal{L}_k(E)$; je dis que A vérifie les propriétés énoncées dans b) . Il est d'abord clair que $A \supset K$; en outre, d'après le th.4, on a :

$$[D:k] \cdot [A:k] = [\mathcal{L}_k(E):k] = [D^0 \otimes K] \cdot [K:k] = [D:k] \cdot [K:k]^2 ,$$

d'où $[A:k] = [K:k]^2$; enfin, puisque A est identique à l'algèbre des endomorphismes de E considéré comme espace vectoriel sur D^0, A est isomorphe à une algèbre de matrices sur D , donc appartient à la classe $\mathcal{A}$ donnée.

Pour prouver que b) $\Rightarrow$ a), il suffit évidemment de montrer que A est décomposée par K ; pour cela, désignons par E l'algèbre A considérée comme k-espace vectoriel. D'après le cor.3 au th.1 on peut identifier $A \otimes A^0$ à $\mathcal{L}(E)$; d'après le lemme 1, le commutant de $k \otimes K$ dans $A \otimes A^0$ est $A \otimes K$, puisque K est son propre commutant dans A^0 (cor.2 au th.4) ; en d'autres termes, ceci signifie que $A \otimes K$ est l'algèbre des K-endomorphismes de E , et A est bien décomposée par K .

COROLLAIRE 1. Soit D un corps gauche fini sur k et de centre k ; posons $[D:k] = r^2$. Pour tout corps de décomposition K de D , $[K:k]$ est un multiple de r .

Soit $\mathcal{A}$ la classe d'algèbres qui contient D , $A \in \mathcal{A}$ l'algèbre qui vérifie les propriétés b) du th.5 . A est une algèbre de matrices d'ordre n sur D . On a donc $[A:k] = n^2 r^2$, d'où $[K:k] = nr$.

COROLLAIRE 2. Soit D un corps gauche, de rang fini sur son centre k . Tout sous-corps commutatif maximal de D est corps de décomposition de D .

En effet, un tel sous-corps K contient k et d'après le cor.3 du th.4 on a $[D:k] = [K:k]^2$; on peut donc appliquer le th.5 .

Remarque. Il ne faudrait pas croire que tout corps de décomposition de D contient un sous-corps commutatif maximal de D , ni que les sous-corps commutatifs maximaux de D sont isomorphes.

Par exemple, si k est un corps p-adique, et si $[D:k] = r^2$, toute extension K/k de degré r est isomorphe à un sous-corps commutatif maximal de D .

9. Existence de corps de décomposition galoisiens.

LEMME 3. Soit D un corps gauche, de rang fini sur son centre k , et distinct de k . Il existe un sous-corps commutatif M de D , contenant k , séparable sur k , et distinct de k .

Si k est fini, le lemme est évident puisque toute extension d'un corps fini est séparable. Nous pouvons donc supposer k infini.

Si le lemme était inexact, tout élément de D serait radiciel sur k , donc vérifierait une équation de la forme :

$$x^{p^e} = a \in k \quad , \quad p \text{ étant l'exposant caractéristique.}$$

En outre, si $[D:k] = r^2$, le degré de l'extension $k(x)/k$ est au plus r , ce qui montre que l'on peut prendre $p^e \leqslant r$. Il existe donc un entier f tel que :

$$x^{p^f} \in k \qquad \text{quel que soit } x \in D .$$

Soit e_i une base de D sur k , telle que $e_1 = 1$. Tout élément $x \in D$ s'écrit $x = \sum x_i e_i$, $x_i \in k$, et l'élément x^{p^f} s'écrit :

$$x^{p^f} = \sum_j P_j(x_i).e_j \quad ,$$

les P_j étant certains polynômes par rapport aux x_i dont les coefficients ne font intervenir que les coefficients de la table de multiplication de D . Par hypothèse, on a $P_j(x_i)=0$ si $j\neq 1$ quelles que soient les valeurs que l'on donne aux x_i dans k . Puisque k est infini, ceci entraîne que les P_j sont identiquement nuls.

Etendons maintenant le corps de base à un corps de décomposition K de D . L'équation :

$$x^{p^f} = \sum_j P_j(x_i).e_j \quad ,$$

reste encore valable, les x_i prenant leurs valeurs dans K . Comme les polynomes P_j sont identiquement nuls pour $j\neq 1$, il s'ensuit que l'on a : $x^{p^f} \in K$ quelque soit $x \in D_{(K)}$.

Mais $D_{(K)}$ est isomorphe à $M_r(K)$, et contenant donc des idempotents n'appartenant pas au centre, ce qui est en contradiction avec ce qui précède.

THEOREME 6. Tout corps gauche D , fini sur son centre k , contient un sous-corps commutatif maximal qui est séparable sur k .

Soit L un sous-corps séparable maximal de D , et montrons que L est sous-corps commutatif maximal de D , ou, ce qui revient au même, que L coïncide avec son commutant L' dans D . Ce commutant est un corps gauche de centre L d'après le th.4 . S'il n'était pas confondu avec L , il existerait, d'après le Lemme 3, un corps K , avec $L \subset K \subset L'$, $K \neq L$, et K séparable sur L . Mais alors K serait séparable sur k , ce qui est contraire au caractère maximal de L .

COROLLAIRE. Quel que soit le corps commutatif k , le groupe de Brauer $\mathcal{G}_k$ de k est réunion des sous-groupes $\mathcal{H}_{K/k}$ correspondant aux extensions galoisiennes finies K de k .

En d'autres termes, toute classe d'algèbre $\mathcal{A} \in \mathcal{G}_k$ possède un corps de décomposition qui est galoisien sur k .

En effet, d'après le th.6 joint au cor.2 du th.5, $\mathcal{A}$ possède un corps de décomposition L qui est fini et séparable sur k . L'extension galoisienne K engendrée par L est *a fortiori* corps de décomposition de $\mathcal{A}$.

10. Classes d'algèbres simples décomposées par une extension galoisienne du corps de base. (Remarques).

Pour étudier le groupe de Brauer $\mathcal{G}_k$ d'un corps k , il suffit d'après le cor. au th.6, d'étudier les sous-groupes $\mathcal{H}_{K/k}$ correspondant à une extension galoisienne finie K de k . Le résultat principal est alors

Soit G le groupe de Galois de K/k ; le groupe $\mathcal{H}_{K/k}$ est isomorphe au second groupe de cohomologie de G à coefficients dans le groupe K^* . Autrement dit : $\mathcal{H}_{K/k} \approx H^2(G,K)$.

Il n'est pas question de parler de cohomologie ici, et on ne peut donc pas démontrer le résultat précédent. Mais on pourrait, sans introduire aucune espèce de "système de facteurs", démontrer le résultat équivalent (modulo la cohomologie) suivant :

Il y a une correspondance biunivoque entre les éléments $\mathcal{A} \in \mathcal{H}_{K/k}$ et les classes d'extensions du groupe de Galois G par le groupe K^* (les opérations de G sur K^* étant évidemment données).

Cette correspondance est la suivante :

1. Soit $\mathcal{A} \in \mathcal{H}_{K/k}$, et soit A l'algèbre attachée à $\mathcal{A}$ par le th.5 ; soit E l'ensemble des éléments inversibles de A tels que $x.K.x^{-1} = K$. E contient le groupe multiplicatif K^* , et tout élément de E induit sur K^* un automorphisme $\sigma \in G$. D'où une suite d'homomorphismes :

$$\{1\} \to K^* \to E \to G \to \{1\} ,$$

que l'on démontre immédiatement être exacte ; on a bien obtenu une extension de G par K^* .

2. Réciproquement, soit E une telle extension ; si à chaque classe modulo K^* on ajoute un élément "0", on peut définir sur chaque classe une structure d'espace vectoriel de dimension 1 sur K (par translation à partir de K^*). L'espace vectoriel somme directe de ces différents espaces vectoriels peut être muni d'une structure d'anneau de façon évidente (grâce à la multiplication dans E), et on obtient une algèbre A sur k qui est simple et de centre k .

On constate enfin que les deux correspondances précédentes sont bien réciproques.

(Pour plus de détails, voir Sém.Cartan, 50-51, exp.VII).

Il n'y a pas trace de cohomologie là-dedans. La cohomologie viendrait ultérieurement, pour déterminer le groupe des classes d'extensions d'un groupe G par un groupe abélien à opérateurs A .

Exercices à ajouter à ceux de l'état précédent.

(Les 3 premiers figuraient dans l'état 2 comme théorèmes).

1. Soient K et L deux extensions d'un corps commutatif k telles que $[K:k] < +\infty$, et que L/k soit séparable. Montrer que $K \otimes L$ est semi-primitif.

2. Si k est ordonné maximal, tout corps gauche de centre k et fini sur k est isomorphe au corps des quaternions sur k .

3. Soit D un corps gauche fini sur son centre k et possédant un anti-automorphisme involutif $x \to x'$ tel que $x+x'$ et xx' appartiennent à k et que $a'=a$ pour tout $a \in k$. Montrer que, si la caractéristique de D est différente de 2 , D est un corps de quaternions sur k .

4. Soient A une algèbre séparable sur un corps k , B une algèbre arbitraire de radical r(B). Montrer que le radical de $A \otimes B$ est $A \otimes r(B)$.

5. Soit k un corps parfait et soit Ω un clôture algèbrique de k . Supposons que pour tout entier n il existe un corps K_n et un seul tel que $k \subset K_n \subset \Omega$ et que $[K_n:k] = n$. Montrer que le groupe de Brauer de k est réduit à $\{e\}$.

(cf. Schilling, Th. des Val't, VI,1 où l'on trouvera d'autres exer.).

§ 5. Représentations des groupes.

1. Norme et trace d'une représentation.

Soient A une algèbre sur un corps commutatif k , E un espace vectoriel de dimension finie sur k , M une représentation linéaire de A dans E (§ 2, n°3).

DEFINITION 1. On appelle trace (resp. norme) d'un élément $x \in A$ relativement à la représentation $x \to M(x)$ de A , la trace (resp. le déterminant) de l'endomorphisme $M(x)$.

Il est clair que la trace et la norme ne changent pas lorsque l'on remplace M par une représentation semblable, autrement dit ne dépendent que de la classe $\mathfrak{D}$ de la représentation. On les notera respectivement $\mathrm{Tr}_{\mathfrak{D}}(x)$ et $N_{\mathfrak{D}}(x)$. Les formules suivantes résultent immédiatement des propriétés de la trace et du déterminant d'un endomorphisme :

$$\mathrm{Tr}_{\mathfrak{D}}(x+y) = \mathrm{Tr}_{\mathfrak{D}}(x) + \mathrm{Tr}_{\mathfrak{D}}(y)$$

$$N_{\mathfrak{D}}(xy) = N_{\mathfrak{D}}(x).N_{\mathfrak{D}}(y)$$

$$\mathrm{Tr}_{\mathfrak{D}}(xy) = \mathrm{Tr}_{\mathfrak{D}}(yx)$$

$$\mathrm{Tr}_{\mathfrak{D}}(\lambda x) = \lambda.\mathrm{Tr}_{\mathfrak{D}}(x) , \qquad \lambda \in k ,$$

$$N_{\mathfrak{D}}(\lambda x) = \lambda^{r}.N_{\mathfrak{D}}(x)$$ où r est le degré des représentations de la classe $\mathfrak{D}$.

Soient M et M' deux représentations de A dans des espaces vectoriels E et E'. La somme directe de E et E', considérés comme A-modules, est encore un A-module, et définit donc une représentation linéaire de A dans E+E' qui est dite somme des représentations M et M' . La classe $\mathfrak{D}''$ de cette représentation ne dépend évidemment que des classes $\mathfrak{D}$ et $\mathfrak{D}'$ de M et M' , et l'on écrit :

$$\mathfrak{D}'' = \mathfrak{D} + \mathfrak{D}' .$$

Le degré de $\mathcal{D}''$ est égal à la somme des degrés de $\mathcal{D}$ et de $\mathcal{D}'$ et l'on a les formules :

$$\mathrm{Tr}_{\mathcal{D}+\mathcal{D}'}(x) = \mathrm{Tr}_{\mathcal{D}}(x) + \mathrm{Tr}_{\mathcal{D}'}(x)$$
$$\mathrm{N}_{\mathcal{D}+\mathcal{D}'}(x) = \mathrm{N}_{\mathcal{D}}(x) \cdot \mathrm{N}_{\mathcal{D}'}(x) .$$

Lorsque M et M' sont des représentations matricielles $x \longrightarrow \underline{M}(x)$ et $x \longrightarrow \underline{M}'(x)$, la somme des représentations M et M' est semblable à la représentation matricielle $x \longrightarrow \begin{pmatrix} \underline{M}(x) & 0 \\ 0 & \underline{M}'(x) \end{pmatrix}$.

PROPOSITION 1. Soient k un corps commutatif de caractéristique nulle, A une algèbre sur k, $\mathcal{D}$ et $\mathcal{D}'$ deux classes de représentations complètement réductibles de degré fini de l'algèbre A. Si

$$\mathrm{Tr}_{\mathcal{D}}(x) = \mathrm{Tr}_{\mathcal{D}'}(x) \qquad \text{pour tout } x \in A ,$$

on a $\mathcal{D} = \mathcal{D}'$.

En d'autres termes, $\mathrm{Tr}_{\mathcal{D}}$ caractérise $\mathcal{D}$ si $\mathcal{D}$ est complètement réductible et si le corps de base est de caractéristique nulle.

Soient $\mathfrak{a}$ et $\mathfrak{a}'$ les noyaux des représentations $\mathcal{D}$ et $\mathcal{D}'$; les algèbres $A/\mathfrak{a}$ et $A/\mathfrak{a}'$ sont isomorphes à des sous-algèbres d'algèbres de matrices sur k et sont donc de rang fini sur k. Soit $\mathfrak{m} = \mathfrak{a} \cap \mathfrak{a}'$; l'algèbre $A/\mathfrak{m}$ est isomorphe à une sous-algèbre de l'algèbre produit $A/\mathfrak{a} \times A/\mathfrak{a}'$ et est également de rang fini sur k. Puisque $\mathfrak{m}$ est contenu dans le noyau de $\mathcal{D}$ et dans celui de $\mathcal{D}'$, $\mathcal{D}$ et $\mathcal{D}'$ définissent des classes de représentations de $A/\mathfrak{m}$ que nous noterons encore $\mathcal{D}$ et $\mathcal{D}'$. Puisque $\mathcal{D}$ et $\mathcal{D}'$ sont complètement réductibles, le radical de $A/\mathfrak{m}$ est contenu à la fois dans $\mathfrak{a}/\mathfrak{m}$ et dans $\mathfrak{a}'/\mathfrak{m}'$, et est réduit à (0). Nous sommes donc ramenés à démontrer la proposition dans le cas particulier où A est une algèbre semi-simple.

Soit $A = \prod_i A_i$ la décomposition de A en produit d'algèbres simples ; pour chaque i, soit $\mathcal{D}_i^\circ$ l'unique classe de représentation irréductible de A_i, et soit $\mathcal{D}_i$ la représentation irréductible de A définie par $\mathcal{D}_i^\circ$ et par l'homomorphisme canonique $A \to A_i$. On sait (§ 3, n°7) que toute représentation irréductible de A est semblable à l'une des représentations $\mathcal{D}_i$, ce qui montre que

$$\mathcal{D} = \sum_i n_i \cdot \mathcal{D}_i \quad , \quad \mathcal{D}' = \sum_i n_i' \mathcal{D}_i \quad ,$$

où les n_i et les n_i' sont des entiers $\geqslant 0$.

Soient e_i l'élément unité de A_i, ε_i l'élément de A dont toutes les coordonnées sont nulles, sauf le i-ème qui est égale à e_i, r_i le degré de $\mathcal{D}_i$. On a évidemment $\mathrm{Tr}_{\mathcal{D}_i}(\varepsilon_i) = r_i$, puisque l'endomorphisme correspondant à ε_i dans une représentation de la classe $\mathcal{D}_i$ est l'automorphisme identique. D'autre part, on a $\mathrm{Tr}_{\mathcal{D}_j}(\varepsilon_i) = 0$ si $j \neq i$, puisque ε_i est contenu dans le noyau de $\mathcal{D}_j$. D'où $\mathrm{Tr}_{\mathcal{D}}(\varepsilon_i) = n_i \cdot r_i$, $\mathrm{Tr}_{\mathcal{D}'}(\varepsilon_i) = n_i' \cdot r_i$, et comme $\mathrm{Tr}_{\mathcal{D}} = \mathrm{Tr}_{\mathcal{D}'}$, $n_i \cdot r_i = n_i' \cdot r_i$ <u>dans le corps</u> k. Comme k est de caractéristique nulle, cela donne $n_i \cdot r_i = n_i' \cdot r_i$ <u>dans</u> N, d'où $n_i = n_i'$, et $\mathcal{D} = \mathcal{D}'$.

<u>Remarque.</u> Comme on le verra dans la suite de ce traité, on peut, dans certains cas, étendre la notion de trace aux représentations de degré infini. Pour plus de détails (et notamment pour l'extension de la proposition 1) nous renvoyons aux travaux de nos éminents collègues (?).

2. <u>Représentations linéaires des groupes</u>.

Soient G un groupe, k un corps commutatif, $A = k^{(G)}$ (quelle sale notation !) l'algèbre du groupe G relativement au corps k. On appelle <u>représentation linéaire</u> du groupe G dans un espace vectoriel E sur k

un homomorphisme $s \to M(s)$ de G dans le groupe des éléments inversibles de l'algèbre $\mathcal{L}(E)$ des endomorphismes de E . On a donc :

$$\begin{cases} M(e) = 1 & , \text{ e étant l'élément neutre de G ,} \\ M(st) = M(s).M(t) & , \text{ si } s,t \in G . \end{cases}$$

Un tel homomorphisme s'étend par linéarité en un homomorphisme de l'algèbr A dans $\mathcal{L}(E)$ qui transforme l'élément unité de A en l'élément unité de $\mathcal{L}(E)$; réciproquement si $M : A \to \mathcal{L}(E)$ est un tel homomorphisme, on a $M(s).M(s^{-1}) = M(s^{-1}).M(s) = M(e) = 1$, ce qui montre que $M(s)$ est inversible pour tout $s \in G$, et l'application $s \to M(s)$ est une représentation linéaire du groupe G dans E .

Il y a donc une correspondance biunivoque canonique entre les représentations linéaires <u>du groupe</u> G , et les représentations linéaires <u>de l'algèbre</u> A . Toutes les notions relatives aux représentations des algèbre se transportent aux représentations des groupes : représentations semblables, classes de représentations, représentations irréductibles, complètement réductibles, etc..

Si $\mathfrak{D}$ est une classe de représentations de degré fini du groupe G , la fonction $s \to \mathrm{Tr}_{\mathfrak{D}}(s)$, $s \in G$, est appelée le <u>caractère</u> de la classe $\mathfrak{D}$ (certains auteurs réservent ce nom au cas où $\mathfrak{D}$ est irréductible ; faut-il trancher cette question ici ?). Comme tout élément de $A = k^{(G)}$ est combinaison linéaire d'éléments de G , la connaissance du caractère de $\mathfrak{D}$ détermine $\mathrm{Tr}_{\mathfrak{D}}(x)$ pour tout $x \in A$, donc, d'après la prop.1, détermi aussi $\mathfrak{D}$ si $\mathfrak{D}$ est complètement réductible et si la caractéristique du corps de base est nulle.

Soient M et M' deux représentations linéaires d'un groupe G dans des espaces rectoriels E et F'. L'application $s \to M(s) \otimes M'(s)$ est une

représentation linéaire de G dans l'espace E⊗E' ; sa classe ne dépend que des classes $\mathcal{D}$ et $\mathcal{D}'$ de M et M' et est notée $\mathcal{D} \otimes \mathcal{D}'$. On a les formules suivantes :

$$\mathcal{D} \otimes \mathcal{D}' = \mathcal{D}' \otimes \mathcal{D}$$

$$(\mathcal{D} \otimes \mathcal{D}') \otimes \mathcal{D}'' = \mathcal{D} \otimes (\mathcal{D}' \otimes \mathcal{D}'')$$

$$(\mathcal{D} + \mathcal{D}') \otimes \mathcal{D}'' = \mathcal{D} \otimes \mathcal{D}'' + \mathcal{D}' \otimes \mathcal{D}'' .$$

En outre, si M(s) a pour matrice (α_{ij}) et M'(s) pour matrice $(\beta_{k\ell})$, M(s)⊗M'(s) a pour matrice $(\gamma_{(i,k)(j,\ell)})$, avec $\gamma_{(i,k)(j,\ell)} = \alpha_{ij}\beta_{k\ell}$; donc $\mathrm{Tr}(M(s) \otimes M'(s)) = \mathrm{Tr}M(s).\mathrm{Tr}(M'(s)$, c'est-à-dire :

$$\mathrm{Tr}_{\mathcal{D} \otimes \mathcal{D}'}(s) = \mathrm{Tr}_{\mathcal{D}}(s).\mathrm{Tr}_{\mathcal{D}'}(s) .$$

Soit M une représentation de classe $\mathcal{D}$ dans un espace E ; pour tout $s \in G$, soit $\overset{\vee}{M}(s)$ l'endomorphisme <u>contragrédient</u> de M(s), qui est un automorphisme du dual E^* de E défini par : $\overset{\vee}{M}(s) = {}^tM(s)^{-1}$. L'application $s \longrightarrow \overset{\vee}{M}(s)$ est une représentation linéaire de G dans E , dite représentation <u>contragrédiente</u> de M , et dont la classe est désignée par $\overset{\vee}{\mathcal{D}}$. Si $\mathcal{D}$ et $\mathcal{D}'$ sont des classes de degré fini, on a les formules

$$\overset{\vee}{\overset{\vee}{\mathcal{D}}} = \mathcal{D}$$

$$\overset{\vee}{(\mathcal{D} + \mathcal{D}')} = \overset{\vee}{\mathcal{D}} + \overset{\vee}{\mathcal{D}}'$$

$$\overset{\vee}{(\mathcal{D} \otimes \mathcal{D}')} = \overset{\vee}{\mathcal{D}} \otimes \overset{\vee}{\mathcal{D}}' .$$

Comme la trace d'un endomorphisme est égale à celle de son transposé, on a :

$$\mathrm{Tr}_{\overset{\vee}{\mathcal{D}}}(s) = \mathrm{Tr}_{\mathcal{D}}(s^{-1}) .$$

3. <u>Théorème de Maschke</u>.

THEOREME 1. <u>Soient</u> G <u>un groupe fini d'ordre</u> h, k <u>un corps commutatif dont la caractéristique est première à</u> h . <u>Toute représentation linéaire de</u> G <u>dans un espace vectoriel sur</u> k <u>est complètement réductible</u>.

Soit M une représentation linéaire de G dans un espace vectoriel E ; nous poserons $s.x = M(s)(x)$ si $s \in G$ et $x \in E$. Soit V un sous-espace vectoriel de E stable par les opérations de G ; nous devons montrer que V possède un supplémentaire stable.

Soit W l'espace quotient E/V , et soit p la projection canonique de E sur W . Le groupe G opère, par passage à quotient, sur W , et nous noterons encore $x \longrightarrow s.x$ les opérations ainsi obtenus. On sait que tout supplémentaire de V dans E correspond biunivoquement à une application linéaire $q : W \to E$ telle que $p \circ q = 1$; pour que ce supplémentaire soit invariant par G , il faut et il suffit que l'on ait $s \circ q = q \circ s$, $s \in G$.

Soit alors $r : W \to E$ une application telle que $p \circ r = 1$ (une telle application existe toujours, cf. Alg. II, § 3, prop. 5), et posons :

$$q = 1/h \cdot \sum_{t \in G} t^{-1} \circ r \circ t \ ,$$

l'expression $1/h$ ayant un sens puisque la caractéristique de k est première à h . On a $p \circ q = 1/h \sum_{t \in G} t^{-1} \circ 1 \circ t = 1$, et d'autre part : $s \circ q = 1/h \sum_{t \in G} s \circ t^{-1} \circ r \circ t = 1/h \sum_{ts^{-1} \in G} (ts^{-1})^{-1} \circ r \circ (ts^{-1}) \circ s = q \circ s$, ce qui démontre le théorème, d'après ce qui a été dit plus haut.

Exercices à ajouter à ceux de l'état précédent.

1. (Figurait dans l'état 2 comme remarque). Soit K/k une extension séparable finie d'un corps k , $\mathfrak{D}$ la représentation régulière de K . Montrer que $Tr_{\mathfrak{D}}(x) = Tr_{K/k}(x)$ et $N_{\mathfrak{D}}(x) = N_{K/k}(x)$ si $x \in K$.

2. Soient E un espace vectoriel de dimension finie sur un corps k de caractéristique nulle, GL(E) le groupe des automorphismes de E . En faisant opérer les éléments de GL(E) sur $\otimes^p E$ par transport de structure on obtient une représentation linéaire $u \longrightarrow M(u)$ de GL(E) ; soit A la sous-algèbre de $\mathcal{L}(\otimes^p E)$ engendrée par les M(u) .

D'autre part, on définit une représentation linéaire du groupe symétrique d'ordre p $\mathfrak{S}_p$ dans $\overset{p}{\otimes} E$, comme il est dit dans Alg.III, § 5 ; soit B la sous-algèbre de $\mathcal{L}(\overset{p}{\otimes} E)$ engendrée par les transformations ainsi obtenues.

a) Montrer que le commutant de B dans $\mathcal{L}(\overset{p}{\otimes} E)$ est égal à A . En déduire le fait que A est semi-simple (utiliser la prop.4 du § 3) et que le commutant de A est égal à B .

b) Montrer que, sur un corps de caractéristique nulle, tout sous-espace tensoriel d'un espace tensoriel (au sens de Alg.III, § 4) admet un supplémentaire tensoriel.

3. Soit A un espace affine de dimension n sur un corps k , identifié à un hyperplan affine d'un espace vectoriel E de dimension n+1 ; soit H l'hyperplan parallèle à A passant par l'origine.

a) Montrer que tout automorphisme affine de A est induit par un automorphisme de E et un seul.

b) Soit G un groupe, et soit $s \to N(s)$ une représentation de G dans le groupe des automorphismes de A (représentation affine de G). Montrer qu'il existe une représentation linéaire $s \to M(s)$ de G dans E et une seule qui induise N(s). Pour que H admette un supplémentaire stable par M(s), $s \in G$, il faut et il suffit qu'il existe $a \in A$ fixe par les transformations N(s).

c) Réciproquement, soit M(s) une représentation linéaire de G dans un espace E , H un sous-espace stable de E . Montrer que les supplémentaires de H dans E forment un espace affine sur lequel opère G ; cet espace affine possède un point fixe si et seulement s'il existe un supplémentaire de H qui soit stable par G .

d) Déduire de ce qui précède que, si G est un groupe (resp. un groupe topologique), on a (1) $\Leftrightarrow$ (2), (1') $\Leftrightarrow$ (2') et (1") $\Leftrightarrow$ (2"), avec :

(1) (resp. (1'), (1")) - Toute représentation linéaire (resp. de dimension finie, resp. continue et de dimension finie) de G est complètement réductible.

(2) (resp. (2'),(2")) - Toute représentation affine (resp. de dimension finie, resp. de dimension finie et continue) de G possède un point fixe.

e) Soit G un groupe possédant un sous-groupe invariant H tel que H et G H vérifient (1) (resp. (1'),(1")). Montrer que G vérifie (1) (resp. (1'),(1")). (On utilisera l'équivalence avec (2),(2'),(2")).

APPENDICE. Le radical d'une algèbre quelconque.

1. Modules sur une algèbre.

Soit C un anneau commutatif à élément unité, A une algèbre sur C pouvant ou non posséder un élément unité. On appelle module à gauche sur l'algèbre A un groupe abélien E muni d'une structure de bimodule à gauche par rapport à A et C telle que la structure de C-module sous-jacente soit unitaire.

Autrement dit, si l'on note multiplicativement les deux structures de modules, on a les identités :

$a.(x+y) = a.x + a.y$, $\lambda.(x+y) = \lambda.x + \lambda.y$, $a \in A$, $\lambda \in C$, $x,y \in E$,

$(a+b).x = a.x + b.x$, $(\lambda+\mu).x = \lambda.x + \mu.x$, $a,b \in A$, $\lambda,\mu \in C$, $x \in E$,

$a.(b.x) = (ab).x$, $\lambda.(\mu.x) = (\lambda\mu).x$, $a.(\lambda.x) = (\lambda a).x$ $\left\{ \begin{array}{l} a,b \in A, \lambda,\mu \in C \\ x \in E \end{array} \right.$

$1.x = x$, $x \in E$, 1 étant l'élément unité de C .

Conformément aux définitions générales, un sous-groupe F de E est dit un sous-module si c'est un sous-module à la fois pour la structure de A-module et de C-module. Un module E est dit simple s'il est différent de (0) et si ses seuls sous-modules sont (0) et E) ; il est dit semi-simple s'il est somme directe de modules simples.

Lorsque l'algèbre A possède un élément unité e , et que l'on suppose que E est un A-module unitaire, on a pour tout $\lambda \in C$:

$$\lambda.x = \lambda.(e.x) = (\lambda e).x \ ,$$

ce qui montre que la structure de C-module de E est déterminée entièrement par la structure de A-module, et il n'y a plus de distinction à faire entre modules sur l'algèbre A et modules sur l'anneau A .

Si l'on ne suppose pas E unitaire, on peut écrire, pour tout $x \in E$: $x = e.x + (x-e.x)$. L'ensemble des $e.x$, $x \in E$, forme un sous-module E' de E l'ensemble des $x-e.x$ forme un sous-module E" ; E est somme directe de E' et de E" ; E' est un A-module unitaire, alors que E" est un A-module trivial : on a $a.x = 0$ si $a \in A$ et $x \in E"$.

2. Le radical d'une algèbre.

Soit A une algèbre sur C . On appelle radical de l'algèbre A l'intersection des annulateurs des modules simples sur l'algèbre A .

Une algèbre semi-primitive est une algèbre dont le radical est (0). On voit comme au § 2, n°1 que pour qu'une algèbre A soit semi-primitive il faut et il suffit qu'il existe un module semi-simple et fidèle sur l'algèbre A .

Lorsque A possède un élément unité cette nouvelle définition du radical est en accord avec celle du § 2 (ceci montre que le radical de A ne dépend que de la structure d'anneau de A , et pas de sa structure d'algèbre Il faudrait s'assurer que ce n'est pas toujours vrai si A n'a pas d'élément unité !). En effet, il est évident, d'une part, que tout module unitaire sur l'anneau A qui est simple au sens du § 1 est aussi un module simple sur l'algèbre A ; d'autre part, il résulte de la décomposition en somme directe $E = E' + E$ donnée plus haut que tout module simple sur l'algèbre A est, soit unitaire, soit trivial. Comme dans le dernier cas son annulateur est A tout entier, notre assertion est démontrée.

3. Adjonction d'un élément unité.

Soit A une algèbre sur l'anneau commutatif C . Sur l'ensemble $A' = C \times A$, définissons les lois de composition suivantes :

$$(\lambda, a) + (\mu, b) = (\lambda + \mu, a + b)$$

$$(\lambda, a).(\mu, b) = (\lambda\mu,\ ab + \mu a + \lambda b)$$

$$\lambda.(\mu, a) = (\lambda\mu, \lambda a) .$$

On vérifie aussitôt que ces trois lois définissent sur A' une structure d'algèbre sur C dont l'élément (1,0) est l'élément unité ; l'ensemble $\{0\} \times A$ est un idéal bilatère de A' isomorphe à A en tant qu'algèbre sur C.

Soit E un module sur l'algèbre A , et posons :

$$(\lambda, a).x = \lambda.x + a.x \qquad \text{si} \quad \lambda \in C\ ,\ a \in A\ ,\ x \in E\ .$$

On vérifie aussitôt que cette loi de composition munit E d'une structure de module unitaire sur l'anneau A' ; par restriction de l'anneau

d'opérateurs à A et C on retrouve les structures de A-module et de C-module de E . Inversement, la donnée d'un A'-module unitaire définit sans ambiguïté un module sur l'algèbre A, ce qui montre l'équivalence des deux notions. En particulier, " E est un module simple sur l'algèbre A" $\Leftrightarrow$ "E est un A'-module simple" . Il s'ensuit que le radical R de A est l'intersection de A avec le radical R' de A', ce qui va nous permettre de déterminer le radical de A en utilisant les résultats du § 2 .

Pour cela, soit (1,a) un élément de A' et cherchons si (1,a) possède un inverse à gauche (λ,x), $\lambda \in C$, $x \in A$. On doit avoir $\lambda \cdot 1 = 1$ d'où $\lambda = 1$, et $a + x + x.a = 0$. Si nous appelons conversible à gauche tout élément $a \in A$ tel qu'il existe $x \in A$ avec $a + x + x.a = 0$, nous voyons que a doit être conversible à gauche.

THEOREME 1. Pour que $a \in A$ appartienne au radical R de l'algèbre A , il faut et il suffit que $ba + \lambda a$ soit conversible à gauche quels que soient $b \in A$ et $\lambda \in C$. Dans ces conditions $ba + \lambda a$ et $ab + \lambda a$ sont conversibles à droite et à gauche.

En effet, pour que $a \in A$ appartienne à R , il faut et il suffit que $(0,a) \in R'$, c'est-à-dire, d'après le th.1 du § 2, que l'élément $1 - (\lambda,b).(0,a)$ soit inversible à gauche quel que soit $(\lambda,b) \in A'$. Comme $1-(\lambda,b).(0,a) = (1, ba + \lambda a)$, il est donc nécessaire et suffisant que $ba + \lambda a$ soit conversible à gauche.

La seconde partie du théorème se prouve de même, en utilisant le cor.1 au th.1 du § 2 .

COROLLAIRE. Le radical d'une algèbre est identique au radical de l'algèbre opposée.

Remarque. Si A possède un élément unité e , dire que $e + a$ $(a \in A)$ est inversible à gauche dans A équivaut à dire que a est conversible à gauche. La condition du théorème précédent est donc équivalente à celle du th.1 du § 2, ce qui montre à nouveau que le radical de l'algèbre A est identique au radical de l'anneau A tel qu'il a été défini au § 2 .