ALGEBRE
CHAPITRE IX
ANNEAUX PRIMITIFS (ETAT 2)

Rédaction n° 092

Nombre de pages : 46

Nombre de feuilles : 46

A 92 2

N. Bourbaki

ALGÈBRE.

CHAPITRE IX

ANNEAUX PRIMITIFS (Etat 2).

Commentaire.

Etant donné qu'il s'agit d'un état 2, le rédacteur a pris une liberté avec le plan adopté à Strasbourg ; il a voulu séparer l'étude des anneaux au moyen de leurs modules (§ 1) (et en déduit immédiatement le lemme de Schur et le th. de densité), - de leur étude interne (§ 2) (radical, idéaux primitifs). Il a ajouté, au § 1, les propriétés des modules complètement réductibles (chassés du chap.II) qui lui ont été nécessaires.

A la place du mot "régulier" ("idéaux réguliers" de Segal-Godement) il a adopté le mot "unitaire" qui veut dire quelque chose. Malgré l'emploi au chap.II du mot "module normal", qui ne veut rien dire, il a systématiquement parlé de "modules fidèles", ce qui est aussi plus conforme à la terminologie usuelle.

Au moyen des éléments primordiaux il a donné, au § 4, une condition nécessaire et suffisante de semi-primitivité du produit tensoriel de deux corps commutatifs, ce qui n'était pas fait dans l'état 1 . La propriété "$K \otimes K'$ est une algèbre de matrices sur le centre de K ", démontrée élémentairement, a été transférée au § des produits tensoriels ; on l'a fait suivre de la définition du groupe de Brauer. On a également donné la définition et une caractérisation, presqu'évidente, des algèbres séparables ; mais, après étude des mémoires de Hochschild, le rédacteur a jugé que leur caractérisation au moyen des dérivations, c'est-à-dire de la cohomologie, sortait par trop du cadre de ce chapitre ; il tient à la disposition de Bourbaki une démonstration assez simple du cas commutatif.

Le § 5 (isomorphismes) suit de près les idées du mémoire de Dieudonné

Quant au § 6 (représentations linéaires des groupes et algèbres) il a conformément aux décisions de Strasbourg, été réduit à sa plus primitive expression.

P l a n

Les anneaux considérés dans ce chapitre ne seront, sauf mention expresse du contraire, soumis à aucune restriction, que ce soit de Commutativité ou d'existence d'un élément unité. Sauf mention expresse du contraire nous laisserons au lecteur le soin de traduire en termes d'idéaux à droite les considérations relatives aux idéaux à gauche ; à cet effet, et à titre de prime, des miroirs seront distribués. Lorsque des considérations seront faites sur des idéaux sans spécification d'espèce, elles se rapporteront aussi bien à des idéaux à gauche, qu'à des idéaux à droite ou bilatères.

§ 1 - Anneaux primitifs et semi-primitifs ; étude externe.

1)- Sommes, produits et intersections d'idéaux.

Soit A un anneau ; rappelons que l'intersection $\bigcap_\alpha \mathfrak{a}_\alpha$ d'une famille $\mathfrak{a}_\alpha$ ($\alpha \in \Lambda$) d'idéaux de A est un idéal de A ; d'autre part le plus petit idéal contenant tous les idéaux $\mathfrak{a}_\alpha$ est l'idéal somme $\sum_\alpha \mathfrak{a}_\alpha$, ensemble des sommes $\sum_\alpha a_\alpha$, où $a_\alpha \in \mathfrak{a}_\alpha$ et $a_\alpha = 0$

sauf pour un nombre fini d'indices. Il est clair que l'on a les inclusions suivantes :

(1) $\mathfrak{a} \cap (b+b') \supset (\mathfrak{a} \cap b) + (\mathfrak{a} \cap b')$

(2) $\mathfrak{a} + (b \cap b') \subset (\mathfrak{a} + b) \cap (\mathfrak{a} + b')$

L'égalité des deux membres dans (1) et (2) n'est pas toujours vraie (cf. exercice 1).

Définition 1 - Soient B et B' deux sous groupes du groupe additif sous-jacent de l'anneau A ; nous noterons BB' l'ensemble des sommes $\sum_{i=1}^{n} b_i b'_i$ où $b_i \in B$ et $b'_i \in B'$.

Il est clair que BB' est un sous groupe additif de A ; si B est un idéal à gauche, BB' est un idéal à gauche ; si, de plus, B' est un idéal à droite, BB' est un idéal bilatère. On vérifie aussitôt les relations suivantes :

(3) $bb' \subset b \cap b'$ lorsque b est un idéal à droite, et b' un idéal à gauche.

(4) $b + cc' \supset (b+c)(b+c')$ si b est un idéal bilatère.

(5) $B(C + C') = BC + BC'$.

(6) $(BC)D = B(CD)$.

L'égalité des deux membres des formules (3) et (4) n'est pas toujours vraie (cf. exercices).

Nous noterons b^n et appellerons n-ème puissance de b le produit de n idéaux égaux à b ; on a évidemment $b^{n+1} \subset b^n$. Si $b^2 = b$ on dit que b est un idéal idempotent ; s'il existe $n > 0$ tel que $b^n = (0)$ on dira que b est un idéal nilpotent.

Il n'est pas vrai qu'un idéal dont tous les éléments sont nilpotents (un "nilidéal") soit nilpotent (cf. exercice).

2)- Modules simples, semi-simples, complètement réductibles.

Soit A un anneau, E un groupe abélien sans opérateurs ; définir sur E une structure de A-module (chap.II, § 1, n°1) à gauche, équivaut

à se donner un homomorphisme φ de A dans l'anneau $\mathcal{L}(E)$ des endomorphismes du groupe abélien E ; de même définir sur E une structure de A-module à droite revient à se donner un homomorphisme dans $\mathcal{L}(E)$ de l'anneau A' opposé de A . Nous ne parlerons plus que de modules à gauche ; et, sauf mention expresse du contraire, nous exclurons les modules tels que $\varphi(A) = (0)$ (modules "triviaux").

Soit A un anneau, E et E' deux A-modules à gauche, φ et φ' les homomorphismes de A dans $\mathcal{L}(E)$ et $\mathcal{L}(E')$ respectivement ; nous dirons que E et E' sont deux modules isomorphes s'il existe un isomorphisme Ψ de E sur E', considérés comme groupes abéliens, tel que $\varphi'(a).\Psi(x) = \Psi(\varphi(a).x)$ pour tous $a \in A$, $x \in E$.

Soit E un A-module ; nous noterons en général les éléments de A par des minuscules latines du début de l'alphabet (a,b,c,...), ceux de E par des minuscules latines de la fin de l'alphabet (x,y,z,...).

Définition 2 - On dit qu'un A-module E est simple s'il ne possède d'autres sous-modules que lui-même et $\{0\}$; un A-module est dit complètement réductible s'il est somme directe de modules simples ; il est dit semi-simple s'il est somme directe d'un nombre fini de modules simples.

On en déduit immédiatement :

Proposition 1 - Tout module simple non trivial est monogène et engendré par n'importe lequel de ses éléments non nuls.

Proposition 2 - Si un A-module E est somme d'une famille (E_λ) $(\lambda \in \Lambda)$ de modules simples, il est complètement réductible et somme directe d'une sous-famille (E_ι) $(\iota \in I)$ de la famille (E_λ).

Soit $\mathcal{F}$ l'ensemble des parties J de Λ telles que $\sum_{\lambda \in J} E_\lambda$ soit une somme directe ; $\mathcal{F}$ n'est pas vide puisqu'il contient $\emptyset$ et toute partie de Λ réduite à un élément ; ordonné par inclusion $\mathcal{F}$ est un

un ensemble ordonné inductif (ens. R,) ; il possède donc un élément maximal I , d'après le th. de Zorn. Soit $E' = \sum_{\lambda \in I} E$; pour tout $\lambda_o \in \Lambda$ on a $E_{\lambda_o} \subset E'$, sinon $E_{\lambda_o} \cap E'$ serait un sous-module du module simple E_{λ_o} différent de E_{λ_o} ; alors on aurait $E_{\lambda_o} \cap E' = \{0\}$; donc $E' + E_{\lambda_o}$ serait une somme directe contrairement à la maximalité de I . Par conséquent $E' = E$.

Si Λ est un ensemble fini, la prop.1 prouve que E est un module semi-simple.

Proposition 3 - Tout sous-module F d'un module complètement réductible est complètement réductible et admet un supplémentaire.

Soit (E_λ) $(\lambda \in \Lambda)$ l'ensemble des sous-modules simples de E ; pour tout $\lambda \in \Lambda$, $E_\lambda \cap F$ est un sous-module de E_λ , donc est égal à E ou à $\{0\}$. Soit I (resp. J) l'ensemble des $\lambda \in \Lambda$ tels que $E_\lambda \cap F = E_\lambda$ (resp. $E_\lambda \cap F = \{0\}$) ; on a $I \cup J = \Lambda$, $I \cap J = \emptyset$. Au moyen du th. de Zorn nous extrayons de J une sous-famille maximale J' telle que $(\sum_{\lambda \in J'} E_\lambda) \cap F = \{0\}$; soit $F' = \sum_{\lambda \in J'} E_\lambda$; pour tout $\lambda_o \in \Lambda$ on a $E_{\lambda_o} \subset F + F'$, sinon $F + F' + E_{\lambda_o}$ serait une somme directe. Donc $F + F' = E$, et F' est supplémentaire de F . Ce supplémentaire est complètement réductible (prop.2). De même F' admet un supplémentaire complètement réductible F" ; comme celui-ci est isomorphe à F, F est complètement réductible.

3) - Annulateurs ; anneaux primitifs et semi-primitifs ; radical.

Soit E un A-module, D une partie quelconque de E ; on appelle annulateur de D et on note $\mathscr{A}(D)$ l'ensemble des $a \in A$ tels que $ax=0$ pour tout $x \in D$; il est clair que $\mathscr{A}(D)$ est un idéal à gauche de A . Si D est la partie $\{x\}$ réduite à un élément $x \in E$, l'annulateur de D se note $\mathscr{A}(x)$. Si $D = \bigcup_{\lambda \in \Lambda} D_\lambda$, alors $\mathscr{A}(D) = \bigcap_{\lambda \in \Lambda} \mathscr{A}(D_\lambda)$.

Lorsque D est un sous-module de E, son annulateur $\mathfrak{a}(D)$ est un idéal bilatère, car, si $a \in \mathfrak{a}(D)$, si $b \in A$, et si $x \in D$, alors $bx \in D$ et $(ab)x = a(bx) = 0$. En particulier l'annulateur du module E lui-même est un idéal bilatère $\mathfrak{a}(E)$ que l'on appelle le noyau du module E. Lorsque $\mathfrak{a}(E) = (0)$, on dit que E est un module fidèle.

Remarquons qu'en général le groupe abélien sous-jacent de E peut être muni d'une structure de $A/\mathfrak{a}(E)$-module ; muni de cette structure c'est un module fidèle.

Le but de ce chapitre est d'étudier certaines classes d'anneaux au moyen de modules sur ces anneaux :

Définition 3 - On dit qu'un anneau A est primitif s'il possède un A-module simple et fidèle ; un anneau A est dit semi-primitif s'il possède un A-module semi-simple et fidèle. On appelle radical de l'anneau A l'intersection des annulateurs des A-modules simples ; A est dit sans radical si son radical est réduit à (0).

Proposition 4 - Le radical d'un anneau A est un idéal bilatère.

Proposition 5 - Un anneau semi-primitif A est composé direct d'anneaux primitifs.

Soit $E = \sum_{i=1}^{n} E_i$ un A-module semi-simple et fidèle, les E_i étant des modules simples, et la somme étant directe. Soit $\mathfrak{a}_i$ l'idéal bilatère de A annulateur du sous module E_i ; par définition $A/\mathfrak{a}_i$ est un anneau primitif. On a $\bigcap_{i=1}^{n} \mathfrak{a}_i = (0)$; nous supposerons que $(\mathfrak{a}_i)_{1 \leqslant i \leqslant n}$ est une famille minimale d'idéaux ayant ces propriétés. Pour tout $a \in A$ soit $\varphi_i(a)$ la classe de a mod. $\mathfrak{a}_i$. L'application φ $a \longrightarrow (\varphi_i(a))_n$ est un homomorphisme de A dans $A' = \prod_{i=1}^{n} A/\mathfrak{a}_i$; puisque $\bigcap_{i=1}^{n} \mathfrak{a}_i = (0)$, φ est un isomorphisme. Il nous reste à montrer que φ est un isomorphisme sur ; pour cela il nous suffira de montrer que les axes de coordonnées $A/\mathfrak{a}_i$ appartiennent à $\varphi(A)$;

soit donc $a \in A/\mathfrak{a}_i$, $x \neq 0$ un élément de E , et $y = ax$ (E étant considéré comme $A/\mathfrak{a}_i$-module) ; considérons $b_i = \bigcap_{j \neq i} \mathfrak{a}_j$; b_i est $\neq (0)$ par hypothèse ; $b_i x$ est un sous-module de E_i , évidemment égal à E_i ; il existe donc $b \in b_i$ tel que $y = bx$; donc $\varphi_i(b) = a$, car, de $(\varphi_i(b)-a)x = 0$, on déduit $(\varphi_i(b)-a)E_i = 0$; et comme $\varphi_j(b)=0$ pour $j \neq i$, on a $\varphi(b) = a$,.

Proposition 6 - Tout idéal bilatère non nul $\mathfrak{a}$ d'un anneau primitif A est un anneau primitif.

Soit en effet E un A-module simple et fidèle. Pour tout $x \in E$, $\mathfrak{a}x$ est un sous-module de E ; l'ensemble des $x \in E$ tels que $\mathfrak{a}x = \{0\}$ est un sous-module F de E puisque $\mathfrak{a}$ est bilatère. On ne peut avoir $F = E$ puisque E est fidèle et que $\mathfrak{a} \neq (0)$. Donc, pour tout $x \neq 0$ dans E , on a $\mathfrak{a}x = E$, ce qui montre que E est un $\mathfrak{a}$-module simple ; et il est clair que E est un $\mathfrak{a}$-module fidèle.

4) - Structure des anneaux primitifs.

Soit E un A-module, $\mathcal{L}(E)$ l'anneau des endomorphismes du groupe abélien sous-jacent de E , φ l'homomorphisme canonique de A dans $\mathcal{L}(E)$. Rappelons qu'il revient au même de dire que φ est un isomorphisme, et de dire que E est un module fidèle.

L'ensemble A' des éléments $a \in \mathcal{L}(E)$ qui permutent avec tout élément de $\varphi(A)$ est un sous-anneau de $\mathcal{L}(E)$ qu'on appelle le commutant de $\varphi(A)$ (ou de A par abus de langage). L'ensemble des éléments de $\mathcal{L}(E)$ permutables avec tout élément de A' est un sous-anneau A" de $\mathcal{L}(E)$ qu'on appelle l'anticommutant de A ; il est clair que $\varphi(A) \subset A"$.

Théorème 1 (lemme de Schur) - Le commutant A' d'un A-module simple E est un corps K .

Il nous suffit de montrer que tout élément $a \neq 0$ de A' admet un inverse dans $\mathcal{L}(E)$, c'est-à-dire que a est un automorphisme du groupe

abélien sous-jacent de E . Il est clair que $a(E)$ est un sous A-module de E ; puisque $a \neq 0$, on a $a(E)=E$. D'autre part $a^{-1}(\{0\})$ est aussi un sous A-module de E ; puisque $a \neq 0$, on a $a^{-1}(\{0\}) \neq E$, donc $a^{-1}(\{0\}) = \{0\}$. Ceci prouve que a est un automorphisme.

Soit $\mathfrak{a}$ un idéal à gauche de A , non contenu dans le noyau de E . Soit $x \in E$ tel que $\mathfrak{a}x \neq \{0\}$; on a alors $\mathfrak{a}x = E$ puisque $\mathfrak{a}x$ est un sous-module de E . Soit $a \in \mathcal{L}(E)$ permutable à tout élément de $\varphi(\mathfrak{a})$; pour tous $a \in \mathfrak{a}$, $b \in A$, on a :

$$a\,\varphi(b)\,\varphi(a) = a\,\varphi(ba) = \varphi(ba)a = \varphi(b)\varphi(a)a = \varphi(b)\,a\,\varphi(a)$$

Donc $(a\,\varphi(b)-\varphi(b)a)ax = 0$, $(a\,\varphi(b)-\varphi(b)a)E = 0$; par conséquent $a \in A'$, et le commutant de $\mathfrak{a}$ est identique à A' .

Le lemme de Schur nous montre donc que E a une structure d'espace vectoriel (à gauche) sur K ; nous noterons E_K le groupe E muni de cette structure. Son anticommutant A'' est donc l'anneau de tous les endomorphismes de E_K , anneau dont la structure est bien connue (cf. §3, n° 4) .

Lorsque E est un module fidèle, A peut être considéré comme un sous-anneau de A'' ; le théorème suivant va donner quelques indications sur l'inclusion de A dans A'' :

Théorème 2 (théorème de densité) - Soient A un anneau primitif, E un A-module simple et fidèle, K et A'' le commutant et l'anticommutant de A ; quels que soient $a \in A''$ et les éléments $x_1, \ldots, x_n$ de E en nombre fini, il existe $a \in A$ tel que $ax_i = ax_i$ $(1 \leqslant i \leqslant n)$.

Considérons le A-module produit E^n ; soient E_i le i-ème axe de coordonnées de E^n , π_i la projection de E^n sur E_i , φ_i l'application canonique de E sur E_i . Soient B' et B'' le commutant et l'anticommutant de A relatifs au module E^n . Il est clair que la condition nécessaire et suffisante pour que l'endomorphisme β du groupe additif de E^n

appartienne à B' est que tous les $\beta_{ij} = \varphi_i^{-1} \circ \pi_i \circ \beta \circ \varphi_j$ soient éléments de K . Donc l'endomorphisme $\overline{a}$ de E^n défini par $\overline{a}(y_1,\dots,y_n) = (a\,y_1,\dots,a\,y_n)$ est élément de l'anticommutant B" , puisque $a \in A$" . Soient maintenant $X = (x_1,..,x_1) \in E^n$, F_1 le sous-module AX , F_2 un supplémentaire de F (prop.3) ; les projections de E^n sur F_1 et F_2 appartiennent à B' , en sorte que B" conserve F_1 et F_2 . En particulier $\overline{a}X \in AX$, et il existe $a \in A$ tel que $ax_1 = ax_i$ pour $1 \leqslant i \leqslant n$.

Corollaire - Les notations étant les mêmes que dans le th.2, étant donnés n éléments $y_1,\dots,y_n$ de E , linéairement indépendants sur K , et n éléments arbitraires $z_1,\dots,z_n$ de E , il existe $a \in A$ tel que $ay_1 = z_i$ pour $1 \leqslant i \leqslant n$.

En effet il existe un endomorphisme a de E_K tel que $ay_i = z_i$.

§ 2 - Etude interne des anneaux primitifs. Le radical d'un anneau.

Nous venons d'étudier les anneaux primitifs au moyen de modules sur ces anneaux. Nous nous proposons maintenant d'étudier ces anneaux au moyen de considérations qui ne nous ferons pas sortir de l'anneau étudié.

1) - Modules internes. Idéaux unitaires.

Soit A un anneau, $\mathfrak{a}$ un idéal à gauche de A ; le groupe quotient $A/\mathfrak{a}$ est muni d'une structure de A-module à gauche ; muni de cette structure $A/\mathfrak{a}$ sera appelé un module interne de A .

Proposition 1 - Tout A-module monogène E est isomorphe à un A-module interne.

Soit $x \in E$ tel que $E = Ax$, et soit $\mathfrak{a}(x)$ l'annulateur de x dans A . Pour tout $y \in E$ on peut écrire $y = a_y x$ avec $a \in A$, et a_y est déterminé mod. $\mathfrak{a}(x)$; donc la classe $\varphi(y) = a_y + \mathfrak{a}(x)$ est bien déterminée et φ est évidemment l'isomorphisme cherché de E sur $A/\mathfrak{a}(x)$.

Remarquons que l'idéal $\mathfrak{a}(x)$ n'est pas en général déterminé de façon unique par E . Remarquons aussi qu'il existe un élément e de A tel que $x = ex$; donc, pour tout $a \in A$, on a $ax = aex$; donc $a - ae \in \mathfrak{a}(x)$; e est donc une unité à droite mod. $\mathfrak{a}(x)$. Nous poserons en général la définition suivante :

Définition 1 - On dit qu'un idéal à gauche $\mathfrak{a} \subset A$ est unitaire, s'il existe une unité à droite e mod. $\mathfrak{a}$, c'est-à-dire si, pour tout $a \in A$, on a $ae - a \in \mathfrak{a}$.

Il revient évidemment au même de dire que le module interne $A/\mathfrak{a}$ est monogène et engendré par la classe $e + \mathfrak{a}$.

Remarques.- 1)- Si A admet un élément unité, tout idéal à gauche est unitaire.

2)- Tout idéal à gauche contenant un idéal unitaire est unitaire.

3)- Si $\mathfrak{a}$ est un idéal bilatère et unitaire en tant qu'idéal à gauche et à droite, $A/\mathfrak{a}$ est un anneau ayant un élément unité.

Si $\mathfrak{a}$ est un idéal à gauche quelconque de A , le noyau $\mathring{\mathfrak{a}}$ du module interne $A/\mathfrak{a}$ est appelé le noyau de l'idéal $\mathfrak{a}$.

Proposition 2 - Le noyau d'un idéal à gauche unitaire $\mathfrak{a} \subset A$ est le plus grand idéal bilatère contenu dans $\mathfrak{a}$.

$\mathring{\mathfrak{a}}$ est l'ensemble des $b \in A$ tels que $bA \subset \mathfrak{a}$. Soit e une unité à droite mod. $\mathfrak{a}$. Pour tout $b \in \mathring{\mathfrak{a}}$, on a $be \in \mathfrak{a}$ et $be - b \in \mathfrak{a}$, donc $b \in \mathfrak{a}$ et $\mathring{\mathfrak{a}} \subset \mathfrak{a}$. Si d'autre part $\mathfrak{b}$ est un idéal à droite contenu dans $\mathfrak{a}$, on a $\mathfrak{b}A \subset \mathfrak{b} \subset \mathfrak{a}$; donc $\mathfrak{b} \subset \mathring{\mathfrak{a}}$.

Nous avons même démontré que $\mathring{\mathfrak{a}}$ est le plus grand idéal à droite contenu dans $\mathfrak{a}$.

2)- Idéaux maximaux. Idéaux primitifs.

Rappelons que les sous-modules du module interne $A/\mathfrak{a}$ sont de la forme $\mathfrak{b}/\mathfrak{a}$ où $\mathfrak{b}$ est un idéal à gauche de A contenant $\mathfrak{a}$. Donc la condition nécessaire et suffisante pour que $A/\mathfrak{a}$ soit un module simple est que $\mathfrak{a}$ soit un idéal à gauche maximal(*). Deux cas peuvent se présenter : ou bien $A/\mathfrak{a}$ n'est pas un module trivial, et alors il est engendré par l'un quelconque de ses éléments non nuls, -ou bien $A/\mathfrak{a}$ est un groupe abélien simple annulé par A, ce qui veut dire que $A^2 \subset \mathfrak{a}$. Donc :

Proposition 3 - Tout idéal à gauche maximal $\mathfrak{a}$ qui ne contient pas l'idéal bilatère A^2 est unitaire.

Nous ne considèrerons plus dans ce § que des idéaux à gauche maximaux unitaires ; la prop.3 montre que tout idéal à gauche unitaire maximal est un idéal à gauche maximal.

Le noyau $\mathring{\mathfrak{a}}$ d'un idéal à gauche unitaire maximal est donc tel que l'anneau quotient $A/\mathring{\mathfrak{a}}$ soit primitif ; on dit alors que l'idéal bilatère $\mathring{\mathfrak{a}}$ est primitif. Réciproquement tout idéal bilatère primitif $\mathfrak{b}$ est le noyau d'un idéal à gauche unitaire maximal, car un $A/\mathfrak{b}$ - module simple et fidèle est isomorphe (prop.1) à un $A/\mathfrak{b}$ - module interne $A/\mathfrak{a}$ où $\mathfrak{a}$ est un idéal à gauche unitaire maximal contenant $\mathfrak{b}$.

Proposition 4 - (lemme de Segal) - Tout idéal à gauche $\mathfrak{a} \neq A$ (resp. bilatère) unitaire est contenu dans au moins un idéal à gauche (resp. bilatère) maximal unitaire.

(*) Dans tout ce chapitre l'épithète maximal se rapportera exclusivement aux épithètes qui le précèdent : ainsi un idéal à gauche maximal bilatère est maximal dans la famille des idéaux à gauche, et se trouve être bilatère ; tandis qu'un idéal bilatère maximal n'est maximal que dans la famille des idéaux bilatères.

Soit en effet e une unité à droite mod. $\mathfrak{a}$; il est clair que e est aussi une unité à droite mod. $\mathfrak{a}'$ pour tout idéal à gauche $\mathfrak{a}' \supset \mathfrak{a}$; si $\mathfrak{a}' \neq A$, on a $e \notin \mathfrak{a}'$, car, sinon, on aurait, pour tout $a \in A$, $ae \in \mathfrak{a}'$, d'où $a = ae-(ae-a) \in \mathfrak{a}'$. La prop.4 s'obtient alors en appliquant le th. de Zorn à la famille des idéaux à gauche contenant $\mathfrak{a}$ et ne contenant pas e .

Proposition 5 - Tout idéal bilatère maximal et unitaire $\mathfrak{b}$ de A est primitif.

En effet $\mathfrak{b}$ est contenu dans au moins un idéal à gauche maximal et unitaire $\mathfrak{a}$; et on a $\mathfrak{b} \subset \mathring{\mathfrak{a}} \subset \mathfrak{a}$ (prop.2) ; d'où $\mathfrak{b} = \mathring{\mathfrak{a}}$.

En particulier tout anneau simple A (c'est à dire sans idéaux bilatères non triviaux) et tel que $A^2 \neq \{0\}$ (alors $A^2 = A$) est primitif.

Soit maintenant $\mathfrak{b}$ un idéal bilatère primitif de A ; c'est l'annulateur d'un A-module simple E ; pour tout $x \in E$, $x \neq 0$, l'annulateur $\mathfrak{a}(x)$ est un idéal à gauche maximal unitaire, et E est isomorphe au module interne $A/\mathfrak{a}(x)$ (prop.1) ; donc $\mathfrak{b} = \bigcap_{x \in E, x \neq 0} \mathfrak{a}(x)$. Ceci nous amène donc à énoncer la proposition suivante :

Proposition 6 - Tout idéal bilatère primitif est l'intersection des idéaux à gauche maximaux qui le contiennent ; c'est aussi l'intersection des idéaux à droite maximaux unitaires qui le contiennent.

La première partie est déjà démontrée. Pour démontrer la seconde nous passerons aux quotients et démontrerons le lemme suivant :

Lemme - Soit A un anneau primitif ; l'intersection des idéaux à droite maximaux unitaires de A est réduite à (0) .

Soit $\mathfrak{b}$ l'intersection des idéaux à droite maximaux unitaires de A ; d'après la première partie de la prop.6 , appliquée aux idéaux à droite, $\mathfrak{b}$ est un idéal bilatère. Soit E un A-module simple et fidèle ;

A est un sous-anneau de l'anneau d'endomorphismes $\mathcal{L}(E)$. Je dis que pour tout $b \in \mathfrak{b}$, l'endomorphisme $b+1$ de E est inversible :

a) Les $bc + c$ ($c \in A$) forment tout A ; sinon ils constitueraient un idéal à droite $\mathfrak{a} \neq A$; $-b$ est évidemment une unité à gauche mod. $\mathfrak{a}$, et $\mathfrak{a}$ est unitaire ; il existe alors un idéal à droite maximal unitaire $\mathfrak{m}$ contenant $\mathfrak{a}$ (prop.4) ; on a $b \in \mathfrak{b} \subset \mathfrak{m}$, donc $-b \in \mathfrak{m}$, contrairement au fait que c'est une unité à gauche mod. $\mathfrak{m}$.

b) En particulier il existe $c \in A$ tel que $bc + c = -b$; donc $(b + 1)(c + 1) = 1$: $b + 1$ est inversible à droite, et $c + 1$ est inversible à gauche.

c) Mais, puisque $c = -b-bc$, et que $\mathfrak{b}$ est bilatère, on a $c \in \mathfrak{b}$. D'après b) $c + 1$ est donc inversible à droite ; comme il est inversible à gauche il est inversible, et admet $b + 1$ pour inverse.

Ceci étant, soit $b \in \mathfrak{b}$ et $x \in E$; je dis que $bx = 0$ (ce qui démontre le lemme puisque E est un module fidèle) ; sinon, E étant simple, il existerait $a \in A$ tel que $abx = -x$, en sorte que $ab + 1$ ne serait pas inversible, contrairement au fait que $ab \in \mathfrak{b}$.

3) - Le radical. Eléments inversibles.

D'après la déf. 3 (§ 1) le radical $\mathcal{R}$ de A est l'intersection des noyaux des idéaux bilatères primitifs de A ; c'est donc (prop.6) l'intersection des idéaux à gauche maximaux unitaires de A, et aussi l'intersection des idéaux à droite maximaux unitaires de A. Remarquons que la notion d'idéal primitif, déduite de celle de module à gauche, est une notion unilatère ; et, sans nos conventions générales, nous aurions dû parler d'anneaux et d'idéaux primitifs à gauche.

C'est d'ailleurs un problème non résolu que de montrer que tout anneau primitif à gauche est primitif à droite ; il semble probable que la question sera résolue par la négative.

Au contraire les considérations précédentes montrent que le radical peut être défini aussi bien au moyen des idéaux, ou modules, à gauche que des idéaux, ou modules à droite.

Soit maintenant $a \in A$; l'ensemble des éléments de la forme $ca + c$ ($c \in A$) est un idéal à gauche $\mathscr{R}_a$; $\mathscr{R}_a$ est unitaire puisque $-a$ est une unité à droite mod. $\mathscr{R}_a$; si donc $\mathscr{R}_a \neq A$, il existe un idéal à gauche maximal unitaire $\mathscr{M}$ contenant $\mathscr{R}_a$ (prop.4), et qui ne contient évidemment pas a. Donc $a \in \mathscr{R}$ implique que $\mathscr{R}_a = A$, donc que l'on ait $-a = ca + c$, c'est-à-dire qu'il existe $c \in A$ tel que :

$$a + c + ca = 0 \qquad (1).$$

Remarquons que, de $a + c + ca = 0$, et de l'analogue à droite $a + c' + ac' = 0$ on déduit $ac' + cc' + cac' = 0$ et $ca + cc' + cac' = 0$, d'où, par soustraction, $ca = ac'$, et par conséquent $c = c'$. Nous pouvons donc poser la définition suivante :

<u>Définition 2</u> - <u>On dit qu'un élément $a \in A$ est conversible à gauche s'il existe $c \in A$, appelé converse à gauche de a, tel que</u> $ca + a + c = 0$. <u>On dit que a est conversible s'il est à la fois conversible à gauche et à droite ; il possède alors un seul et même converse à gauche et à droite.</u>

Si A a un élément unité il revient au même de dire que a est conversible à gauche (resp. conversible), et de dire que $1 + a$ est inversible à gauche (resp. inversible).

Nous venons de voir que tout élément du radical $\mathscr{R}$ est conversible. Puisque $\mathscr{R}$ est un idéal bilatère tout élément $bab' + na$ ($b, b' \in A$, $n \in Z$) est conversible. Soit réciproquement a un élément de A tel que, pour tout $b \in A$ et tout $n \in Z$, l'élément $ba + na$ soit conversible ; considérons un A-module simple E ; si, pour $x \neq 0$, $x \in E$, on avait $ax \neq 0$, le module E serait engendré par ax ; d'où en particulier des éléments $b \in A$ et $n \in Z$ tels que $-x = bax + nax$; ainsi $\varphi(ba + na) + 1$

ne serait pas inversible dans $\mathcal{L}(E)$, contrairement au fait que $ba + na$ est conversible dans A ; donc $aE = \{0\}$ pour tout A-module simple E , et a (§ 1, déf. 3). Nous pouvons donc résumer les propriétés du radical :

Théorème 1 - Dans un anneau A , le radical $\mathcal{R}$ peut être caractérisé comme étant l'un des ensembles (égaux) suivants :

1) L'ensemble des $a \in A$ annulant tout A-module à gauche simple.

1a) L'ensemble des $a \in A$ annulant tout A-module à droite simple.

2) L'intersection des idéaux à gauche maximaux unitaires de A .

2a) L'intersection des idéaux à droite unitaires maximaux de A .

3) L'intersection des idéaux bilatères primitifs à gauche de A .

3a) L'intersection des idéaux bilatères primitifs à droite de A .

4) L'ensemble des $a \in A$ tels que, pour tous $b \in A$, $n \in Z$, $ba + na$ soit conversible.

4a) L'ensemble des $a \in A$ tels que, pour tous $b \in A$, $n \in Z$, $ab + na$ soit conversible.

Il est évident que le radical est un idéal centre-gauche.

§ 3) - Anneaux d'Artin.

1)- Le radical d'un anneau d'Artin.

Définition 1 - On dit qu'un anneau A est un anneau d'Artin (gauche) s'il satisfait à l'une des conditions équivalentes suivantes :

(A) - Tout ensemble 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 , on a $\mathfrak{a}_{n+1} = \mathfrak{a}_n$ à partir d'un certain rang.

Il est clair que (A) entraîne (A'). Supposons réciproquement (A') vérifié, et soit Φ un ensemble d'idéaux à gauche ; si Φ ne possèdait

pas d'élément minimal, on pourrait, par récurrence, trouver une suite infinie strictement décroissante d'idéaux appartenant à .

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

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

Proposition 1 - Dans un anneau quelconque tout élément nilpotent est conversible. Dans un anneau d'Artin tout élément du radical est nilpotent.

Soit a tel que $a^n = 0$; il est clair que $-a + a^2 - \dots (-1)^{n-1} a^{n-1}$ est converse à droite et à gauche de a . Soit a un élément d'un anneau d'Artin A ; la suite des idéaux (Aa^n) étant décroissante, on a $Aa^n = Aa^{n+1}$, d'où $a^n = -ba^{n+1}$; si a appartient au radical, ba est conversible et il existe $c \in A$ tel que $ba + c + cba = 0$; multipliant à droite par a^n on obtient $ba^{n+1} + ca^n + cba^{n+1} = ba^{n+1} - cba^{n+1} + cba^{n+1} = ba^{n+1} = 0$; d'où $a^n = 0$.

D'après le th.1, § 2 (4)) nous concluons donc que tout idéal à gauche dont tous les éléments sont nilpotents (tout "nilidéal à gauche") est contenu dans le radical, et que le radical lui-même est un nilidéal. Mais nous pouvons dire quelque chose de plus précis :

Théorème 1 (Hopkins) - Dans un anneau d'Artin A tout nilidéal à gauche $\mathfrak{a}$ est nilpotent. En particulier le radical d'un anneau d'Artin est le plus grand idéal nilpotent de A .

La suite d'idéaux $(\mathfrak{a}^n)$ étant décroissante, on a, à partir d'un certain rang, $\mathfrak{a}^n = \mathfrak{a}^{n+1} = \mathfrak{a}^{n+2} = \dots$; soit $\mathfrak{b} = \mathfrak{a}^n$. Supposons que $\mathfrak{b} \neq (0)$; considérons la famille Φ des idéaux à gauche $\mathfrak{n}$ tels que $\mathfrak{n} \subset \mathfrak{b}$ et que $\mathfrak{b}\mathfrak{n} \neq (0)$; Φ n'est pas vide car $\mathfrak{b}^2 = \mathfrak{b} \neq (0)$; considérons un élément minimal $\mathfrak{n}$ de Φ ; puisque $\mathfrak{b}^2\mathfrak{n} = \mathfrak{b}\mathfrak{n} \neq (0)$, on a $\mathfrak{b}\mathfrak{n} \in \Phi$, donc $\mathfrak{b}\mathfrak{n} = \mathfrak{n}$ étant donné que $\mathfrak{n}$ est minimal dans Φ.

Il existe donc $c \in \mathcal{N}$ tel que $\mathfrak{b}c \neq 0$; donc $\mathfrak{b}(Ac + Zc) \neq (0)$, et, puisque $\mathcal{N}$ est minimal dans Φ, $\mathcal{N} = Ac + Zc$. De $\mathcal{N} = \mathfrak{b}\mathcal{N}$ on déduit donc l'existence de $b \in \mathfrak{b}$ tel que $c = bc$; d'où $c = bc = b^2c = \ldots = b^nc$. Mais, $\mathfrak{b}$ étant un nilidéal, on a $b^q = 0$ pour q assez grand ; d'où $c = b^qc = 0$, en contradiction avec les hypothèses.

Remarque - Il n'est pas vrai que, dans tout anneau, le radical soit nilpotent, comme le montre l'exemple de l'anneau des séries formelles sur un corps, où le radical est l'ensemble des séries formelles sans terme constant.

2)- Anneaux d'Artin primitifs.

Proposition 2 - Si un anneau primitif A possède un idéal à gauche minimal $\mathfrak{l}$, tout A-module simple et fidèle est isomorphe à $\mathfrak{l}$.

D'après le th.1 aucun idéal de A n'est nilpotent ; donc, puisque $\mathfrak{l}^2 \subset \mathfrak{l}$, on a $\mathfrak{l}^2 = \mathfrak{l}$; il existe donc un élément e de $\mathfrak{l}$ tel que $\mathfrak{l}e \neq (0)$, donc tel que $\mathfrak{l}e = \mathfrak{l}$. Soit E un A-module simple et fidèle ; puisque $\mathfrak{l} \neq (0)$, le sous-module $\mathfrak{l}E$ est égal à E ; ainsi $E = \mathfrak{l}eE$, et il existe $x \in E$ tel que $\mathfrak{l}ex \neq (0)$, c'est-à-dire que $E = \mathfrak{l}ex$. Pour tout $y \in E$ on peut donc écrire $y = a_yex$ avec $a_y \in \mathfrak{l}$. Les éléments $b \in \mathfrak{l}$ tels que $bex = 0$ forment évidemment un idéal à gauche contenu dans $\mathfrak{l}$ et différent de $\mathfrak{l}$; donc $bex = 0$ implique $b = 0$, et par filtre l'élément $a_y \in \mathfrak{l}$ est déterminé de façon unique par $y = a_yex$. L'application $y \to a_y$ de E dans $\mathfrak{l}$ est donc un isomorphisme de E dans pour leurs structures de A-modules ; l'image de E étant un sous-module $\neq (0)$ de $\mathfrak{l}$, c'est $\mathfrak{l}$ lui-même, ce qui démontre la prop.2.

On connaît des exemples d'anneaux primitifs possédant plusieurs modules simples et fidèles non isomorphes.

Considérons toujours un anneau primitif A . Un A-module simple et fidèle E est muni d'une structure d'espace vectoriel (à gauche) sur le corps K commutant de A (§ 1, th.1). Soit (V_n) une suite strictement croissante, finie ou infinie, de sous-espaces vectoriels de dimension finie de E , et soit $\mathfrak{a}_n$ l'idéal à gauche de A annulateur de V_n . La suite $(\mathfrak{a}_n)$ est décroissante ; lorsque $V_{n'} \subset V_n$ et $V_{n'} \neq V_n$, il existe un élément $a \in A$ annulant $V_{n'}$ et transformant un vecteur $x \in V_n$, $x \notin V_{n'}$, en un vecteur $y \neq 0$ arbitrairement donné (cor. du th.2, § 1). Donc la suite (V_n) est strictement décroissante. Si nous supposons que A est un anneau d'Artin ceci montre que la suite (V_n) est finie, donc que E est de dimension finie sur K . D'après le cor. du th. de densité, nous voyons donc que A est isomorphe à l'anneau de tous les endomorphismes de l'espace vectoriel E . Par conséquent :

Théorème 2 (Wedderburn) - Tout anneau d'Artin primitif est isomorphe à un anneau $K'_{(n)}$ de matrices carrées de degré n sur un corps K' .

Il faut remarquer que le corps K' (commutatif ou non) du th.2 est l'opposé du corps K de la démonstration, car, d'après la définition des matrices (chap.II, §6), il faut considérer E comme module à droite ce que E est sur K' et non sur K .

3) - Anneaux d'Artin sans radical.

Proposition 3 - Dans un anneau d'Artin A le radical $\mathscr{R}$ est intersection d'un nombre fini d'idéaux primitifs.

Dans un anneau quelconque le radical est l'intersection $\bigcap_{\lambda \in \Lambda} \mathfrak{b}_\lambda$ de tous les idéaux bilatères primitifs. Pour toute sous-famille finie $F \subset \Lambda$ soit $\mathfrak{a}_F = \bigcap_{\lambda \in F} \mathfrak{b}_\lambda$. Supposons que A soit un anneau d'Artin (Il suffit d'ailleurs de supposer que A satisfait à la condition minimale pour les idéaux bilatères) ; il existe alors, dans l'ensemble des idéaux $\mathfrak{a}_F$, un idéal minimal $\mathfrak{a}_{F_o}$; et il est clair que $\mathfrak{a}_{F_o} = \mathscr{R}$.

Soit A un anneau d'Artin sans radical ; d'après la prop.3 il possède un module semi-simple et fidèle ; c'est donc un anneau semi-primitif, composé direct d'anneaux primitifs. Ces anneaux primitifs, étant isomorphes à des anneaux quotients de A , sont des anneaux d'Artin, et on a le théorème suivant :

Théorème 3 (Wedderburn) - Tout anneau d'Artin sans radical est isomorphe à un composé direct d'anneaux de matrices carrées sur des corps.

4) - Etude des anneaux d'endomorphismes d'espaces vectoriels.

Soit E un espace vectoriel à gauche de dimension n sur un corps K , commutatif ou non ; et soit A l'anneau des endomorphismes de l'espace vectoriel E . A est un module à gauche de dimension n^2 sur l'opposé K' de K ; c'est donc un anneau d'Artin. A est un anneau primitif, car E est un A-module simple et fidèle ; donc A ne possède pas d'idéaux nilpotents.

Proposition 4 - L'anneau A des endomorphismes d'un espace vectoriel E de dimension finie n sur un corps K est somme directe d'idéaux minimaux; il ne possède d'autres idéaux bilatères que lui-même et (0) (A est un anneau simple) .

Remarquons d'abord que, si l'on rapporte E à une base, les matrices dont toutes les colonnes sont nulles sauf celle d'indice j constituent un idéal à gauche $\mathfrak{a}_j$ de A , annulateur des éléments de la base sauf celui d'indice j . Puisque $\mathfrak{a}_j$ est de dimension n sur K' , c'est un idéal minimal (prop.2), ce qui démontre la première partie. Soit alors $\mathfrak{b}$ un idéal bilatère non trivial de A ; on ne peut avoir $\mathfrak{a}_j \cap \mathfrak{b} = \mathfrak{a}_j$ pour tout j , sinon $A = \mathfrak{b}$; donc il existe un idéal à gauche minimal $\mathfrak{a}_{j_0} = \mathfrak{l}$ tel que $\mathfrak{l} \cap \mathfrak{b} \neq \mathfrak{l}$; comme $\mathfrak{l}$ est minimal ceci implique que $\mathfrak{l} \cap \mathfrak{b} = (0)$. Comme A est un anneau d'Artin, $\mathfrak{b}$ contient un idéal à gauche minimal $\mathfrak{l}'$. Mais (prop.2) $\mathfrak{l}$ et $\mathfrak{l}'$ sont

isomorphes en tant que A-modules à gauche ; soit φ cet isomorphisme de $\mathfrak{r}$ sur $\mathfrak{r}'$; on a $\mathfrak{r}\mathfrak{r}' = \mathfrak{r}\varphi(\mathfrak{r}) = \varphi(\mathfrak{r}^2)$; mais $\mathfrak{r}^2 = \mathfrak{r}$ puisque $\mathfrak{r}$ n'est pas nilpotent ; donc $\mathfrak{r}\mathfrak{r}' = \mathfrak{r}' \neq (0)$. Mais $\mathfrak{r}\mathfrak{r}' \subset \mathfrak{r}\mathfrak{b} \subset \mathfrak{r} \cap \mathfrak{b} = \{0\}$ ce qui est absurde.

Proposition 5 - Le centre de l'anneau des endomorphismes A d'un espace vectoriel de dimension finie r sur un corps K , est un corps isomorphe au centre k de K .

Soient c_{ij} $(1 \leqslant i, j \leqslant n)$ les n^2 éléments matriciels de la base de A sur K' ; si $a = \sum_{i,j} a_{ij} c_{ij}$ est un élément du centre de A , on a en particulier $ac_{1h} = c_{1h}$ a pour tout indice h , ce qui donne $\sum_{i=1}^{n} a_{i1} c_{ih} = \sum_{j=1}^{n} a_{hj} c_{1j}$; d'où $a_{hj} = 0$ si $h \neq j$, $a_{hh} = a_{11}$ pour tout h , ce qui démontre la proposition.

Corollaire - Le centre d'un anneau d'Artin sans radical est composé direct d'un nombre fini de corps commutatifs.

Nous allons maintenant montrer une correspondance biunivoque entre les sous-espaces vectoriels de V et les idéaux à gauche de l'anneau d'endomorphismes A de V . Soit, plus généralement, E un module à gauche sur un anneau B , et $E = \sum_{i=1}^{n} E_i$ une décomposition de E en somme directe de sous-modules. Soit A l'anneau des endomorphismes du B-module E , c'est-à-dire le commutant de B dans l'anneau des endomorphismes du groupe abélien sous-jacent de E ; il est clair que les projections π_i de E sur E_i $(1 \leqslant i \leqslant n)$ appartiennent à A ; on a $\pi_i^2 = \pi_i$, $\pi_i \pi_j = 0$ si $i \neq j$, et $\sum_{i=1}^{n} \pi_i = 1$. Considérons les idéaux $A\pi_i$ de A ; A est la somme de ces idéaux à gauche ; je dis que cette somme est directe : en effet, de $0 = \sum_{i=1}^{n} a_i \pi_i$ $(a_i \in A)$, on déduit, par multiplication à droite par π_j , que $a_j \pi_j = 0$. De même A est somme directe des idéaux à droite $\pi_i A$. Les éléments de $A\pi_i$ sont caractérisés par la relation $a\pi_i = a(1)$; $A\pi_i$ est donc l'annulateur

du sous B-module $F_j = \sum_{i \neq j} E_i$: en effet $a = a\pi_i$ entraîne $a(F_i) = \{0\}$; si $a(F_i) = \{0\}$, on a pour tout $x \in F_i$, $a\pi_i(x) = a(x) = 0$, et pour tout $y \in E_i$, $a\pi_i(y) = a(y)$, -d'où, pour tout $z \in E$, $a(z) = a\pi_i(z)$, et $a = a\pi_i$. Les éléments de l'idéal à droite $\pi_i A$ sont caractérisés par la relation $a = \pi_i a$ (2) ; je dis que ce sont les endomorphismes a tels que $a(E) \subset E_i$; en effet, si $a = \pi_i a$, $a(E) = \pi_i(a(E)) \subset \pi_i(E) = E_i$; si réciproquement on a $a(E) \subset E_i$, on a $\pi_i(a(x)) = a(x)$ pour tout $x \in E$, donc $\pi_i a = a$. En résumé :

Proposition 6 - A tout sous-module F d'un module E, admettant un supplémentaire, sont attachés, dans l'anneau A des endomorphismes du module E, un idéal à gauche $\mathfrak{a}(F)$ annulateur de F, et un idéal à droite $\mathfrak{r}(F)$, ensemble des endomorphismes a de E tels que $a(E) \subset F$. Si π est une projection quelconque de E sur F, on a $\mathfrak{a}(F) = A(1-\pi)$ et $\mathfrak{r}(F) = \pi A$.

Supposons maintenant que B soit un corps K, et E un espace vectoriel de dimension finie n sur K. Alors tout sous-espace F de E admet un supplémentaire et on peut lui appliquer la prop.6. Dans ce cas tout idéal à gauche de A est de la forme $\mathfrak{a}(F)$, et tout idéal à droite de A est de la forme $\mathfrak{r}(F)$; pour le voir il nous suffira de montrer, par exemple, que tout idéal à gauche $\mathfrak{a}$ est de la forme Ae, où e est un idempotent, F étant alors le sous-espace $\overline{e}^1(\{0\})$; remarquons que, puisque A est un A-module à gauche semi-simple (prop.4) $\mathfrak{a}$ admet un supplémentaire $\mathfrak{b}$ (§ 1, prop.3) ; on peut donc écrire $A = \mathfrak{a} + \mathfrak{b}$ d'où, de façon unique, $1 = e+f$, $e \in \mathfrak{a}$, $f \in \mathfrak{b}$; de $e = e^2 + ef$ on déduit (e, $e^2 \in \mathfrak{a}$, $eb \in \mathfrak{b}$) que $e = e^2$ et $ef = 0$; de même $f = f^2$, $fe = 0$; tout élément de $\mathfrak{a}$ s'écrit donc $a = ae + af$; mais $a - ae \in \mathfrak{a}$, $af \in \mathfrak{b}$; donc $a - ae = 0$, $a = ae$, et $\mathfrak{a} = Ae$ où e est un idempotent.

Proposition 7 - Dans un anneau de matrices carrées sur un corps, tout idéal (à droite ou à gauche) est principal, et engendré par un idempotent . Tout idéal à gauche (resp. à droite) est l'annulateur de F (resp. l'ensemble des endomorphismes a de E tels que $a(E) \subset F$), F étant un sous-espace vectoriel de E .

§ 4 - Produits tensoriels d'algèbres primitives.

1) - Réduction du problème.

Soient A et B deux algèbres finies sur un corps commutatifs k , et semi-primitives ; d'après le second th. de Wedderburn (th.3, § 3) elles sont composées directes d'algèbres primitives : $A = \sum_{i=1}^{n} A_i$, $B = \sum_{j=1}^{n} B_j$. Donc le produit tensoriel $A \otimes B$ (sur k) sera isomorphe (chap.III,) au composé direct $\sum_{i,j} A_i \otimes B_j$. Nous sommes donc ramenés à étudier les produits tensoriels d'algèbres primitives.

b) Soient donc A et B deux algèbres primitives finies sur un corps commutatif k ; d'après le premier th. de Wedderburn (th.2, § 3), elles sont isomorphes à des anneaux de matrices carrées sur des corps K et L : $A = K_{(n)}$, $B = L_{(m)}$. Mais l'anneau de matrices $K_{(n)}$ est isomorphe au produit tensoriel $k_{(n)} \otimes K$ de l'algèbre $k_{(n)}$ des matrices carrées d'ordre n sur k , par l'extension K de k . Donc le produit tensoriel $A \otimes B$ est isomorphe à $k_{(n)} \otimes K \otimes k_{(m)} \otimes L$, c'est-à-dire à $k_{(mn)} \otimes K \otimes L$. Faisant abstraction du trivial facteur $k_{(mn)}$, nous sommes donc ramenés à étudier les produits tensoriels de corps.

c) Proposition 1 - Soient K et L deux corps (gauches) finis sur un corps commutatif k , et de centres E et F ; pour que le produit tensoriel $K \otimes L$ (sur k) soit une algèbre semi-primitive, il faut et il suffit que $E \otimes F$ soit une algèbre semi-primitive.

Si $E \otimes F$, qui est un anneau d'Artin, n'est pas semi-primitif, il possède un élément nilpotent z : $z^n = \emptyset$, $z \neq 0$. L'idéal bilatère engendré par z dans $K \otimes L$ est alors nilpotent car z commute avec tout élément de K L . Ceci montre que la condition est <u>nécessaire</u>. Pour démontrer qu'elle est suffisante nous supposerons que $K \otimes L$ possède un idéal bilatère nilpotent $\mathcal{A} \neq (0)$, et il s'agira de montrer que $\mathcal{A} \cap (E \otimes F)$ ne se réduit pas à (0) ; nous procéderons pour ce faire en deux étapes, et il suffira de montrer que $\mathcal{A} \cap (E \otimes L)$ est $\neq (0)$.

$\mathcal{A}$ est un sous-espace vectoriel de $K \otimes L$ considéré comme espace vectoriel sur K ; d'après le th. d'échange (chap.II, § 3,) comme toute base de L sur k est une base de $K \otimes L$ sur K , il existe un sous-espace vectoriel M de L (sur k) tel que le sous-espace KM qu'il engendre sur K dans $K \otimes L$ soit supplémentaire de $\mathcal{A}$; puisque $\mathcal{A} \neq (0)$, il existe $x \in L$, $x \notin M$; nous pouvons donc écrire, et de façon unique, $x = y + z$ avec $y (\neq 0) \in \mathcal{A}$, $z \in KM$; pour tout $u \in K$ on a $ux = xu$, d'où $uy - yu = zu - uz$; mais uy et yu appartiennent à $\mathcal{A}$ qui est un idéal bilatère ; d'autre part $uz \in KM$ par définition, et $zu \in KM$ puisque u $(\in K)$ permute avec tout élément de M $(\subset L)$; la somme $\mathcal{A} + KM$ étant directe, on a donc $uy = yu$; donc y permute avec tout élément de K . Soit $y = \sum_\lambda a_\lambda e_\lambda$ où (e_λ) est une base de L sur k , et où $a_\lambda \in K$; écrivant que y permute avec $a \in K$ il vient : $\sum_\lambda u a_\lambda e_\lambda = \sum_\lambda a_\lambda e_\lambda u = \sum_\lambda a_\lambda u e_\lambda$, puisque $u \in K$ permute avec $e_\lambda \in L$; d'où $u a_\lambda = a_\lambda u$, ce qui montre que $a \in E$, centre de K , et que $y \in E \otimes L$.

<u>Remarques</u> - 1) La dernière partie de la démonstration montre que $E \otimes F$ est le centre de $K \otimes L$. Ceci est valable pour deux algèbres <u>quelconques</u> K et L sur k .

2) On peut montrer, en précisant quelque peu le milieu de la démonstration, que, si $\mathfrak{a}$ est un idéal bilatère quelconque de $K \otimes L$ (K et L étant des corps), $\mathfrak{a}$ est engendré par $\mathfrak{a} \cap (E \otimes F)$.

Corollaire - Pour que le produit tensoriel de deux algèbres semi-primitives soit une algèbre semi-primitive, il faut et il suffit que le produit tensoriel de leurs centres soit semi-primitif.

Nous sommes ainsi ramenés à étudier le produit tensoriel de deux extensions commutatives finies d'un corps k .

2) - Produit tensoriel de deux corps commutatifs.

Soient E et F deux extensions commutatives de dimension linéaire finie d'un corps k . Nous nous proposons d'étudier le produit tensoriel $E \otimes F$ (sur k) ; il s'agit de voir si $E \otimes F$ est, ou non, une algèbre semi-primitive, c'est-à-dire, puisque c'est un anneau d'Artin commutatif, si $E \otimes F$ possède ou non des éléments nilpotents.

Soit F_s la plus grande extension séparable de k contenue dans F ; F est une extension p-radicielle de F_s (chap.V, § 7,), et F_s est une extension monogène $k(\theta)$ de k d'après le th. de l'élément primitif (chap.V, § 7, prop.15) ; $E \otimes F$ est isomorphe au produit tensoriel, sur F_s, de $E \otimes F_s$ (sur k) par F . Si f(X) est le polynome minimal de θ sur k, F_s est isomorphe à $K[X]/(f)$, donc $E \otimes F_s$ est isomorphe à l'anneau $E[X]/(f)$. Soit $f = \prod_{i=1}^{q} g_i$ la décomposition de f en facteurs irréductibles dans $E[X]$ (chap.VII, § 2,) ; les g_i sont tous distincts car f , polynome minimal d'un élément θ séparable sur k , n'a pas de racines multiples. Donc (chap.VII, § 4,) $E[X]/(f)$ est isomorphe au composé direct $\prod_{i=1}^{q} E[X]/(g_i)$ des corps $K_i = E[X]/(g_i)$. Ainsi $E \otimes F$ est isomorphe au composé direct $\prod_{i=1}^{q} (F \otimes K_i)$ (sur F_s).

Si $x \in E \otimes F$ est nilpotent, soit $x^n = 0$, les projections x_i de x sur $F \otimes K_i$ $(1 \leqslant i \leqslant q)$ sont aussi nilpotentes et satisfont à $x_i^n = 0$,

car $x_i x_j = 0$ pour $i \neq j$. Soit (b_λ) une base de F sur F_s ; pour certain exposant f on a $b^{p^f} \in F_s$ pour tout λ ; on peut écrire $x_i = \sum_\lambda a_{i\lambda} b_\lambda$ avec $a_{i\lambda} \in K_i$; donc $x_i^{p^f} = \sum_\lambda a_{i\lambda}^{p^f} b_\lambda^{p^f}$ est un élément du sous-corps de $F \otimes K_i$ canoniquement isomorphe à F_s. De $x_i^n = 0$, on déduit donc $(x_i^{p^f})^n = 0$, d'où $x_i^{p^f} = 0$, et par suite $x^{p^f} = 0$. D'où :

Proposition 2 - Si un élément x du produit tensoriel $E \otimes F$ de deux extensions commutatives finies d'un corps k est nilpotent, il existe un exposant $f > 0$ tel que $x^{p^f} = 0$, p désignant l'exposant caractéristique de k.

Soit maintenant (e_λ) une base de E sur k ; (e_λ) est aussi une base de $E \otimes F$ sur F. L'ensemble $\mathcal{Q}$ des éléments nilpotents de $E \otimes F$ est, en particulier, un espace vectoriel sur F ; soit $x = \sum_\lambda x_\lambda e_\lambda$ $(x_\lambda \in F)$ un élément primordial de celui-ci relatif à la base (e_λ) (chap.II, §5, déf.1). De $x^{p^f} = 0$, on déduit $\sum_\lambda x_\lambda^{p^f} e_\lambda^{p^f} = 0$; ceci montre que les $e_\lambda^{p^f}$ ne sont pas linéairement indépendants sur k, c'est-à-dire que E n'est pas séparable sur k ; on en déduit aussi que, si $\sum_\lambda a_{i\lambda} e_\lambda^{p^f} = 0$ $(a_{i\lambda} \in k)$ $(1 \leqslant i \leqslant m)$ sont les relations primordiales entre les $e_\lambda^{p^f}$ sur k (chap.II, §5,), on a $x^{p^f} = \sum_i y_i a_i$ $(y_i \in F)$, donc $x_\lambda = a_{i_0\lambda}$ puisqu'il s'agit d'éléments primordiaux. Donc :

Théorème 1 - Pour que le produit tensoriel $E \otimes F$ de deux extensions commutatives finies d'un corps k ne soit pas un anneau semi-primitif il faut et il suffit que E soit une extension non séparable de k, et que F contienne une extension p-radicielle R de k dont E ne soit pas linéairement disjointe.

Corollaire - Le produit tensoriel $E \otimes F$ d'une extension séparable finie E de k par une extension algébrique quelconque F de k, est un anneau semi-primitif, composé direct de corps commutatifs.

La restriction aux extensions F finies est ici inutile, car un élément nilpotent de $E \otimes F$ appartient à certain $E \otimes F'$ où $F' \subset F$ est une extension finie de k.

3) - Extension du corps de base d'une algèbre semi-primitive. Algèbres séparables.

Soit A une algèbre semi-primitive finie sur un corps k, K une extension de k. Rappelons qu'on appelle algèbre obtenue à partir de A en étendant le corps de base en K, le produit tensoriel $A \otimes K$ (chap. III, § ,). Soit $\prod_{i=1}^{q} Z_i$ le centre de A, composé direct de surcorps Z_i de k (§ 3, cor. de la prop.5) ; $A \otimes K$ sera semi-primitive avec son centre $\prod_{i=1}^{q} (Z_i \otimes K)$ (cor. de la prop.1). Posons la définition suivante :

Définition 1 - On dit qu'une algèbre semi-primitive finie A sur k est séparable si tous les corps composants Z_i de son centre $\prod_i Z_i$ sont séparables sur k.

On a donc la proposition suivante :

Proposition 2 - Pour qu'une algèbre semi-primitive finie A sur k soit séparable il faut et il suffit que toute algèbre obtenue de A par extension du corps de base k soit semi-primitive (on dit aussi que "A reste semi-primitive dans toute extension").

Les algèbres séparables sont caractérisées par la propriété suivante, qui généralise la caractérisation des extensions séparables au moyen des dérivations (chap.V, § 7, n°10): toute dérivation de A, considérée comme algèbre sur k, est intérieure (c'est-à-dire de la forme : $x \to ax-xa$, $a \in A$).

4) - Corps gauches. Groupe de Brauer.

Soit A un corps gauche de rang fini sur son centre k ; l'algèbre étendue $A \otimes K$, K étant une extension commutative de k, aura K pour centre et sera donc primitive . Cependant $A \otimes K$ ne sera pas toujours un corps ; soit en effet Ω la cloture algèbrique de k ; $A \otimes \Omega$ est un anneau de matrices sur un corps Ω' de centre Ω ; mais, si $x \in \Omega'$, le corps $\Omega(x)$ est une extension commutative finie de Ω , donc $\Omega(x) = \Omega$ (chap.V, §6, prop.), et $\Omega' = \Omega$. Donc $A \otimes \Omega$ est l'algèbre des matrices carrées d'un certain degré r sur Ω . Remarquant que le rang de A sur k est égal à celui de $A \otimes \Omega$ sur Ω , on obtient la proposition suivante :

Proposition 3 - Si un corps A est de rang fini sur son centre k , ce rang est un carré parfait r^2 , et, si Ω désigne la cloture algèbrique de k , $A \otimes \Omega$ est isomorphe à l'algèbre des matrices carrées de degré r sur Ω .

D'une manière générale nous dirons qu'une extension K du centre k d'un corps gauche A est un corps de décomposition de A , si l'algèbre étendue $A \otimes K$ est une algèbre de matrices sur K . Nous venons de voir que la cloture algèbrique Ω de k est un corps de décomposition de tout corps gauche A de centre k . Nous verrons, au § 5, qu'il existe des extensions finies de k qui sont des corps de décomposition de A .

Proposition 4 - Soit K un corps de dimension finie n sur son centre k ; le produit tensoriel $K \otimes K'$, sur k , de K et de son opposé K' est une algèbre de matrices sur k .

K , étant à la fois module à gauche et à droite sur lui-même, est module à gauche sur K et K' ; ces deux lois externes étant permutables d'après l'associativité, de K, K possède une structure de module à gauche sur $K \otimes K'$ (chap.III, app.II). Les homothéties de K relatives

à cette structure sont évidemment des endomorphismes de K pour sa structure d'espace vectoriel sur k . Comme $K \otimes K'$ est un anneau simple (3,prop.4), K est un $K \otimes K'$-module fidèle, et $K \otimes K'$ est isomorphe à une sous-algèbre (sur k) de l'algèbre $\mathcal{L}(K)$ des endomorphismes de K , considéré comme espace vectoriel sur k . Comme $K \otimes K'$ et $\mathcal{L}(K)$ ont toutes deux dimensions n^2 sur k , la proposition est démontrée.

Considérons maintenant l'ensemble $\mathcal{A}$ des algèbres primitives finies de centre k ; toute $A \in \mathcal{A}$ est de la forme $A = k_{(n)} \otimes K$, où K est un corps de centre k . Si nous identifions les algèbres $A \in \mathcal{A}$ qui ont le même corps K , nous obtenons un ensemble quotient $\mathcal{G}$ de $\mathcal{A}$ que l'on appelle l'ensemble des classes d'algèbres centrales-primitives sur k. La loi de composition interne sur $\mathcal{G}$ obtenue par passage au quotient du produit tensoriel dans $\mathcal{A}$ est associative d'après l'associativité du produit tensoriel ; la classe de k est élément neutre ; et la prop.4 montre que la classe de l'opposée A' de A est inverse de la classe de A . $\mathcal{G}$ est donc muni d'une structure de groupe abélien. Muni de cette structure $\mathcal{G}$ est appelé le groupe de Brauer du corps k , Remarquons que les classes des corps de centre K qui admettent une extension donnée E de k comme corps de décomposition forment un sous-groupe $\mathcal{G}_K$ du groupe de Brauer $\mathcal{G}$; l'étude des sous-groupes $\mathcal{G}_K$ est l'instrument le plus puissant pour étudier le groupe de Brauer $\mathcal{G}$.

§ 5 - Isomorphismes d'algèbres primitives.

1) - Modules sur les anneaux d'Artin semi-primitifs.

Proposition 1 - Une condition nécessaire et suffisante pour qu'un anneau d'Artin A soit semi-primitif, est que tout A-module unitaire E soit complètement réductible.

Pour la nécessité il nous suffira de montrer que E est somme de modules simples (§ 1, prop.1) ; pour cela il suffit de montrer que, pour tout $x \in E$, le module monogène Ax est somme de modules simples ; or Ax est isomorphe à un module interne $A/\mathfrak{a}$ (§ 2, prop.1) ; mais (prop.4, § 3) A est un A-module semi-simple ; donc (§ 1, prop.3) $\mathfrak{a}$ admet un supplémentaire semi-simple, isomorphe à $A/\mathfrak{a}$. La condition est aussi suffisante ; considérons le A-module A_s ; il est fidèle puisque A admet un élément unité, et semi-simple par hypothèse et d'après la condition D'Artin ; donc A est semi-primitif (déf. 2, § 1).

Remarques - 1) Si E est un A-module quelconque, on peut, pour tout $x \in E$, écrire $x = 1.x + (x - 1.x)$; les ensembles E' et E" des 1.x et des x-1.x sont évidemment des sous-modules de E ; de $1.x = y - 1.y$ on déduit, par multiplication par 1, $1.x = 0$; donc E est somme directe de E' et E". E' est évidemment unitaire ; et, pour tout $a \in A$, on a $aE" = \{0\}$ ("décomposition de Peirce"). Donc E est somme directe d'un module complètement réductible E', et d'un module trivial E".

2) On peut montrer que, si tout A-module est somme directe d'un module complètement réductible et d'un module trivial, alors A est un anneau semi-primitif d'Artin, et admet donc un élément unité.

3) Lorsque A est un anneau primitif d'Artin, tout A-module unitaire est (3, prop.1) somme directe de modules simples tous isomorphes.

2) - Anneaux primitifs d'endomorphismes d'un groupe abélien.

Soit E un groupe abélien, $\mathcal{L}(E)$ l'anneau de tous les endomorphismes de E, A un sous-anneau de $\mathcal{L}(E)$, B le commutant de A dans $\mathcal{L}(E)$. Nous conserverons ces notations dans tout ce n°.

Proposition 2 - Si A est un anneau d'Artin primitif dont l'élément unité coïncide avec celui de $\mathcal{L}(E)$, B est un anneau complet de matrices (finies ou infinies) sur le corps K des endomorphismes du A-module simple et fidèle ; et A est le commutant de B .

E, considéré comme A-module, est somme directe $\sum_{\alpha \in I} E_\alpha$ de A-modules simples et fidèles tous isomorphes entre eux. Pour tout $b \in B$, et tout $x \in E$, soit $b_{\beta\alpha}(x)$ le composant de $b.x$ dans E_β ; il est clair que l'application $x \longrightarrow b_{\beta\alpha}(x)$ (que nous noterons $b_{\beta\alpha}$) est un homomorphisme de E_α dans E_β ; comme E_α et E_β sont simples, $b_{\beta\alpha}$ est soit nul, soit un isomorphisme ; on voit aussitôt que, si α est donné, tous les $b_{\beta\alpha}$ sont nuls sauf un nombre fini d'entre eux. Soit M un modèle fixe de A-module simple et fidèle, φ_α un isomorphisme de M sur E_α ; posons $\lambda_{\beta\alpha} = \varphi_\beta^{-1} \circ f_{\beta\alpha} \circ \varphi_\alpha$; $\overset{\lambda}{\underset{\beta\alpha}{}}$ est un élément du corps K des endomorphismes de M . Soit $V = K_\alpha^{(I)}$ un espace vectoriel à droite sur K , et $(\epsilon_\alpha)_{\alpha \in I}$ sa base canonique ; si, à tout $b \in B$, on fait correspondre l'endomorphisme $\overline{b}$ de V défini par $\overline{b}(e_\alpha) = \sum_\beta e_\beta \lambda_{\beta\alpha}$ on définit évidemment un isomorphisme de B sur l'anneau des endomorphismes de l'espace vectoriel V .

Soit maintenant C le commutant de B dans $\mathcal{L}(E)$, et soit M_α un sous-A-module simple de E ; M_α est un espace vectoriel sur K , et, par hypothèse, l'ensemble $\overline{A}$ des restrictions à M_α des endomorphismes de A est l'ensemble de tous les endomorphismes de M_α ; $\overline{A}$ est donc identique à l'ensemble $\overline{C}$ des restrictions à M_α d'endomorphismes de C ; ceci montre que A est identique à C .

Supposons maintenant que A est une algèbre finie sur un corps k contenu dans le centre de A ; E est alors muni d'une structure d'espace vectoriel sur k , que nous supposerons de dimension finie.

Il est clair que le commutant B de A contient k dans son centre, et que A et B sont des anneaux d'endomorphismes de E considéré comme espace vectoriel sur k . Soit C l'algèbre de tous les endomorphismes de E considéré comme espace vectoriel sur k ; A et B sont commutants l'un de l'autre dans C . Soit $A = K_{(n)}$, m^2 le rang du corps gauche K sur son centre Z , et $q = [Z:k]$; soit h le xm nombre des sous A-modules simples dont E est somme directe ; puisque l'un quelconque de ces sous-modules a dimension n sur K , on a $[E:k] = nm^2hq$. D'autre part $[A:k] = (nm)^2q$. Mais B est un anneau de matrices carrées de degré h à éléments dans K ; on a donc $[B:k] = h^2m^2q$. De $[E:k] = nm^2hq$, on déduit $[C:k] = n^2m^4h^2q^2$. Donc :

$$(1) \qquad [A:k].[B:k] = [C:k] .$$

Proposition 3 - Soit A un anneau d'Artin primitif, E son module simple et fidèle, K le corps des endomorphismes de E ; A et K sont linéairement disjoints sur leur centre commun k .

Il nous faut montrer que, si $(u_i)_{1 \leqslant i \leqslant n}$ sont n éléments de A linéairement indépendants sur k , les u_i sont linéairement indépendants sur K . Supposons le contraire et soit $\sum_i \lambda_i u_i = 0$ ($\lambda_i \in K$) une relation primordiale entre les u_i ; on a, pour tout $x \in E$, $\sum \lambda_i u_i(x) = 0$, donc $\sum_i \lambda_i \ u_i(\mu x) = 0$ ($\mu \in K$), ce qui s'écrit $\sum_i \lambda_i \mu \ u_i(x) = 0$, ou encore $\sum_i \lambda_i \mu u_i = 0$. Puisque $\sum \lambda_i \ u_i = 0$ est primordiale il existe $\rho \in K$ tel que $\lambda_i \mu = \rho \lambda_i$ pour tout i ; comme un des indices k est tel que $\lambda_k = 1$, on a $\mu = \rho$, donc $\lambda_i \mu = \mu \lambda_i$ pour tout $\mu \in K$, et $\lambda_i \in k$.

3) - Isomorphismes d'algèbres primitives.

Soient A et A' deux sous-anneaux isomorphes de $\mathcal{L}(E)$, et $u \to \overline{u}$ un isomorphisme de A sur A' ; cet isomorphisme permet de définir sur E une nouvelle structure de A-module en posant $u.x = \overline{u}(x)$.

Dans le cas où les deux structures de A-module ainsi obtenues sont isomorphes, il existe une application φ de E sur lui-même telle que $\varphi(x+y) = \varphi(x) + \varphi(y)$ et $\varphi(u(x)) = \overline{u}(\varphi(x))$; autrement dit $\overline{u} = \varphi u \varphi^{-1}$. En outre, si B et B' sont les commutants respectifs de A et A' dans $\mathcal{L}(E)$, on a $B' = \varphi B \varphi^{-1}$: en effet, si b B , on a $(\varphi b \varphi^{-1})(\overline{u})(x) = \varphi\, bu\, \varphi^{-1}(x) = \varphi\, ub\, \varphi^{-1}(x) = \overline{u}\, \varphi b \varphi^{-1}(x)$ et vice-versa ; l'application $b \longrightarrow \varphi b \varphi^{-1}$ est donc un isomorphisme de B sur B' .

L'isomorphisme des deux structures de A-module sera assurée si A est un anneau d'Artin primitif ($\S$ 3,prop.2), et si E a le même nombre de composantes simples en tant que A-module et que A'-module. Supposons donc que A et A' sont des sous-algèbres primitives d'une algèbre primitive $C = K_{(n)}$ de rang fini sur son centre k,A et A' contenant k. Prenons pour E un C-module simple et fidèle, qui, en posant $\left[K:k\right] = m^2$, est muni d'une structure d'espace vectoriel de dimension nm^2 sur k . Les A-modules et A'-modules simples et fidèles ayant même dimension sur k,E sera somme directe d'un même nombre h de A-modules et de A'-modules simples, et les considérations précédentes s'appliqueront. Elles s'appliqueront aussi en remplaçant A et A' par les algèbres $A \otimes K'$ et $A' \otimes K'$ qui peuvent être considérées (prop.3) comme plongées dans $\mathcal{L}(E)$ (K', antiisomorphe à K , désigne le corps des endomorphismes du C-module simple E) ; celles-ci sont primitives ($\S$ 4) car k est le centre de K', et on peut leur prolonger l'isomorphisme ψ A sur A' . On a alors $\psi(u) = \varphi\, u\, \varphi^{-1}$ $(u \in A \otimes K')$; si $u \in K'$, $\psi(u) = u$, donc φ appartient au commutant de K' qui est C (prop.2). Par conséquent :

Proposition 4 - Soit C une algèbre primitive finie sur son centre k , A et A' deux sous-algèbres primitives de C contenant k ; tout isomorphisme de A sur A' est de la forme $x \longrightarrow axa^{-1}$ où a est un élément inversible de C .

En particulier :

Théorème 1 (Skolem-Noether) - Etant donnée une algèbre A primitive et finie sur son centre k , tout automorphisme de A laissant invariants les éléments de k est un automorphisme intérieur.

4) - Corps de décomposition d'un corps gauche.

Soit K un corps de dimension finie m^2 sur son centre k ; nous nous proposons de déterminer les extensions commutatives finies T de k qui sont corps de décomposition de K , c'est-à-dire telles que $K \otimes T$ soit un anneau de matrices sur T . Si K' désigne l'opposé de K , il est clair que $T \otimes K'$ sera aussi un anneau de matrices sur T ; $T \otimes K'$ est un anneau primitif (§ 4) dont nous désignerons par E un module simple et fidèle ; si $\mathscr{L}(E)$ désigne l'anneau des endomorphismes du groupe abélien sous-jacent de E, $T \otimes K'$ peut être considéré comme un sous-anneau de $\mathscr{L}(E)$ (prop.3) ; il résulte de l'hypothèse que le commutant de $T \otimes K'$ dans $\mathscr{L}(E)$ est T lui-même (chap.II, § 2,) ; en particulier T est contenu dans le commutant de K' dans $\mathscr{L}(E)$; si r désigne la dimension (finie) de E considéré comme espace vectoriel à gauche sur K', ceci exprime que T est un sous-corps commutatif de l'anneau de matrices $K_{(r)}$. T est d'ailleurs un sous-corps commutatif maximal de $K_{(r)}$, car, si T était contenu dans un sous-corps commutatif T_1 de $K_{(r)}$, les éléments de T_1 appartiendraient aux commutants, dans $\mathscr{L}(E)$, de T et de K', donc à celui de $T \otimes K'$. La relation (1) (n°2) donne ici, en prenant $A = B = T$, $C = K_{(r)}$, $\left[T:k\right]^2 = r^2m^2$, donc $\left[T:k\right] = rm$.

Considérons inversement un anneau de matrices quelconque $B = K_{(r)}$, à éléments dans K , et soit S un sous-corps commutatif de B , contenant le centre k de K , et tel que $\left[S:k\right]^2 = \left[B:k\right]$. Soit E un espace vectoriel à gauche de dimension r sur l'opposé K' de K .

Nous supposerons tous les anneaux que nous allons considérer comme plongés dans l'anneau $\mathcal{L}(E)$ des endomorphismes du groupe abélien sous-jacent de E . Le commutant C de S dans $K_{(r)}$ contient S qui est son centre ; d'après la relation (1) ($n^o 2$) il est identique à S ; S est donc un sous-corps commutatif maximal de $K_{(r)}$. Mais S est aussi le commutant de $K' \otimes S$ dans $\mathcal{L}(E)$; donc $K' \otimes S$ est le commutant de S (prop.2), ce qui montre que $K' \otimes S$ est une algèbre de matrices sur S . Donc :

Proposition 5 - Pour qu'une extension commutative finie T du centre k d'un corps K de rang fini sur k soit corps de décomposition de K , il faut et il suffit que T soit isomorphe à un sous-corps S d'un anneau de matrices $K_{(r)}$ sur K , tel que $\left[K_{(r)}:k\right] = \left[S:k\right]^2$.

Nous venons de voir que la relation $\left[K_{(r)}:k\right] = \left[S:k\right]^2$ entraîne que S est un sous-corps commutatif maximal de $K_{(r)}$. Prenons $r = 1$, et soit T un sous-corps commutatif maximal de K ; le commutant de T dans K est un sous-corps de K (chap.V, § 2, prop.) contenant T ; si a est un élément de celui-ci, T(a) est un corps commutatif ; comme T est maximal, on a $a \in T$, et T est son propre commutant dans K ; et la relation (1) ($n^o 2$) donne ici : $\left[K:k\right] = \left[T:k\right]^2$. Donc :

Proposition 6 - Si K est un corps de rang m^2 sur son centre k , tout sous-corps commutatif maximal de K est une extension de degré m de k , et un corps de décomposition de K .

5) - Applications - I Corps finis.

Théorème 2 (Wedderburn) - Tout corps fini K est commutatif.

Soit k le centre de K ; deux sous-corps commutatifs maximaux de K ont même degré (prop.6) sur k , donc (Chap.V, § 9) sont isomorphes ; ils sont donc transformés l'un en l'autre par un automorphisme intérieur de K (prop.4). Or tout élément de K appartient à un sous-corps

commutatif maximal de K ; donc, si T est un sous-corps commutatif maximal de K, K est réunion des xTx^{-1} , où $x \in K^*$. On en conclut que le groupe multiplicatif K^* est réunion des conjugués xT^*x^{-1} de son groupe T^* . Si $x' = xt$, $t \in T^*$, on a $x'T^*x'^{-1} = xtT^*t^{-1}x^{-1} = xT^*x^{-1}$; le nombre des conjugués xT^*x^{-1} est donc au plus égal à l'indice $(K^* : T^*)$; d'autre part, chacun des conjugués de T^* ayant le même nombre d'éléments que T^*, K^* ne peut être réunion des xT^*x^{-1} que si ces ensembles forment une partition de K^* ; comme ils ont en commun l'élément unité de K , ils sont au nombre de 1, et on a $K = T$.

6) - Applications - II Corps gauches sur un corps quasi-réel maximal. Théorème 3 (Frobénius) - Sur un corps quasi réel maximal S , tout corps non commutatif de rang fini est isomorphe au corps des quaternions sur S .

Soit en effet K un tel corps, k son centre, T un sous-corps commutatif maximal de K ; posons $[T:k] = m$, d'où $[K:k] = m^2$. T et k étant des extensions commutatives finies de S , sont isomorphes à S ou à S(i) ; comme $m > 1$ par hypothèse, on a $k = S$, $T = S(i)$, $m = 2$. L'unique automorphisme de S(i) sur S , distinct de l'identité, transforme i en -i , et est la restriction à S(i) d'un automorphisme intérieur de K (prop.4) ; donc il existe $u \neq 0$ tel que $uiu^{-1} = -i$; u ne peut appartenir à S(i) , donc 1 et u forment une base de K considéré comme espace vectoriel à gauche sur S(i). D'autre part $u^2iu^{-2} = i$, donc u^2 est permutable avec i ; étant aussi permutable avec u , il appartient au centre S de K , soit $u^2 = a \in S$. On ne peut avoir $a \geqslant 0$, car on en déduirait $u^2 = a = v^2$, $v \in S$, d'où $(u-v)(u+v) = 0$, $u = v$ ou $u = -v$, et u appartiendrait à S , ce qui est absurde. On a donc $u^2 = -b^2$, $b \in S$. Si on pose $j = ub$, et $ij = k$, K a pour base (1,i,j,k) sur S,

avec la table de multiplication $i^2 = j^2 = -1$, $ij = -ji = k$, $k^2 = ijij = -i^2j^2 = -1$, $ki = -ik = j$, $jk = -kj = i$; d'où le théorème.

7) - Applications - III Corps réflexifs.

Définition 1 - On dit qu'un corps non commutatif K fini sur son centre k est réflexif, s'il admet un antiautomorphisme involutif $x \to x'$ $(x \in K)$ tel que xx' et $x+x'$ appartiennent à k , et que l'on ait $a' = a$ pour tout $a \in k$.

Théorème 4 - Tout corps réflexif de caractéristique différente de 2 , est un corps de quaternions sur son centre.

Puisque $x^2-(x+x')x+xx' = 0$, tout élément x de K est de degré 1 ou 2 sur k ; un sous-corps commutatif maximal T de K a donc pour degré sur k une puissance de 2 , et, comme la caractéristique de k est $\neq 2$, il est séparable sur k ; le th. de l'élément primitif donne donc $\left[T:k\right] = 2$, et $\left[K:k\right] = 4$. L'application $x \to x'$ induit sur T un automorphisme, qui est aussi induit par un automorphisme intérieur de K , $x \to vxv^{-1}$ $(v \in K)$. Comme on peut écrire $T = k(u)$ avec $u^2 = a \in k$ (la caractéristique de T est $\neq 2$), et que $u' = -u$, on a $vuv^{-1} = -u$; d'où, comme ci-dessus, $v^2 = b \in k$; si l'on pose $w = uv$, $(1,u,v,w)$ est base de K sur k , et la table de multiplication est évidemment celle des quaternions (généralisés).

§ 6 - Représentations linéaires des groupes et des algèbres.

1) - Définitions. Représentations semblables.

Soit A une algèbre sur un corps commutatif K , et $K_{(r)}$ l'algèbre des matrices carrées de degré r sur K . Toute représentation $s \to M(s)$ de A dans $K_{(r)}$ est appelée une représentation linéaire (ou matricielle) de degré r de A . L'idéal bilatère $\mathfrak{a} \subset A$ composé des éléments $s \in A$

tels que $M(s) = 0$ est appelé le noyau de la représentation ; une représentation dont le noyau est réduit à (0) est dite fidèle ; il revient au même de dire que $s \longrightarrow M(s)$ est un isomorphisme de A dans $K_{(r)}$. Soit maintenant G un groupe et K un corps commutatif ; nous appelerons représentation linéaire (ou matricielle) de degré r de G sur K, toute représentation dans $K_{(r)}$ de l'algèbre A du groupe G relative à K ; il revient au même de se donner un homomorphisme de G dans le sous-groupe multiplicatif des éléments inversibles de $K_{(r)}$ (que l'on peut étendre à A par linéarité).

Cette définition s'applique aussi bien à un monoïde qu'à un groupe.

Dans ce qui va suivre, nous nous bornerons en général aux représentations linéaires d'algèbres, laissant au lecteur le soin de traduire en termes de groupes.

On dit que deux représentations linéaires $s \longrightarrow M(s)$ et $s \longrightarrow N(s)$ de l'algèbre A dans $K_{(r)}$ sont semblables, s'il existe une matrice inversible fixe $P \in K_{(r)}$ telle que $N(s) = PM(s)P^{-1}$ pour tout $s \in A$. La relation de similitude est une relation d'équivalence entre représentations de A ; les classes d'équivalence suivant cette relation sont appelées les classes de représentations de A. La plupart des propriétés que nous allons exposer sont des propriétés de ces classes de représentations.

L'algèbre A possède une structure d'espace vectoriel sur K ; supposons-le de dimension finie r. L'application $M(s):t \longrightarrow st$ $(s,t \in A)$ est un endomorphisme de A pour cette structure ; il est clair que $M(s+s') = M(s) + M(s')$ et que $M(ss') = M(s)M(s')$; on a donc ainsi défini une représentation linéaire de degré r de A, appelée la représentation régulière de A. Le noyau de celle-ci est composé

des éléments $s \in A$ tels que $sA = (0)$; par conséquent la représentation régulière d'une algèbre ayant un élément unité est fidèle.

2) - Norme et trace d'une représentation.

Définition 1 - On appelle trace (resp. norme) d'un élément $s \in A$ relative à la représentation linéaire $s \longrightarrow M(s)$ de A, la trace (resp. le déterminant) de l'endomorphisme $M(s)$.

Comme les polynomes caractéristiques de deux matrices semblables sont égaux, la trace et la norme de $s \in A$ sont les mêmes pour toutes les représentations d'une même classe $\mathcal{D}$; on les notera donc $Tr_{\mathcal{D}}(s)$ et $N_{\mathcal{D}}(s)$. On a évidemment les formules suivantes :

$$Tr_{\mathcal{D}}(s + s') = Tr_{\mathcal{D}}(s) + Tr_{\mathcal{D}}(s')$$

$$N_{\mathcal{D}}(ss') = N_{\mathcal{D}}(s).\ N_{\mathcal{D}}(s')$$

$$Tr(ss') = Tr(s's)$$

$$Tr(as) = a.Tr(s) \quad \text{si} \quad a \in K$$

$N(as) = a^r.N(s)$, r désignant le degré des représentations de la classe.

Lorsque A est une extension commutative séparable finie de K, la trace et la norme d'un élément $s \in A$ définies au chap.V, ne sont autres que la trace et la norme de s relatives à la représentation régulière de A. Si s est racine d'une équation irréductible de degré n, et si $\left[A:K(s)\right] = m$, il suffit pour le voir de calculer la matrice correspondant à s dans la représentation régulière de A, A étant rapporté à la base $(s^j u_j)$, où $0 \leqslant j \leqslant n-1$, et où (u_i) $(1 \leqslant i \leqslant m)$ est une base quelconque de A sur $K(s)$.

Dans le cas de la représentation d'un groupe G, l'application χ : $s \rightarrow Tr(s)$ $(s \in G)$ est appelée un caractère du groupe G.

3) - Opérations sur les représentations.

Soient $s \longrightarrow M(s)$, $s \rightarrow N(s)$ deux représentations de degrés m et n de l'algèbre A, et soient $\mathcal{D}$ et $\mathcal{D}'$ leurs classes. Dans l'espace

vectoriel produit $K^n \times K^m = K^{m+n}$, considérons l'application qui, à l'élément (x,y) $(x \in K^n$, $y \in K^m)$ fait correspondre $(M(s)x, N(s)y)$; c'est une application linéaire $P(s)$, et $s \to P(s)$ est évidemment une représentation linéaire de degré $m+n$ de A ; on l'appelle la <u>somme directe</u> des représentations $s \to M(s)$ et $s \to N(s)$. La classe de cette représentation ne dépend que des classes $\mathcal{D}$ et $\mathcal{D}'$; on la note $\mathcal{D} + \mathcal{D}'$.

Si on rapporte K^{m+n} à une base telle que K^m et K^n soient des sous-espaces de coordonnées, la matrice $P(s)$ s'écrit :

$$\begin{pmatrix} M(s) & 0 \\ 0 & N(s) \end{pmatrix}$$

on a les formules suivantes :

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

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

On a défini (chap.III, 1,n°4 et 6) le <u>produit tensoriel</u> $M \otimes N$ de deux applications linéaires (resp. matrices) M et N de degrés m et n , et on a vu que l'on a $M \otimes N = N \otimes M$, $(M_1 M_2) \otimes (N_1 N_2) = (M_1 \otimes N_1)(M_2 \otimes N_2)$. Il en résulte que, si $s \to M(s)$ et $s \to N(s)$ sont deux représentations linéaires de degrés m et n et de classes d'un <u>groupe</u> G , l'application $s \to M(s) \otimes N(s)$ est une représentation linéaire de degré mn de G , appelée <u>produit tensoriel</u> des deux représentations données. Comme on a, pour deux matrices inversibles P et Q , $(PM(s)P^{-1}) \otimes (QN(s)Q^{-1}) =$ $= (P \otimes Q)(M(s) \otimes N(s))(P \otimes Q)^{-1}$, la classe de la représentation $s \to M(s) \otimes N(s)$ ne dépend que de $\mathcal{D}$ et $\mathcal{D}'$. On appelle cette classe le <u>produit tensoriel</u> de $\mathcal{D}$ et de $\mathcal{D}'$ et on la note $\mathcal{D} \otimes \mathcal{D}'$. On a les formules suivantes :

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

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

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

Si $M = (a_{ij})$ et $N = (\beta_{k\ell})$, on a $M \otimes N = (\gamma_{(i,k)(j,\ell)})$, où $\gamma_{(i,k)(j,\ell)} = a_{ij}\beta_{k\ell}$; donc $\mathrm{Tr}(M \otimes N) = \sum_{i,k} a_{ii}\beta_{kk} = \sum_{i} a_{ii} \sum_{k} \beta_{kk} =$ $= \mathrm{Tr}M.\mathrm{Tr}N$; donc :

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

Considérons enfin une représentation linéaire de classe $\mathcal{D}$, $s \to M(s)$ d'un groupe G ($s \in G$) ; pour tout $s \in G$, la matrice $M(s)$ est inversible, et admet donc une matrice contragrédiente (chap.II, § 6, n°6) $\check{M}(s) = ({}^tM(s))^{-1} = {}^tM(s)^{-1}$; puisqu'on a $\widehat{(MN)} = \check{M}\check{N}$, l'application $s \to \check{M}(s)$ est une représentation matricielle du groupe G, de même degré que la représentation donnée, et que l'on appelle sa représentation contragrédiente. De la formule $\widehat{PMP^{-1}} = \check{P}.\check{M}.(\check{P})^{-1}$, on déduit que la classe de la représentation $s \to \check{M}(s)$ ne dépend que de $\mathcal{D}$; on la note $\check{\mathcal{D}}$ et on l'appelle la classe contragrédiente de $\mathcal{D}$. On a les formules suivantes qui montrent que $\mathcal{D} \to \check{\mathcal{D}}$ est un automorphisme involutif de l'ensemble des classes de représentations de G, muni des deux lois de composition internes définies ci-dessus :

$$\widehat{(\mathcal{D} + \mathcal{D}')} = \check{\mathcal{D}} + \check{\mathcal{D}}'$$

$$\widehat{\mathcal{D}.\mathcal{D}'} = \check{\mathcal{D}} \otimes \check{\mathcal{D}}'$$

$$\check{\check{\mathcal{D}}} = \mathcal{D}$$

La trace d'une matrice étant égale à celle de sa transposée, on a :

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

4)- Représentations réductibles, irréductibles, complètement réductibles

Soit $s \to M(s)$ une représentation linéaire de degré r d'une algèbre A, ayant un élément unité, sur un corps K ; l'espace vectoriel K^r est alors muni d'une structure de A-module, et, puisque K peut être identifié au sous-corps $K.1$ de A, la structure d'espace vectoriel de K^r

est sous-jacente à sa structure de A-module ; en particulier les sous A-modules de K^r sont des sous-espaces vectoriels. Comme K^r est de dimension finie, le A-module K a une <u>suite de Jordan-Holder</u> : $(0) = E_0 \subset E_1 \subset \ldots \subset E_n = K^r$, où E_i/E_{i-1} est un A-module simple. En adaptant aux E_i les vecteurs de la base de K^r , les matrices M(s) ont la forme :

$$\begin{pmatrix} P_{11}(s) & P_{12}(s) & \ldots\ldots & P_{1n}(s) \\ 0 & P_{22}(s) & \ldots\ldots & P_{2n}(s) \\ & \ldots\ldots\ldots & \ldots\ldots & \\ 0 & & \ldots\ldots & P_{nn}(s) \end{pmatrix}$$

Posons alors la définition suivante :

<u>Définition 2</u> - <u>On dit qu'une représentation linéaire de degré r d'une algèbre A sur un corps K est irréductible</u> (resp. <u>réductible, complètement réductible</u>) <u>si K est un A-module simple</u> (resp. <u>non simple, semi-simple</u>).

Les applications $s \to P_{ii}(s)$ sont donc des représentations irréductibles de A ; d'après le th. de Jordaneulderre, les classes de ces représentations ne dépendent, à l'ordre près, que de la classe $\mathcal{D}$ de la représentation $s \to M(s)$; on les appelle les <u>facteurs de composition</u> de la classe $\mathcal{D}$.

Dans le cas où la représentation $s \to M(s)$ est complètement réductible, K^r est somme directe de sous-modules simples, et, rapportant K^r à une base convenable, la matrice M(s) prend la "forme diagonale" :

$$\begin{pmatrix} P_{11}(s) & \ldots\ldots & 0 \\ & \ldots\ldots\ldots & \\ 0 & \ldots\ldots & P_{nn}(s) \end{pmatrix}$$

où les représentations $s \to P_{ii}(s)$ sont irréductibles. La classe $\mathcal{D}$ est alors <u>somme directe</u> de ses facteurs de composition.

Nous allons maintenant donner un résultat analogue au lemme de Schur (§ 1, th.1) :

Proposition 1 - Soient $s \to M(s)$ et $s \to N(s)$ deux représentations irréductibles d'une algèbre A ; s'il existe une matrice fixe P telle que, pour tout $s \in A$, on ait $PM(s) = N(s)P$, ou bien $P = 0$, ou bien les deux représentations données ont même degré r et P est une matrice carrée inversible de degré r (donc les deux représentations sont semblables).

Si r et r' sont les degrés de M(s) et N(s), la relation $PM(s)=N(s)P$ implique que la matrice P a r' lignes et r colonnes, et définit donc une application linéaire φ de K^r dans $K^{r'}$; elle montre aussi que φ est un homomorphisme de K^r dans K^r pour leurs structures de A-modules. Puisque $\varphi(K^r)$ et $\varphi^{-1}(\{0\})$ sont des sous-modules de $K^{r'}$ et de K^r, et que $K^{r'}$ et K^r sont des modules simples, on a, ou bien $\varphi^{-1}(\{0\}) = K^r$ et $\varphi = 0$, ou bien φ est un isomorphisme de K^r sur $K^{r'}$.

Corollaire - Soient $s \to M(s)$ et $s \to N(s)$ deux représentations matricielles irréductibles d'un groupe G, de classes $\mathcal{D}$ et $\mathcal{D}'$ et de degrés r et r'. Pour qu'il existe un vecteur de $K^r \otimes K^{r'}$ invariant par toutes les matrices $M(s) \otimes N(s)$ $(s \in G)$, il faut et il suffit que $\mathcal{D}' = \check{\mathcal{D}}$.

Soient en effet (e_i) $(1 \leqslant i \leqslant r)$ et (e'_j) $(1 \leqslant j \leqslant r')$ les bases canoniques de K^r et de $K^{r'}$, et soit $x = \sum_{i,j} a_{ij}.(e_i \otimes e'_j)$ un vecteur de $K^r \otimes K^{r'}$. Si $M(s) = (m_{ik}(s))$ et $N(s) = (n_{j\ell}(s))$, la condition nécessaire et suffisante pour que x soit invariant s'écrit

$\sum_{k\ell} m_{ik}(s).n_{j\ell}(s).a_{k\ell} = a_{ij}$ pour tous i et j ; ou encore, en posant $A = (a_{ij})$, $M(s).A.{}^tN(s) = A$, c'est-à-dire $M(s)A = A\check{N}(s)$, et le cor. se déduit immédiatement de la prop.1 .

5)- Représentations des algèbres primitives et semi-primitives.

La déf.3 (§ 1) se traduit immédiatement en la proposition suivante :

Proposition 2 - Pour qu'une représentation linéaire d'une algèbre A soit complètement réductible il faut et il suffit que l'image de A par cette représentation soit une algèbre semi-primitive.

La prop.1 (§ 5) se traduit en la proposition suivante :

Proposition 3 - Pour qu'une algèbre A ayant un élément unité, et finie sur son corps de base K soit semi-primitive, il faut et il suffit que toutes ses représentations linéaires soient complètement réductibles.

Enfin (§ 3, prop.2) :

Proposition 4 - Une algèbre primitive finie ne possède qu'une seule classe de représentations irréductibles.

6)- Représentations matricielles des groupes finis.

Théorème 1 (Maschke) - Une condition nécessaire et suffisante pour que toute représentation linéaire d'un groupe fini G par des matrices à éléments dans un corps K soit complètement réductible, est que la caractéristique p de K ne divise pas l'ordre h de G .

Il suffit de montrer l'équivalence des propositions : "$p \nmid h$" et "l'algèbre A du groupe G sur K est semi-primitive" (prop.3).

Supposons d'abord que $p \nmid h$. Pour montrer que A est semi-primitive, il nous suffira de montrer que tout A-module unitaire E est complètement réductible (§ 5, prop.1), c'est-à-dire que tout sous-module M de E admet un supplémentaire. Dans E , considéré comme espace vectoriel sur K , soit N un sous-espace supplémentaire de M . Pour tout $x \in E$ soit $f(x)$ le composant de x dans M par rapport à la décomposition directe $E = M + N$; pour tout $s \in G$ on a $f(sx) \in M$, donc $s^{-1}f(sx) \in M$ puisque M est un A-module. Posons $g(x) = \frac{1}{h} \sum_{s \in G} s^{-1}f(sx)$; g est un endomorphisme de E pour sa structure de A-module, car, pour tout $t \in G$,

on a $g(tx) = \frac{1}{h} \sum_{s \in G} s^{-1} f(stx) = \frac{t}{h} \sum_{s \in G} (st)^{-1} f(stx) = t.g(x)$; donc $P = g^{-1}(\{0\})$ est un sous A-module de E . D'autre part pour tout $x \in M$, on a $sx \in M$, $f(sx) = sx$, et $g(x) = \frac{1}{h} hx = x$. Par conséquent E est somme directe des sous-modules M et P .

L'élément $a = \sum_{s \in G} s$ de A est tel que $at = ta = a$ pour tout $t \in G$; donc Ka est un idéal bilatère de A . D'autre part $a = ha = 0$, si $p \mid h$; A possède alors un idéal bilatère nilpotent Ka et n'est pas semi primitive.

7)- Représentations matricielles des groupes abéliens finis.

Soit $s \to M(s)$ une représentation irréductible de degré r d'une algèbre A . Rappelons que le lemme de Schur (§ 1,th.1) expriment que les matrices Q de degré r telles que $QM(s) = M(s)Q$ pour tout $s \in A$ forment un sous-corps de l'algèbre des matrices $K_{(r)}$. Si, en particulier, le corps K est algèbriquement clos, ce sous-corps se réduit au sous-corps des matrices diagonales K.1 . Donc :

Proposition 5 - Toute représentation irréductible d'une algèbre commutative A sur un corps algèbriquement clos K est de degré 1 .

Ainsi une telle représentation se réduit à son caractère $s \longrightarrow \chi(s)$. Prenons en particulier pour A l'algèbre d'un groupe abélien fini G relative à un corps algèbriquement clos K dont la caractéristique p ne divise pas l'ordre h de G . Toute représentation de A étant complètement réductible (th.1), il nous suffira d'étudier les représentations irréductibles de A , c'est-à-dire les caractères de G , homomorphismes $s \longrightarrow \chi(s)$ $(s \in G)$ de G dans le groupe multiplicatif K^* de K . Si s est un élément d'ordre k de G , on a $(\chi(s))^k = \chi(s^k) = \chi(e) = 1$, donc $\chi(s)$ est une racine k-ème de l'unité.

Mais G est (chap.VII) produit direct de groupes cycliques $H_1, \ldots, H_n$ d'ordres $h_1, \ldots, h_n$; désignons par $a_1, \ldots, a_n$ des générateurs de $H_1, \ldots, H_n$. Si χ est un caractère de G , $\chi(a_i) = \xi_i$ est une

racine h-ème de l'unité, et $\chi(a_1^{m_1}\ldots a_n^{m_n}) = \xi_1^{m_1}\ldots\ldots\xi_n^{m_n}$. Si réciproquement, $\xi_1,\ldots,\xi_n$ sont des racines h_1-,...,h_n-èmes de l'unité dans K, la formule $\chi(a_1^{m_1},\ldots,a_n^{m_n}) = \chi_1^{m_1}\ldots\chi_n^{m_n}$ définit évidemment un caractère de G. On voit donc que G possède $h = h_1\ldots h_n$ caractères distincts.

Si χ et χ' sont deux caractères de G, $\chi\chi'$, défini par $\chi\chi'(s) = \chi(s)\,\chi'(s)$ $(s\in G)$, et χ^{-1}, défini par $\chi^{-1}(s)=(\chi(s))^{-1}$, sont des caractères de G. Donc les caractères de G forment un <u>groupe abélien</u> G' d'ordre h. L'ensemble des caractères χ de G tels que $\chi(a_i)=1$ pour $i \neq j$ est un sous-groupe cyclique H'_j de G', isomorphe au groupe des racines h_j-èmes de l'unité ; G' est évidemment produit direct des H'_j. Ainsi <u>le groupe des caractères G' de G est isomorphe à G</u>.

Pour tout $s\in G$, l'application ρ_s de G' dans K définie par $\rho_s(\chi) = \chi(s)$ $(\chi\in G')$ est un <u>caractère</u> de G'. Donc G est <u>canoniquement isomorphe</u> au groupe G" des caractères de G', puisqu'ils ont le même nombre d'éléments. En résumé :

<u>Théorème 2</u> - <u>Les caractères d'un groupe abélien fini G forment un groupe G' isomorphe à G. La formule</u> $\rho_s(\chi) = \chi(s)$ $(s\in G, \chi\in G')$ <u>définit un isomorphisme canonique de G sur le groupe G" des caractères de G'</u>.

-x-x-x-x-x-x-