LIVRE II
ALGEBRE
CHAPITRE II (ETAT 4)
ALGEBRE LINEAIRE

Rédaction n° 036

Nombre de pages : 116

Nombre de feuilles : 116

A 36

LIVRE II

ALGÈBRE

CHAPITRE II (Etat 4)

ALGÈBRE LINÉAIRE

§1. Modules et espaces vectoriels.

1. Définition des modules et des espaces vectoriels. **Définition 1.** Etant donné un anneau A, on appelle module à gauche par rapport à A (ou, par abus de langage, module à gauche sur A, ou encore A-module à gauche) un ensemble E muni d'une structure algèbrique définie par la donnée : 1° d'une loi de groupe abélien dans E (notée additivement) ; 2° d'une loi de composition externe partout définie $(\alpha,x) \longrightarrow \alpha \top x$ dont le domaine d'opérateurs est l'anneau A, et qui satisfait aux axiomes suivants :

(M_I) $\alpha \top (x+y)=(\alpha \top x)+(\alpha \top y)$ quels que soient $\alpha \in A$, $x \in E$, $y \in E$;

(M_{II}) $(\alpha+\beta) \top x = (\alpha \top x)+(\beta \top x)$ quels que soient $\alpha \in A$, $\beta \in A$, $x \in E$;

(M_{III}) $\alpha \top (\beta \top x)=(\alpha\beta) \top x$ quels que soient $\alpha \in A$, $\beta \in A$, $x \in E$.

Si, dans cette définition, on remplace l'axiome (M_{III}) par :

(M'_{III}) $\alpha \top (\beta \top x)=(\beta\alpha) \top x$ quels que soient $\alpha \in A$, $\beta \in A$, $x \in E$,

on dit que E, muni de la structure algèbrique ainsi définie, est un module à droite par rapport à A, ou (par abus de langage) un module à droite sur A (ou encore un A-module à droite).

Le plus souvent, la loi de composition externe d'un module à gauche (resp. d'un module à droite) se note multiplicativement, en écrivant l'opérateur à gauche (resp. à droite) ; la condition (M_{III}) s'écrit alors $\alpha(\beta x)=(\alpha\beta)x$, la condition ($M'_{III}$) s'écrit $(x\beta)\alpha = x(\beta\alpha)$.

Si A^0 désigne l'anneau opposé (chap.I, §8) de A, tout module à droite sur l'anneau A est un module à gauche sur l'anneau A^0.

Il en résulte que, dans l'étude des propriétés générales des modules, on peut se borner à ne considérer que des modules à gauche ou des modules à droite ; dans ce paragraphe et le suivant, nous n'étudierons en principe que les modules à gauche, et lorsque nous parlerons de module (sans préciser), il s'agira d'un module à gauche, dont la loi externe sera notée multiplicativement.

Il n'y a évidemment pas lieu de distinguer les notions de module à droite et de module à gauche par rapport à un anneau commutatif .

Remarque. Un module est un groupe abélien à opérateurs particulier (chap.I, §6,n°9) : l'axiome (M_I) signifie en effet que la loi externe d'un A-module E est distributive par rapport à l'addition dans E .

L'axiome (M_{II}) signifie que cette loi externe est distributive par rapport à l'ensemble des deux lois additives dans A et dans E ; l'axiome (M_{III}) enfin, qu'elle est associative par rapport à la multiplication dans A .

Les applications $x \longrightarrow ax$ d'un module E dans lui-même s'appellent les homothéties de E ; ce sont des endomorphismes de la structure de groupe abélien (sans opérateur) de E , d'après (M_I) ; on a donc $a.0=0$ pour tout $a \in A$. D'après (M_{II}), on a aussi $0.x=0$ pour tout $x \in E$; de ces deux identités, il résulte que $a(-x)=(-a)x=-(ax)$ quels que soient $a \in A$ et $x \in E$.

Si on s'est donné sur un ensemble E une structure de module à gauche par rapport à un anneau A , et si B est un sous-anneau quelconque de A , la loi de groupe abélien dans E et la restriction de la loi externe au sous-anneau B de A (chap.I, §3) définissent sur E une structure de module à gauche par rapport à B .

Exemples. 1) Un anneau est à la fois module à gauche et module à droite par rapport à un quelconque de ses sous-anneaux, et en particulier par rapport à lui-même. Lorsque nous considérerons un anneau A comme A-module à gauche (resp. à droite), nous l'écrirons A_s (resp. A_d) s'il y a lieu, pour éviter toute confusion.

2) La structure de groupe à opérateurs définie sur un groupe abélien G (noté additivement) par la loi externe $(n,x) \longrightarrow n.x$ (chap.I, §6,n°9) est une structure de module par rapport à l'anneau $\mathbb{Z}$ des entiers rationnels.

3) Soit G un groupe abélien noté additivement, et $\mathfrak{E}$ l'anneau des endomorphismes de G (chap.I, §8,n°1 : on rappelle que le produit fg de deux endomorphismes est par définition l'endomorphisme $f \circ g$); la loi externe $(f,x) \longrightarrow f(x)$ entre opérateurs $f \in \mathfrak{E}$ et éléments $x \in G$ définit sur G une structure de module à gauche par rapport à l'anneau $\mathfrak{E}$.

4) G désignant toujours un groupe abélien additif, et A un anneau quelconque, on définit sur G une structure de A-module à gauche, en posant $ax=0$ quels que soient $a \in A$ et $x \in G$.

Définition 2. On dit qu'un A-module à gauche E est unitaire si l'anneau A possède un élément unité ε qui est en même temps opérateur neutre pour la loi externe (autrement dit, si $\varepsilon x = x$ quel que soit $x \in E$) .

Dans un module unitaire E , on a , pour tout entier $n \in \mathbb{Z}$ et tout $x \in E$, $n.x=(n.\varepsilon)x$.

La plupart des modules qui interviennent en Algèbre sont des modules unitaires. Si un anneau A possède un élément unité, les A-modules A_s et A_d sont évidemment unitaires ; les modules définis dans les exemples 2 et 3 ci-dessus sont unitaires.

Les plus importants des modules unitaires sont ceux dont l'anneau d'opérateurs est un corps :

Définition 3 . On appelle espace vectoriel à gauche (resp. à droite) sur un corps K , un K-module à gauche (resp. à droite) unitaire.

Les éléments d'un espace vectoriel sont souvent appelés vecteurs ; les éléments du corps d'opérateurs sont alors qualifiés de scalaires.

Exemples. 1) Si K est un corps quelconque, les modules K_s et K_d sont des espaces vectoriels par rapport à K .

2) L'espace numérique à trois dimensions R^3 de la géométrie classique est un espace vectoriel par rapport au corps des nombres réels R , le produit tx d'un nombre réel t et d'un point x de coordonnées x_1, x_2, x_3 étant le point de coordonnées tx_1, tx_2, tx_3 . De même, l'ensemble des fonctions numériques définies dans un ensemble quelconque F , est un espace vectoriel par rapport à R , le produit tf d'un nombre réel t et d'une telle fonction étant la fonction numérique $x \to tf(x)$. *

Dans un espace vectoriel E sur un corps K , toute homothétie $x \to ax$ correspondant à un élément $a \neq 0$ de K , est un automorphisme de la structure de groupe abélien (sans opérateur) de E , car de la relation $y = ax$ on tire $x = a^{-1}(ax) = a^{-1}y$.

2. Sous-modules et modules quotients. Soit E un module à gauche par rapport à un anneau A ; si M est un sous-groupe stable de E (chap.I, § 6, n°10), il est immédiat que la structure induite sur M (chap.I, § 4, n°2) par la structure de module à gauche de E est une structure de module à gauche par rapport à A ; l'ensemble M , muni de cette structure, est appelé un sous-module de E .

Toutes les propriétés des sous-groupes stables sont donc applicables aux sous-modules. En particulier, si M et N sont deux sous-modules d'un module E , leur somme M+N et leur intersection $M \cap N$ sont des sous-modules de E .

Si E est un module unitaire, tous ses sous-modules sont unitaires. En particulier, tout sous-module d'un <u>espace vectoriel</u> E est un espace vectoriel, qu'on appelle encore <u>sous-espace vectoriel</u> de E .

<u>Exemples</u>. 1) Dans un module quelconque E , l'ensemble réduit à 0 est un sous-module (sous-module <u>nul</u>) .

2) Soit A un anneau, A_s (resp. A_d) l'ensemble A muni de sa structure de A-module à gauche (resp. à droite). Les sous-modules de A_s (resp. A_d) ne sont autres que les <u>idéaux à gauche</u> (resp. <u>idéaux à droite</u>) de l'anneau A .

3) Soit E un A-module à gauche, x un élément de E , $\mathfrak{a}$ un idéal à gauche de l'anneau A . L'ensemble des éléments ax , où a parcourt $\mathfrak{a}$, est un sous-module de E , qu'on note $\mathfrak{a}x$.

4) Dans un groupe abélien additif G , considéré comme module par rapport à Z (avec la loi $(n,x) \to n.x$) tout sous-groupe de G est aussi un sous-module. Il en est de même quand on munit G de la structure de module par rapport à un anneau quelconque A , où le produit $ax=0$ quels que soient $a \in A$ et $x \in G$.

<u>Remarque</u>. Soit E un A-module, B un sous-anneau de l'anneau A . Tout sous-module du A-module E est aussi un sous-module du B-module E , mais la réciproque est inexacte ; par exemple, si A admet un élément unité, qui soit aussi élément unité de B , le B-module à gauche B_s n'est pas un A-module si $B \neq A$.

Soit E un module à gauche par rapport à un anneau A . Toute relation d'équivalence compatible (chap.I, § 4) avec la structure de module de E est de la forme $x-y \in M$, où M est un sous-groupe stable de E (chap.I, § 6), donc un sous-module de E . En outre, on vérifie immédiatement (cf. chap. I, § 5) que la structure de groupe à opérateurs du groupe quotient E/M (chap.I, § 6) est une structure de A-module à gauche ; muni de cette structure, E/M est appelé module quotient de E par le sous-module M .

Si E est un A-module unitaire, tout module quotient E/M est unitaire, car l'élément unité ε de A laisse invariant tout élément de E , et par suite toute classe mod.M . En particulier tout module quotient d'un espace vectoriel E est un espace vectoriel, qu'on appelle espace vectoriel quotient de E .

Exemple. Tout idéal à gauche $\mathfrak{a}$ dans un anneau A définit un module quotient $A_s/\mathfrak{a}$ du A-module à gauche A_s ; ce module quotient se note souvent, pour abréger, $A/\mathfrak{a}$, mais, lorsque $\mathfrak{a}$ est un idéal bilatère, il faut se garder de confondre la structure d'anneau quotient de $A/\mathfrak{a}$ (chap.I, § 8, n°5), et sa structure de module à gauche par rapport à l'anneau A .

Les relations entre les sous-modules et modules quotients d'un module quotient E/M , et les sous-modules et modules quotients de E , sont résumées par la proposition suivante (simple traduction du th.6 du chap.I, § 6) :

Proposition 1. Soit M un sous-module d'un module E , f l'application canonique de E sur le module quotient E/M = E' .

a) Si N' est un sous-module quelconque de E/M , $N = f^{-1}(N')$ est un sous-module de E , contenant M , on a N'=f(N), et N' est isomorphe au module quotient N/M .

b) Si N est un sous-module de E contenant M, et $N'=f(N)$, le module quotient E/N est isomorphe au module quotient E'/N'.

c) Si N est un sous-module quelconque de E, $f(N)$ est un sous-module de E/M, isomorphe aux modules quotients $(N+M)/M$ et $N/(M\cap N)$.

En raison de a), pour un sous-module $N \supset M$, on identifie le plus souvent $f(N)$ et N/M ; la propriété b) s'énonce alors en disant que E/N est isomorphe à $(E/M)/(N/M)$.

3. Produit de modules. Soit $(E_\iota)_{\iota\in I}$ une famille de modules à gauche par rapport à un même anneau A. On vérifie immédiatement que, sur l'ensemble produit $E = \prod_{\iota\in I} E_\iota$, le produit des structures de groupe à opérateurs des E_ι (chap.I, § 6, n°15) est une structure de module à gauche par rapport à A. Muni de cette structure, l'ensemble E est appelé le module produit des modules E_ι. Toutes les propriétés des produits de groupes à opérateurs établies au chap.I (§ 6, n°15) sont applicables aux produits de modules. En particulier, si pour tout $\iota\in I$, M_ι est un sous-module de E_ι, le produit $M = \prod_{\iota\in I} M_\iota$ est un sous-module du produit E, isomorphe au produit des modules M_ι. Si on prend $M_\iota = E_\iota$ pour tous les indices d'une partie J de I, $M_\iota = \{0\}$ pour les indices $\iota \in \complement J$, le module $E'_J = \prod_{\iota\in I} M_\iota$ est isomorphe au module produit $E_J = \prod_{\iota\in J} E_\iota$. Lorsque J est un ensemble réduit à un seul élément $\varkappa$, le sous-module E'_J se note encore $E'_\varkappa$; il est isomorphe à $E_\varkappa$, et on l'appelle le sous-module composant d'indice $\varkappa$ de E. De même, si N est un sous-module quelconque de E, le sous-module $N'_\varkappa$ de $E'_\varkappa$, formé des éléments dont les coordonnées d'indice $\neq\varkappa$ sont nulles, et la coordonnée d'indice $\varkappa$ égale à $\mathrm{pr}_\varkappa x$, où x parcourt N, est appelé le module composant d'indice $\varkappa$ de N ; il est isomorphe à la projection de N sur $E_\varkappa$.

Si tous les modules E_ι sont unitaires, il en est de même de leur produit. En particulier, le produit d'une famille d'espaces vectoriels est un espace vectoriel.

Un exemple important de produit de modules est celui où tous les modules facteurs E_ι sont identiques au module A_s (ensemble A muni de sa structure de A-module à gauche) ; on le désigne par la notation A_s^I (ou simplement par A^I quand aucune confusion n'est à craindre) ; les éléments de ce module sont les applications de I dans A .

4. Transporteurs et annulateurs. Soit E un module à gauche sur un anneau A , M un sous-module de E . Si F est une partie non vide quelconque de E , on appelle transporteur de F dans M l'ensemble des éléments $a \in A$ tels que $a.F \subset M$ (c'est-à-dire que, pour tout $x \in F$, $ax \in M$) . Si deux parties F,G sont telles que $F \subset G$, le transporteur de G est contenu dans celui de F . Si (F_ι) est une réunion de parties non vides de E , le transporteur de la réunion $\bigcup_\iota F_\iota$ dans M est l'intersection des transporteurs des F_ι dans M .

Il est immédiat que le transporteur d'une partie non vide F de E dans un sous-module M est un idéal à gauche de A . Le transporteur dans M d'un sous-module N de E est un idéal bilatère de A : en effet, si $ax \in M$ pour tout $x \in N$, on a aussi $a(\beta x) \in M$ pour tout $x \in N$ et tout $\beta \in A$, donc $a\beta$ appartient au transporteur de N dans M pour tout $\beta \in A$.

Lorsque $M = \{0\}$, le transporteur d'une partie F de E dans M prend le nom d'annulateur de F : c'est l'ensemble des $a \in A$ tels que $ax = 0$ pour tout $x \in F$. L'annulateur d'une partie F de E est l'intersection des annulateurs des éléments de F . L'annulateur d'un sous-module de E (et en particulier, l'annulateur de E lui-même) est un idéal bilatère de A .

Exemple : caractéristique d'un groupe abélien. Soit G un groupe abélien, écrit additivement, et considéré comme module par rapport à $\mathbb{Z}$. L'annulateur du groupe G est l'ensemble des entiers $m \in \mathbb{Z}$ tels que $m.x=0$ pour tout $x \in G$; c'est un idéal principal (c) (chap.I, § 8, n^{os} 5 et 6), intersection des annalateurs de tous les éléments de G ; comme l'annulateur d'un élément x est (0) si x est d'ordre infini dans G, (p) si x est d'ordre fini $p > 0$, on voit qu'on aura $c=0$ si G admet des éléments d'ordre infini ; dans le cas contraire, c n'est autre que le p.p.c.m. (chap.I, § 8, n°6) des ordres des éléments de G d'ordre fini. En particulier, si G est un groupe fini d'ordre n, c est un diviseur de n (chap.I, § 6, cor. de la prop.3).

Le nombre c est appelé la caractéristique du groupe additif G. Si A est un anneau quelconque, sa caractéristique est par définition la caractéristique de son groupe additif.

Au chap.VI, nous verrons que la caractéristique d'un corps est 0 ou un nombre premier.

Remarque. La notion de transporteur peut aussi se ramener à celle d'annulateur : en effet, si f est l'application canonique de E sur le module quotient E/M, le transporteur de F dans M est identique à l'annulateur de f(F) dans E/M ; on peut en conclure en particulier que le transporteur de F dans M est identique au transporteur de F+M dans M.

Définition 4. On dit qu'un élément x d'un module E est régulier si son annulateur est nul (autrement dit, si la relation $ax=0$ entraîne $a=0$). On dit que E est un module régulier si tous ses éléments $\neq 0$ sont réguliers.

Si $x \in E$ est régulier, la relation $\alpha x = \beta x$ entraîne $\alpha = \beta$ d'après (M_{II}); dans un module régulier, la relation $\alpha x = 0$ est équivalente à "$\alpha = 0$ ou $x = 0$" . On peut encore exprimer qu'un module E est régulier en disant que, pour tout $\alpha \neq 0$, l'homothétie $x \to \alpha x$ est une application biunivoque de E dans E ; cela montre en particulier que tout espace vectoriel est un module régulier. Tout sous-module d'un module régulier est régulier ; tout produit de modules réguliers est régulier.

Remarques. 1) Dire qu'un élément $\xi \in A$ est régulier dans le A-module A_s signifie que ξ n'est pas diviseur de zéro à droite. En particulier, l'élément unité de A (s'il existe) est régulier dans A_s (et dans A_d) .

2) On observera que si, dans un A-module E , x est un élément tel que le sous-module A.x soit $\neq \{0\}$, ce sous-module (et a fortiori E) ne peut être régulier que si A est un anneau sans diviseur de zéro ; en effet, il existe $\gamma \in A$ tel que γx soit régulier ; s'il existait deux éléments non nuls $\alpha \in A$, $\beta \in A$, tels que $\alpha\beta = 0$, on aurait $(\alpha\beta)(\gamma x) = 0$, c'est-à-dire $\alpha(\beta\gamma x) = 0$; comme $\alpha \neq 0$, cela entraînerait par hypothèse $\beta(\gamma x) = 0$, et comme $\gamma x \neq 0$, on en conclurait $\beta = 0$, contrairement au choix de α et β .

On dit qu'un module E est normal si son annulateur est nul ; il est clair qu'un module régulier est normal, mais la réciproque est inexacte.

Par exemple, si A est un anneau ayant un élément unité ε , le module A_s est normal puisque, pour tout $\alpha \neq 0$, on a $\alpha\varepsilon = \alpha \neq 0$, et par suite $\alpha.A \neq \{0\}$. Par contre, A_s n'est régulier que si A ne possède pas de diviseur de zéro .

D'une façon générale, si on désigne par u_a l'homothétie $x \to ax$ définie par un opérateur $a \in A$ dans un A-module E, il résulte des axiomes (M_{II}) et (M_{III}) que l'application $a \to u_a$ de A dans l'anneau des endomorphismes $\mathfrak{E}$ du groupe abélien (sans opérateur) E, est une représentation de A dans $\mathfrak{E}$; l'image réciproque de 0, par cette représentation, est précisément l'idéal bilatère $\mathfrak{a}$, annulateur de E. Si $\mathfrak{a}$ est un élément quelconque de l'anneau quotient $A/\mathfrak{a}$, l'élément ax de E est le même pour tout $a \in \mathfrak{a}$; si on le désigne par $\mathfrak{a}x$, la loi de composition $(\mathfrak{a},x) \to \mathfrak{a}\,x$ définit sur E une structure de module normal par rapport à l'anneau d'opérateurs $A/\mathfrak{a}$; muni de cette structure, E est appelé le module normal associé au A-module E. On observera que tout sous-module d'un A-module E est également un sous-module du module normal associé à E, et réciproquement.

Remarque. Soit E un groupe abélien à opérateurs quelconque, noté additivement, $\mathfrak{E}$ l'anneau des endomorphismes de la structure de groupe abélien (sans opérateur) de E (chap.I, § 8, n°1). Pour tout opérateur a d'une quelconque des lois externes $\perp$ de E, soit u_a l'application $x \to a \perp x$ produite par a ; par hypothèse, u_a est un élément de l'anneau $\mathfrak{E}$. Soit alors A le sous-anneau de $\mathfrak{E}$ engendré par les u_a correspondant à tous les opérateurs de toutes les lois externes de E ; il est immédiat que A est le sous-groupe additif de $\mathfrak{E}$ engendré par les composés d'un nombre fini d'endomorphismes u_a. Si alors on considère sur E la structure de A-module définie par la loi externe $(v,x) \to v(x)$ (pour tout endomorphisme $v \in A$), tout sous-groupe stable de E (pour la structure de groupe à opérateurs donnée sur E) est un sous-module de E et réciproquement. De même, si F est un groupe abélien à opérateurs homologue (chap.I, § 4, n°1)

de E , et si on munit F de la structure correspondante de A-module, toute <u>représentation</u> du groupe à opérateurs E dans le groupe à opérateurs F est aussi une représentation du A-module E dans le A-module F , et réciproquement. On peut donc ramener l'étude des groupes abéliens a opérateurs généraux à celle des modules ; c'est pourquoi nous n'avons considéré que ces derniers.

5. <u>Modules monogènes</u>. Dans un module E , la notion de sous-module étant identique à celle de sous-groupe stable, le plus petit sous-module M contenant une partie quelconque F de E est identique au sous-groupe stable <u>engendré</u> par F (chap.I, § 6, n° 10) ; on dit que F est un <u>système de générateurs</u> de M .

<u>Définition 5</u>. <u>On dit qu'un module est monogène s'il est engendré par un seul élément</u>.

Si A est un anneau commutatif ayant un élément unité, les sous-modules monogènes du module A_s ($=A_d$) ne sont autres que les <u>idéaux principaux</u> (chap.I, § 8, n° 6) de l'anneau A .

On aura soin de ne pas confondre les notions de <u>groupe monogène</u> (chap.I, § 6, n° 7) et de <u>module monogène</u>. Tout groupe monogène, considéré comme module par rapport à $\mathbb{Z}$, est évidemment un module monogène. Par contre, le groupe additif (sans opérateur) d'un module monogène n'est nullement un groupe monogène en général : par exemple, le corps Q des nombres rationnels, considéré comme Q -module, est un module monogène, mais son groupe additif n'est pas monogène.

Soit E un module <u>unitaire</u> par rapport à un anneau A ; pour tout élément $a \in E$, le sous-module engendré par a est l'ensemble A.a des éléments λa , où λ parcourt A ; en effet, tout sous-module contenant a contient aussi A.a , et on a $a \in A.a$, puisque $a = \varepsilon a$ (ε élément unité de A).

En particulier, si E est monogène, il est identique au module A.a , pour tout élément a qui l'engendre.

En outre, l'application $\lambda \to \lambda a$ est une <u>représentation</u> du module à gauche A_s sur A.a=E , d'après les axiomes (M_{II}) et (M_{III}) ; l'image réciproque de 0 par cette représentation est l'<u>annulateur</u> $\mathfrak{a}$ de a ; donc E est isomorphe au <u>module quotient</u> $A_s/\mathfrak{a}$. Réciproquement, si A est un anneau ayant un élément unité ε et $\mathfrak{a}$ un idéal à gauche quelconque de A , le module quotient $A_s/\mathfrak{a}$ est un A-module monogène engendré par la classe $\dot{\varepsilon} = \varepsilon + \mathfrak{a}$ de ε : en effet, la classe $\dot{\mu} = \mu + \mathfrak{a}$ d'un élément quelconque $\mu \in A$, peut s'écrire $\mu\dot{\varepsilon}$. Ainsi :

<u>Proposition 2</u>. <u>Soit</u> A <u>un anneau ayant un élément unité</u>. <u>Tout module monogène unitaire par rapport à</u> A <u>est isomorphe à un module quotient</u> $A_s/\mathfrak{a}$, <u>où</u> $\mathfrak{a}$ <u>est un idéal à gauche quelconque de</u> A ; <u>réciproquement, tout module quotient de</u> A_s <u>est un module monogène unitaire</u>.

D'après la prop.1, tout sous-module d'un A-module unitaire et monogène E est donc isomorphe à un module quotient $\mathfrak{b}/\mathfrak{a}$, où $\mathfrak{a}$ et $\mathfrak{b}$ sont deux idéaux à gauche de A (tels que $\mathfrak{a} \subset \mathfrak{b}$) ; tout module quotient de E est isomorphe à un module quotient $A/\mathfrak{b}$, donc est lui-même monogène.

Il ne faudrait pas croire qu'un sous-module d'un module monogène soit toujours un module monogène ; par exemple, nous rencontrerons plus tard des anneaux d'intégrité, possédant un élément unité, et dans lequel il existe des idéaux non principaux (chap.V) .

Il résulte aussi de la démonstration de la prop.2 que, si x est un élément <u>régulier</u> dans un A-module unitaire E , le sous-module monogène A.x engendré par x est <u>isomorphe à</u> A_s .

6. Somme de sous-modules. La notion de module monogène permet de préciser la manière dont est obtenu le sous-module engendré par une partie quelconque F d'un module A . En effet, pour tout $x \in F$, ce sous-module contient le module monogène engendré par x ; il est donc identique au sous-module engendré par la réunion des modules monogènes engendrés par les éléments de F .

Nous sommes donc ramenés à étudier, de façon générale, le sous-module engendré par la réunion d'une famille $(M_\iota)_{\iota \in I}$ de sous-modules de E .

Proposition 3. Le sous-module engendré par la réunion d'une famille $(M_\iota)_{\iota \in I}$ de sous-modules d'un module E , est identique au sous-groupe engendré par cette réunion, et se compose donc des sommes finies de la forme $\sum_{\iota \in J} x_\iota$, où J est une partie finie quelconque de I , et et $x_\iota \in M_\iota$.

La démonstration est la même que celle de la prop.3 du chap.I, § 8 .

Lorsque I est fini, le sous-module engendré par la réunion des M_ι n'est autre que la somme $\sum_{\iota \in I} M_\iota$. Par extension, on pose la définition suivante :

Définition 6. On appelle somme d'une famille quelconque $(M_\iota)_{\iota \in I}$ de sous-modules d'un module E , et on note $\sum_{\iota \in I} M_\iota$, le sous-module engendré par la réunion de cette famille.

Si $(x_\iota)_{\iota \in I}$ est une famille infinie d'éléments de E telle que $x_\iota = 0$ sauf pour les indices appartenant à une partie finie J de I , on convient de désigner par $\sum_{\iota \in I} x_\iota$ la somme $\sum_{\iota \in J} x_\iota$, et de l'appeler encore la somme des éléments de la famille infinie $(x_\iota)_{\iota \in I}$; convention qui est justifiée par le fait que, pour toute partie finie $H \supset J$, on a $\sum_{\iota \in H} x_\iota = \sum_{\iota \in J} x_\iota$. On vérifie aussitôt les formules

(1) $$\sum_{\iota\in I} x_\iota + \sum_{\iota\in I} y_\iota = \sum_{\iota\in I} (x_\iota + y_\iota)$$

(2) $$a.\sum_{\iota\in I} x_\iota = \sum_{\iota\in I} ax_\iota \qquad (a\in A).$$

Bien entendu, la notation $\sum_{\iota\in I} x_\iota$ n'a pas de sens pour une famille $(x_\iota)_{\iota\in I}$ pour laquelle $x_\iota \neq 0$ pour une infinité d'indices ι (tout au moins tant que E n'est pas muni d'une structure topologique (cf. Top.gén., chap.III, §4)). Lorsque, dans ce Livre, nous emploierons cette notation, il sera toujours sous-entendu que $x_\iota = 0$ sauf pour un nombre fini d'indices.

Avec la notation ainsi introduite, la prop.3 s'exprime encore en disant que le module engendré par la réunion $\bigcup_{\iota\in I} M_\iota$ d'une famille quelconque de sous-modules est identique à l'ensemble des sommes $\sum_{\iota\in I} x_\iota$, où $(x_\iota)_{\iota\in I}$ parcourt l'ensemble des familles d'éléments de E telles que $x_\iota \in M_\iota$ pour tout ι, et $x_\iota = 0$ sauf pour un nombre fini d'indices.

Définition 7. On appelle combinaison linéaire d'une famille $(a_\iota)_{\iota\in I}$ d'éléments d'un module E sur un anneau A, tout élément de la forme $\sum_{\iota\in I} \lambda_\iota a_\iota$, où $(\lambda_\iota)_{\iota\in I}$ est une famille d'éléments de A (appelés les coefficients de la combinaison linéaire) telle que $\lambda_\iota = 0$ sauf pour un nombre fini d'indices ι.

Avec cette définition, les prop.2 et 3 donnent la suivante :

Proposition 4. Dans un module unitaire E, le sous-module engendré par une famille $(a_\iota)_{\iota\in I}$ d'éléments de E, est l'ensemble des combinaisons linéaires de la famille (a_ι).

7. Somme directe de sous-modules. De même qu'on vient d'étendre la notion de somme d'une famille de sous-modules au cas d'une famille infinie, on peut définir la notion de somme directe d'une famille quelconque de sous-modules, généralisant la notion déjà définie pour le cas d'une famille finie (chap.I, §6, n° 6) :

Définition 8. *On dit que la somme d'une famille* $(M_\iota)_{\iota\in I}$ *de sous-modules d'un module* E *est directe si tout élément de cette somme ne peut s'écrire que d'une seule manière sous la forme* $\sum_{\iota\in I} x_\iota$ (où $x_\iota \in M_\iota$ pour tout ι, et $x_\iota = 0$ sauf pour un nombre fini d'indices).

La définition 8 signifie que la relation $\sum_{\iota\in I} x_\iota = \sum_{\iota\in I} y_\iota$, où $x_\iota \in M_\iota$, $y_\iota \in M_\iota$, entraîne $x_\iota = y_\iota$ pour tout ι, ou encore (en vertu de (1) et du fait que les M_ι sont des sous-modules) que *la relation* $\sum_{\iota\in I} z_\iota = 0$, où $z_\iota \in M_\iota$, *entraîne* $z_\iota = 0$ *pour tout* $\iota \in I$.

On peut aussi mettre cette condition sous la forme suivante :

Proposition 5. *Pour que la somme d'une famille* $(M_\iota)_{\iota\in I}$ *de sous-modules d'un module* E *soit directe, il faut et il suffit que pour tout* $\varkappa \in I$, *l'intersection de* $M_\varkappa$ *et de la somme des modules* M_ι *d'indice* $\iota \neq \varkappa$ *se réduise à* 0.

La condition est évidemment nécessaire d'après la déf. 8 ; elle est suffisante, car la relation $\sum_{\iota\in I} z_\iota = 0$ s'écrit, pour tout $\varkappa \in I$, $z_\varkappa = \sum_{\iota\neq\varkappa} (-z_\iota)$ et entraîne donc $z_\varkappa = 0$.

Si E est somme directe d'une famille (M_ι) de sous-modules, à tout $x \in E$ correspond une famille (x_ι) *unique* telle que $x = \sum_\iota x_\iota$; pour chaque ι, l'élément x_ι qui correspond à x est appelé le *composant* de x dans le sous-module M_ι ; si on le désigne par $k_\iota(x)$, on a la proposition suivante :

Proposition 6. *Quels que soient* $x \in E$, $y \in E$ *et* $a \in A$, *on a*

$$k_\iota(x+y) = k_\iota(x) + k_\iota(y) \tag{3}$$

$$k_\iota(ax) = a k_\iota(x) . \tag{4}$$

Autrement dit, k_ι est une *représentation* du module E sur le sous-module M_ι (cf. § 2).

En effet, on a, d'une part $x+y = \sum_\iota k_\iota(x+y)$, de l'autre, d'après (1) $x+y = \sum_\iota k_\iota(x) + \sum_\iota k_\iota(y) = \sum_\iota (k_\iota(x)+k_\iota(y))$; la déf. 7 entraîne donc (3) quel que soit ι . Démonstration analogue pour la formule (4) .

Si N est un sous-module quelconque de E , $k_\iota(N)$ est un sous-module de M_ι , qu'on appelle encore le <u>composant</u> de N dans M .

On sait (chap.I, §6, n°6) que la somme directe d'une famille <u>finie</u> de sous-modules est <u>isomorphe à leur produit</u>. D'une façon générale, si E est somme directe d'une famille quelconque $(M_\iota)_{\iota\in I}$ de sous-modules, l'application biunivoque qui, à tout $x\in E$, fait correspondre la famille (x_ι) de ses composantes, est, en vertu de la prop.6 , un <u>isomorphisme</u> (dit <u>canonique</u>) de E sur un <u>sous-module</u> M' du produit $M = \prod_{\iota\in I} M_\iota$; mais, comme un élément quelconque de M' n'a jamais qu'un nombre fini de coordonnées $\neq 0$, M' ne peut être identique à M que si I est fini. Dans tous les cas, M' est <u>somme directe</u> des modules <u>composants</u> M'_ι (n°3) du produit $\prod_{\iota\in I} M_\iota$, respectivement isomorphes aux M_ι .

Etant donnée une famille quelconque $(M_\iota)_{\iota\in I}$ de A-modules, on peut donc définir un module qui est somme directe d'une famille de sous-modules respectivement isomorphes aux M_ι ; il suffit de prendre, dans le produit $\prod_{\iota\in I} M_\iota$, le module M' , somme directe des modules composants M'_ι ; par abus de langage, on dira (lorsqu'aucune confusion n'en peut résulter) que M' est <u>la somme directe</u> de la famille (M_ι) ; lorsque tous les M_ι sont isomorphes à un même module M , leur somme directe se note $M^{(I)}$.

<u>Proposition 7</u>. <u>Soit</u> (M_ι) <u>une famille de sous-modules d'un module</u> E ; <u>le sous-module</u> N <u>de</u> E , <u>somme des</u> M_ι, <u>est isomorphe à un module quotient du module</u> M , <u>somme directe de la famille</u> (M_ι) .

En effet, tout élément de M est de la forme (x_ι) , où $x_\iota \in M_\iota$ pour tout ι , et $x_\iota = 0$ sauf pour un nombre fini d'indices ι .

Si à cet élément, on fait correspondre l'élément $\sum_{\iota \in I} x_\iota$ de E , on définit évidemment une <u>représentation</u> de M sur N , en vertu des formules (1) et (2), d'où la proposition.

<u>Définition 4</u>. <u>Dans un module E , on dit que deux sous-modules M_1, M_2 sont supplémentaires, si E est somme directe de M_1 et de M_2</u> .

D'après la prop.5, pour que M_1 et M_2 soient supplémentaires, il faut et il suffit que l'on ait $E = M_1 + M_2$, et $M_1 \cap M_2 = \{0\}$.

<u>Proposition 8</u>. <u>Si M_1 et M_2 sont deux sous-modules supplémentaires dans un module E , le module quotient E/M_1 est isomorphe à M_2</u> .

En effet, l'application $x \to k_2(x)$ qui à tout x fait correspondre son composant dans M_2, est une représentation de E sur M_2 (prop.6), et l'image réciproque de 0 par cette représentation est M_1 (fig.1).

On pourrait aussi démontrer cette proposition en s'appuyant sur l'isomorphie de E et de $M_1 \times M_2$, et le fait que $(M_1 \times M_2)/M_1$ est isomorphe à M_2 (chap.I, § 6) .

COROLLAIRE. <u>Deux sous-modules supplémentaires d'un même sous-module sont isomorphes</u>.

Si E est <u>somme directe</u> d'une famille $(M_\iota)_{\iota \in I}$ de sous-modules, et si (J_1, J_2) est une partition de I , les modules $N_1 = \sum_{\iota \in J_1} M_\iota$ et $N_2 = \sum_{\iota \in J_2} M_\iota$ (où les sommes sont évidemment <u>directes</u>, d'après la prop.5) sont <u>supplémentaires</u> dans E , car on a évidemment $E = N_1 + N_2$, et la relation $\sum_{\iota \in J_1} x_\iota = \sum_{\iota \in J_2} x_\iota$ entraîne $x_\iota = 0$ pour tout ι , d'après la déf. 7 .

Plus généralement, si $(J_\lambda)_{\lambda \in L}$ est une partition quelconque de I , et si on pose $N_\lambda = \sum_{\iota \in J_\lambda} M_\iota$, (somme qui est directe), E est <u>somme directe</u> des N_λ . Réciproquement, si la famille $(M_\iota)_{\iota \in I}$ est telle que,

pour chaque $\lambda \in L$, la somme N_λ de la famille $(M_\iota)_{\iota \in J_\lambda}$ soit directe, et que E soit somme directe de la famille $(N_\lambda)_{\lambda \in L}$, E est également somme directe de la famille $(M_\iota)_{\iota \in I}$.

8. Systèmes libres. Bases. Définition 10. Dans un A-module unitaire E, on dit qu'une famille $(a_\iota)_{\iota \in I}$ d'éléments distincts et $\neq 0$ est un système libre si la somme des modules monogènes $A.a_\iota$ engendrés par les a_ι est directe.

Cette définition équivaut donc à la suivante : la relation $\sum_{\iota \in I} \lambda_\iota a_\iota = 0$ (où $\lambda_\iota = 0$ sauf pour un nombre fini d'indices) entraîne $\lambda_\iota a_\iota = 0$ pour tout $\iota \in I$.

En général, quand (a_ι) est un système libre dans un module E, la relation $\sum_\iota \lambda_\iota a_\iota = 0$ entraîne $\lambda_\iota a_\iota = 0$ pour tout ι, mais non nécessairement $\lambda_\iota = 0$ pour tout ι. Il en est toutefois ainsi lorsque tous les a_ι sont des éléments réguliers de E, et en particulier lorsque (a_ι) est un système libre dans un espace vectoriel. Si une famille d'éléments d'un espace vectoriel forment un système libre, on dit encore qu'ils sont linéairement indépendants.

Toute famille d'éléments distincts d'un module E, qui n'est pas un système libre, est encore appelée système lié ; lorsque E est un espace vectoriel, on dit aussi que les éléments d'un système lié sont linéairement dépendants.

D'après la déf. 10, aucun élément $a_\varkappa$ d'un système libre (a_ι) ne peut être égal à une combinaison linéaire des a_ν d'indice $\neq \varkappa$. Mais inversement, une famille (a_ι) qui remplit cette condition n'est pas nécessairement un système libre.

Par exemple, soit A un anneau d'intégrité ayant un élément unité, considéré comme A-module ; si a et b sont deux éléments

distincts et $\neq 0$, la combinaison linéaire $(-b)a+ab$ est égale à 0 sans que l'on ait $ab=0$, donc a et b forment un système lié. Mais il n'existe pas en général d'élément $x \in A$ tel que $b=xa$ ou $a=xb$.

Toutefois, dans un espace vectoriel E , on a la proposition suivante :

Proposition 9. Pour qu'une famille (a_ι) d'éléments distincts et $\neq 0$ d'un espace vectoriel soit un système libre, il faut et il suffit que, pour aucun indice $\varkappa$, $a_\varkappa$ ne soit égal à une combinaison linéaire des a_ι d'indice $\iota \neq \varkappa$.

En effet, si on a $\lambda_\varkappa a_\varkappa + \sum_{\iota \neq \varkappa} \lambda_\iota a_\iota = 0$, avec $\lambda_\varkappa \neq 0$, on en tire $a_\varkappa = \sum_{\iota \neq \varkappa} (-\lambda_\varkappa^{-1} \lambda_\iota) a_\iota$.

Remarque. On notera qu'un système lié dans un module E sur un anneau A peut devenir libre quand on considère sur E la structure de module obtenue en restreignant le domaine d'opérateurs à un sous-anneau de A . Par exemple, soit K' un sous-corps d'un corps K , distinct de K ; si ε est l'élément unité commun de K et K' , et ξ un élément de K n'appartenant pas à K' , ε et ξ forment un système lié dans le K-module K_s , mais non dans le K-module obtenu en restreignant à K' le domaine d'opérateurs de K_s .

Définition 11. On appelle base d'un module unitaire E , tout système de générateurs de E qui est un système libre.

En d'autres termes, un module unitaire qui admet une base est un module somme directe d'une famille de sous-modules monogènes. Un module unitaire monogène admet évidemment une base ; tout élément qui l'engendre forme à lui seul une base d'un tel module.

D'après la déf.11, tout module unitaire engendré par un système libre admet pour base ce système. Plus généralement, si un module unitaire E est somme directe d'une famille de sous-modules $(M_\iota)_{\iota \in I}$ et si chacun des M_ι admet une base $(a_{\iota\varkappa})_{\varkappa \in K_\iota}$, la réunion des familles $(a_{\iota\varkappa})$, est une base de E .

Un module unitaire n'admet pas nécessairement de base. Par exemple, dans un anneau d'intégrité A ayant un élément unité, et considéré comme A-module, nous venons de voir qu'il n'existe pas de système libre ayant plus d'un élément ; un idéal non principal de A ne peut donc avoir de base ; or nous rencontrerons plus tard des anneaux dans lesquels il existe des idéaux non principaux (chap.V).

Définition 12. Soit A un anneau ayant un élément unité. On dit qu'une base A-module unitaire est régulière lorsque tous les éléments de cette base sont réguliers.

Par exemple, toute somme directe $A_s^{(L)}$ a une base régulière formée des éléments e_λ ($\lambda \in L$), où e_λ désigne l'élément dont tous les composants sont nuls, à l'exception du composant d'indice λ, qui est égal à l'élément unité ε de A ; cette base est appelée la base canonique de $A_s^{(L)}$.

Inversement, si un A-module unitaire E possède une base régulière $(a_\lambda)_{\lambda \in L}$, il est isomorphe au module $A_s^{(L)}$. En effet, tout x se met sous la forme $x = \sum_{\lambda \in L} \xi_\lambda a_\lambda$, où non seulement les éléments $\xi_\lambda a_\lambda$ sont déterminés de façon unique, mais aussi les éléments $\xi_\lambda \in A$; l'élément ξ_λ s'appelle la composante d'indice λ (ou, par abus de langage, coordonnée d'indice λ) de x ; d'après la prop.6, l'application qui à x fait correspondre la famille $(\xi_\lambda)_{\lambda \in L}$ de ses composantes est un isomorphisme de E sur $A_s^{(L)}$.

Si un module unitaire E par rapport à un anneau A possède une base régulière (a_λ), l'annulateur d'un élément $x \neq 0$ ne peut contenir que des diviseurs à gauche de 0 dans A, car si $x = \sum_\lambda \xi_\lambda a_\lambda$, et $ax=0$, on a $a\xi_\lambda = 0$ pour tout λ, et il existe au moins un $\xi_\lambda \neq 0$. En particulier, si A n'a pas de diviseur de 0, E est un module régulier.

9. Modules simples. Modules complètement réductibles. Définition 13. On appelle module simple un module E non réduit à 0, et ne contenant aucun sous-module autre que lui-même et $\{0\}$.

Proposition 10. Pour qu'un A-module unitaire E soit simple, il faut et il suffit qu'il satisfasse à l'une des deux conditions suivantes :

1° E est engendré par un quelconque de ses éléments $\neq 0$;

2° E est isomorphe à un module quotient $A_s/\mathfrak{a}$, où $\mathfrak{a}$ est un idéal à gauche maximal de A.

1° Un module engendré par un quelconque de ses éléments $\neq 0$ est évidemment simple, d'après la déf.13. Inversement, si E est simple, et si $a \in E$ est $\neq 0$, E contient le sous-module monogène A.a, qui n'est pas nul puisqu'il contient a ; donc $E = A.a$.

2° Pour qu'un module quotient $A_s/\mathfrak{a}$ de A_s soit simple, il faut et il suffit que $\mathfrak{a}$ soit un idéal à gauche maximal, car tout sous-module de $A_s/\mathfrak{a}$ est de la forme $\mathfrak{b}/\mathfrak{a}$, où $\mathfrak{b}$ est un idéal à gauche de A contenant $\mathfrak{a}$. D'autre part, d'après le 1°, si E est simple, il est monogène, donc isomorphe à un module quotient de A_s (prop.2).

Définition 14. On dit qu'un module est complètement réductible s'il est somme directe d'une famille de sous-modules simples.

Tout module complètement réductible unitaire admet donc une base d'après la prop. 10.

Théorème 1. Si un module E est somme d'une famille $(M_\iota)_{\iota\in I}$ de sous-modules simples, il est complètement réductible, et somme directe d'une sous-famille $(M_\iota)_{\iota\in J}$ de la famille $(M_\iota)_{\iota\in I}$.

Ce théorème va être une conséquence de la proposition suivante :

Proposition 11. Soit E un module somme d'une famille $(M_\iota)_{\iota\in I}$ de sous-modules simples, N un sous-module quelconque de E ; il existe un sous-module P supplémentaire de N, et somme directe d'une sous-famille $(M_\iota)_{\iota\in J}$ de la famille $(M_\iota)_{\iota\in I}$.

Le th.1 correspond au cas particulier de la prop.11 où $N=\{0\}$.

Pour démontrer la prop.11, désignons par $\mathfrak{F}$ la famille des parties $J\subset I$ telles que la somme $\sum_{\iota\in J} M_\iota$ soit directe et ait avec N une intersection réduite à 0 ; $\mathfrak{F}$ n'est pas vide, car la partie vide de I appartient à $\mathfrak{F}$. D'après la définition d'une somme infinie de modules et la prop.5, la proprieté "$J\in\mathfrak{F}$" est équivalente à "toute partie finie de J appartient à $\mathfrak{F}$" ; autrement dit, $\mathfrak{F}$ est un ensemble de parties de caractère fini (Bas.R, §6,n°11), donc possède un élément maximal J_0, en vertu du théorème de Zorn. Posons $P=\sum_{\iota\in J_0} M_\iota$; la somme N+P est directe puisque $N\cap P=\{0\}$; nous allons montrer que N+P=E, ce qui établira la proposition. Supposons donc $N+P\neq E$; il existe alors un indice λ tel que M_λ ne soit pas contenu dans N+P ; comme M_λ est simple, on a $M_\lambda\cap(N+P)=\{0\}$. On conclut de là que la somme $N+P+M_\lambda = N+(P+M_\lambda)$ est directe. Si on pose $J_1=J_0\cup\{\lambda\}$, la somme $\sum_{\iota\in J_1} M_\iota = P+M_\lambda$ est donc directe et son intersection avec N se réduit à 0, donc on a $J_1\in\mathfrak{F}$, ce qui contredit la définition de J_0.

C.Q.F.D.

Remarque. Lorsque E est somme d'une famille finie $(M_i)_{1 \leqslant i \leqslant n}$ de sous-modules simples, on peut démontrer la prop.11 sans faire intervenir l'axiome de choix. Soit en effet H la partie de l'intervalle $[1,n]$ de $\mathbf{N}$ formée des indices i tels que M_i ne soit pas contenu dans la somme $N + \sum_{j<i} M_j$; comme M_i est simple, on a $M_i \cap (N + \sum_{j<i} M_j) = \{0\}$ pour tout indice $i \in H$; on en conclut par récurrence que, pour tout indice k tel que $1 \leqslant k \leqslant n$, la somme $N + \sum_{j=1}^{k} M_j$ est somme directe de N et des M_i tels que $i \in H$ et $i \leqslant k$; en prenant k=n , on obtient la prop.11 .

En appliquant la prop.11 dans le cas particulier où E est somme directe de la famille (M_ι), on a le théorème suivant (cf. chap.I, §6, prop.14) :

Théorème 2 (théorème d'échange). Soit E un module complètement réductible, somme directe d'une famille $(M_\iota)_{\iota \in I}$ de sous-modules simples. Si N est un sous-module quelconque de E , il existe un sous-module P supplémentaire de N , somme (directe) d'une sous-famille $(M_\iota)_{\iota \in J}$ de la famille $(M_\iota)_{\iota \in I}$.

Ce théorème détermine complètement la structure des sous-modules et des modules quotients d'un module complètement réductible :

Proposition 12. Soit E un module complètement réductible, somme directe d'une famille $(M_\iota)_{\iota \in I}$ de sous-modules simples. Si N est un sous-module quelconque de E , N est complètement réductible : il existe une partie K de I et une famille $(N_\iota)_{\iota \in K}$ de sous-modules simples de N telle que N_ι soit isomorphe à M_ι pour tout $\iota \in K$, que N soit somme directe de la famille $(N_\iota)_{\iota \in K}$, et que E soit somme directe de N et des M_ι d'indice $\iota \in \complement K$.

En effet, avec les notations du th.2, soit K le complémentaire de J dans I , et posons $Q = \sum_{\iota \in K} M_\iota$; Q est supplémentaire de P , donc

donc (cor. de la prop.8) isomorphe à N ; cette remarque et le th.2 entraînent la prop.12.

On peut encore exprimer la prop.12 en disant que, dans la famille $(M_\iota)_{\iota \in I}$ dont E est somme directe, on peut échanger chacun des M_ι d'indice $\iota \in K$ avec le sous-module simple N_ι de même indice, sans que E cesse d'être somme directe de la nouvelle famille obtenue (d'où le nom de "théorème d'échange" donné au th.2).

Proposition 13. Tout module quotient d'un module complètement réductible E est complètement réductible, et isomorphe à un sous-module de E .

C'est un corollaire immédiat du th.2, en vertu de la prop.8 .

Théorème 3. Soient E et F deux modules complètement réductibles isomorphes, sommes directes respectivement des familles $(M_\iota)_{\iota \in I}$ et $(N_\varkappa)_{\varkappa \in K}$ de sous-modules simples. Si l'ensemble I est fini, il existe une application biunivoque φ de I sur K , telle que $N_{\varphi(\iota)}$ soit isomorphe à M_ι pour tout $\iota \in I$.

Tout revient à montrer que l'ensemble K est fini : le théorème n'est plus alors qu'une traduction, pour les modules, de la prop.13 du chap.I, § 6, relative aux groupes à opérateurs quelconques (proposition qui est elle-même une conséquence immédiate du th. de Jordan-Hölder).

Soit n le nombre d'éléments de I ; nous allons montrer qu'en fait le nombre d'éléments de K est $\leqslant n$. Sinon, il existerait un sous-module H de F , distinct de F et somme directe de n des sous-modules simples $N_\varkappa$. Si g est un isomorphisme de F sur E , g(H) serait un sous-module de E , distinct de E , et somme directe de n sous-modules simples ; E serait somme directe de g(H) et d'un certain nombre $p \geqslant 1$ de sous-modules M , d'après le th.2 ; mais cela contredit la prop. 13 du chap.I, § 6 .

On peut aussi donner du th.3 une démonstration s'appuyant sur le th.2, mais n'utilisant pas le th. de Jordan-Hölder. On raisonne par récurrence sur le nombre d'éléments n de I : le th. est évident pour n=1 ; supposons-le démontré pour $n < m$. Soit f un isomorphisme de E sur F , M_α un des sous-modules de la famille (M_ι) ; $f(M_\alpha)$ est un sous-module simple de F ; il admet un supplémentaire dans F , somme directe d'une sous-famille $(N_\varkappa)_{\varkappa \in J}$ de $(N_\varkappa)_{\varkappa \in K}$; par suite $f(M_\alpha)$ est isomorphe à la somme directe des $N_\varkappa$ d'indice $\varkappa \in \complement J$; comme $f(M_\alpha)$ est simple, $\complement J$ se réduit nécessairement à un seul indice β . Mais les supplémentaires $\sum_{\iota \neq \alpha} M_\iota$ et $\sum_{\varkappa \neq \beta} N_\varkappa$ de M_α et N_β respectivement dans E et F sont isomorphes, étant isomorphes respectivement à E/M et $F/f(M_\alpha)$; comme $\sum_{\iota \neq \alpha} M_\iota$ est somme directe de n-1 modules simples, le raisonnement par récurrence s'applique, et achève la démonstration.

Comme conséquence du th.3, on voit que s'il existe deux familles de sous-modules simples d'un module E , telles que E soit somme directe de chacune d'elles, et si l'une d'elles est <u>finie</u>, elles ont le <u>même nombre</u> d'éléments ; ce nombre, qui ne dépend donc que du module complètement réductible E , est ce que nous avons appelé sa <u>longueur</u> (chap.I, §6,n°15). On dit qu'un module complètement réductible somme directe d'une infinité de sous-modules simples est de <u>longueur infinie</u>. Un module complètement réductible de longueur finie est encore dit parfois <u>semi-simple</u> (chap.I, §6,n° 15) .

Le th. 3 entraîne les corollaires suivants :

<u>Corollaire 1</u>. <u>Dans un module semi-simple</u> E <u>de longueur</u> n , <u>tout sous-module est de longueur</u> $\leqslant n$; <u>un sous-module de longueur</u> n <u>est identique à</u> E . <u>Si</u> E <u>est unitaire, le nombre d'éléments de tout système libre d'éléments de</u> E <u>est</u> n ; <u>tout système libre de</u> n <u>éléments est une base de</u> E .

Si E est unitaire, le nombre d'éléments de tout système libre d'éléments de E est $\leqslant n$; tout système libre de n éléments est une base de E .

En effet, si N est un sous-module de E , P un sous-module supplémentaire de N , la longueur de E est la somme des longueurs de N et de P . La seconde partie de l'énoncé résulte de ce que la longueur d'un sous-module de E engendré par un système libre de p éléments est $\geqslant p$.

Corollaire 2. Soient M et N deux sous-modules complètement réductibles d'un module E , de longueurs respectives m et n. Si l'intersection $M \cap N$ est de longueur q , la somme $M+N$ est un module complètement réductible de longueur p telle que

(5) $$p + q = m + n$$

En effet, $(M+N)/(M \cap N)$ est somme des modules $M/(M \cap N)$ et $N/(M \cap N)$ de longueur m-q et n-q respectivement (chap.I, § 6, n°13) ; cette somme est évidemment directe, donc $p-q = (m-q)+(n-q)$.

Corollaire 3. Soit E un module complètement réductible, M et N deux sous-modules de E tels que E/M et E/N soient de longueurs finies m et n . Alors $E/(M \cap N)$ a une longueur finie q , $E/(M+N)$ a une longueur finie p , et on a

(6) $$p + q = m + n .$$

En effet, $E/(M \cap N)$ est somme directe d'un module isomorphe à E/M et d'un module isomorphe à $M/(M \cap N)$; ce dernier est isomorphe à $(M+N)/M$, lui-même sous-module de E/M , donc de longueur finie ; on voit en outre que $M/(M \cap N)$ a pour longueur q-m . De même $N/(M \cap N)$ a pour longueur q-n ; donc $(M+N)/(M \cap N)$, somme directe de $M/(M \cap N)$ et de $N/(M \cap N)$, a pour longueur $2q-(m+n)$; il est d'autre part de longueur q-p , d'où la relation (6) .

Remarques. 1) Le th.3 peut s'étendre au cas où I est un ensemble infini quelconque (exerc. 15).

2) On peut généraliser les th.1,2,3 et leurs conséquences aux groupes à opérateurs non commutatifs (chap.I, 6,ex.18)

10. Structure des espaces vectoriels. Dans un espace vectoriel E par rapport à un corps K, tout élément $x \neq 0$ est régulier, donc le sous-espace vectoriel monogène K.x engendré par x est isomorphe à K_s ; comme K ne contient pas d'idéal à gauche distinct de K et de (0), K.x est un module simple. Or, E est la réunion des sous-espaces K.x, lorsque x parcourt l'ensemble des éléments $\neq 0$ de E ; à fortiori, E est la somme de ces sous-espaces ; le th.1 prouve alors que E est complètement réductible, et est somme directe d'une famille de sous-espaces vectoriels monogènes K.a ; de façon plus précise:

Théorème 4. Quelle que soit la famille $(a_\iota)_{\iota \in I}$ d'éléments d'un espace vectoriel E engendrant cet espace, il existe une sous-famille $(a_\iota)_{\iota \in J}$ de $(a_\iota)_{\iota \in I}$ qui est une base de E.

Par exemple, tout anneau contenant un corps K, et dont l'élément unité est aussi élément unité de K, est un espace vectoriel à gauche sur K, et possède donc une base par rapport à K (voir §4). En particulier, tout sur-corps d'un corps K possède une base par rapport à K.* C'est ainsi que le corps des nombres réels R admet une base (infinie) par rapport au corps des nombres rationnels Q ; toute base de R par rapport à Q est appelée une base de Hamel. *

Tout espace vectoriel E sur un corps K est donc isomorphe à un espace de la forme $K_s^{(L)}$; de façon précise, si $(a_\lambda)_{\lambda \in L}$ est une base de E,

il existe un isomorphisme de E sur $K_s^{(L)}$ appliquant a_λ sur le vecteur e_λ de la base canonique (n°8) de $K_s^{(L)}$.

Le théorème d'échange (th.2) donne, pour les espaces vectoriels l'énoncé suivant :

Théorème 5. Soient $(a_\iota)_{\iota \in I}$ une base d'un espace vectoriel E, et H un sous-espace vectoriel quelconque de E. Il existe un sous-espace vectoriel H' supplémentaire de H, et ayant pour base une sous-famille $(a_\iota)_{\iota \in J}$ de la base $(a_\iota)_{\iota \in I}$.

Corollaire. Si $(a_\iota)_{\iota \in I}$ est une base d'un espace vectoriel E, $(b_\lambda)_{\lambda \in L}$ un système libre quelconque d'éléments de E, il existe une partie J de I telle que la famille formée des b_λ $(\lambda \in L)$ et les a_ι tels que $\iota \in J$ soit une base de E.

Il suffit en effet d'appliquer le th.2 au sous-espace vectoriel engendré par le système libre (b_λ).

Remarque. De ce corollaire, et du th.1, on déduit plus généralement que, si $(b_\lambda)_{\lambda \in L}$ est une famille quelconque d'éléments de E, il existe une partie H de L et une partie J de I telles que $(b_\lambda)_{\lambda \in H}$ soit un système libre engendrant le même sous-espace vectoriel V que la famille $(b_\lambda)_{\lambda \in L}$, et que la famille formée des b_λ tels que $\lambda \in H$ et des a_ι tels que $\iota \in J$ soit une base de E.

Lorsque I est fini, on peut démontrer ce résultat sans faire appel à l'axiome du choix, par exemple par le raisonnement que nous avons indiqué pour la prop.11. On peut aussi modifier légèrement ce raisonnement de la façon suivante : supposons que $I = [1,n]$, et désignons par B_0 la base $(a_i)_{1 \leqslant i \leqslant n}$. Soit b_{λ_1} un élément $\neq 0$ de la famille (b_λ) ; les n+1 éléments $b_{\lambda_1}, a_1, \ldots, a_n$ forment

un système lié ; soit i_1 le plus petit des indices i tels que a_i soit combinaison linéaire de b_{λ_1} et des a_j d'indice $\neq i$; alors b_{λ_1} et les a_i d'indice $\neq i_1$ forment une base B_1 de E , car s'ils ne formaient pas un système libre, b_{λ_1} serait une combinaison linéaire des a_i d'indice $\neq i_1$, et par suite il en serait de même de a_{i_1} , contrairement à l'hypothèse.

Si b_{λ_1} engendre V , la proposition est démontrée ; sinon, il existe un indice λ_2 tel que b_{λ_2} et b_{λ_1} forment un système libre ; par le même raisonnement que ci-dessus (en remplaçant la base B_0 par B_1) , on voit qu'il existe un indice $i_2 \neq i_1$ tel que b_{λ_1} , b_{λ_2} et les a_i d'indice $\neq i_1$ et $\neq i_2$ forment une base B_2 de E . Continuant le raisonnement par récurrence, on aboutit à une base de E formée de $p \leqslant n$ éléments b_{λ_k} $(1 \leqslant k \leqslant p)$ de la famille (b_λ) et de n-p éléments de la base (a_i) , les b_{λ_k} formant une base de V .

Lorsque I et L sont des ensembles <u>explicités</u>, et que les composantes des b_λ par rapport à la base (a_i) sont également explicitées, le procédé que nous venons de décrire permet de déterminer <u>explicitement</u> les b_{λ_k} ; en effet, si $b_{\lambda_1} = \sum_{i=1}^{n} \rho_i a_i$, l'indice i_1 est le plus grand des indices i tels que $\rho_i \neq 0$; on a par suite $a_{i_1} = \rho_{i_1}^{-1} b_{\lambda_1} + \sum_{i \neq i_1} \rho_{i_1}^{-1} \rho_i a_i$, et en portant dans les b_λ d'indice $\neq \lambda_1$, on a leurs composantes explicitées par rapport à la base B_1 , ce qui permet de continuer explicitement la récurrence (méthode "des substitutions successives").

Enfin, du th.3, on déduit :

<u>Théorème 6</u>. <u>Si un espace vectoriel E a une base finie de n éléments, toute autre base de E a aussi n éléments</u>.

Si un espace vectoriel E , par rapport à un corps K a une base finie, sa longueur n'est autre que le nombre d'éléments de cette base ; on l'appelle plus souvent le rang ou la dimension (ou encore le nombre de dimensions) de E par rapport à K. On appelle rang d'une partie quelconque M d'un espace vectoriel E la dimension du sous-espace vectoriel engendré par M (lorsque ce nombre est fini).

Corollaire 1. Soient E et F deux espaces vectoriels sur un même corps K , dont l'un est de dimension finie. Pour qu'ils soient isomorphes, il faut et il suffit qu'ils aient même dimension par rapport à K .

C'est une conséquence immédiate du th.6 .

Corollaire 2. Dans un espace vectoriel E , de dimension n , tout système libre a n éléments au plus (en d'autres termes, tout ensemble de m éléments est un système lié si $m > n$) ; tout système libre de n éléments est une base de E .

C'est la traduction du cor.1 du th.3 pour les espaces vectoriels. Nous laissons au lecteur la traduction analogue des cor.2 et 3 du th.3 .

11. Restriction du corps d'opérateurs d'un espace vectoriel. Soit E un espace vectoriel par rapport à un corps K ; si on restreint l'ensemble des opérateurs à un sous-anneau A de K , E est un A-module régulier. On notera qu'en général un sous-module de E (par rapport à l'anneau A) n'est pas un sous-espace vectoriel de E . De même, en général, E , considéré comme A-module, n'admet pas de base.

Par exemple, si A est un anneau d'intégrité ayant un élément unité, et K son corps des fractions (chap.I, § 9) , dans K , considéré comme A-module, il n'existe pas de système libre ayant plus d'un élément ; si $A \neq K$, K ne peut donc posséder de base par rapport à A .

Nous considèrerons plus particulièrement le cas où on restreint l'ensemble d'opérateurs de E à un sous-corps K' de K ; E devient alors un espace vectoriel par rapport à K' , et d'autre part K lui-même est aussi un espace vectoriel par rapport à K' . On a en outre la proposition suivante :

Proposition 14. Si $(a_\lambda)_{\lambda \in L}$ est une base de E par rapport à K , $(\gamma_\mu)_{\mu \in M}$ une base de K par rapport à K' , $(\gamma_\mu a_\lambda)_{(\lambda,\mu)\in L\times M}$ est une base de E par rapport à K'.

En effet, il est immédiat que la famille $(\gamma_\mu a_\lambda)$ engendre E , considéré comme espace vectoriel sur K' . Elle forme d'autre part un système libre, car une relation de la forme $\sum_{\lambda,\mu} \rho_{\lambda\mu}\gamma_\mu a_\lambda = 0$ avec $\rho_{\lambda\mu} \in K'$ ($\rho_{\lambda\mu}=0$ sauf pour un nombre fini de couples (λ,μ)) s'écrit $\sum_\lambda (\sum_\mu \rho_{\lambda\mu}\gamma_\mu)a_\lambda = 0$, donc entraîne $\sum_\mu \rho_{\lambda\mu}\gamma_\mu = 0$ quel que soit λ, et par suite $\rho_{\lambda\mu}=0$ quels que soient λ et μ .

Corollaire. Si E est de dimension m par rapport à K , et si K est de rang n par rapport à K' , E est de dimension mn par rapport à K' .

Toute famille d'éléments distincts de E , qui est un système libre par rapport à K , est a fortiori un système libre par rapport à K' , mais, comme nous l'avons déjà remarqué, la réciproque n'est pas vraie ; cependant, on a la proposition suivante :

Proposition 15. Soit (a_ι) un système libre par rapport à K , et soit H (resp. $H' \subset H$) le sous-espace vectoriel par rapport à K (resp. K') qu'il engendre ; toute famille d'éléments de H' qui est un système libre par rapport à K' est aussi un système libre par rapport à K .

D'après la définition de la somme d'une famille infinie d'éléments, tout se ramène à prouver la prop. 15 lorsque le système libre considéré (a_i) a un nombre fini n d'éléments. Soient $b_1, b_2, \ldots, b_m$ $(m \leqslant n)$ des éléments de H' formant

un système libre par rapport à K' ; il existe n-m éléments du système libre (a_i), par exemple $a_1,\dots,a_{n-m}$ formant avec les b_i une base de H' (par rapport à K') , donc les n éléments a_i sont des combinaisons linéaires, à coefficients dans $K' \subset K$, de $a_1,..,a_{n-m},b_1,\dots,b_m$; ces derniers engendrent par suite le sous-espace vectoriel H par rapport à K , et comme H a n dimensions, ils forment nécessairement un système libre par rapport à K .

Corollaire. Si M' est un sous-espace vectoriel de H' (par rapport à K'), M le sous-espace vectoriel de H (par rapport à K) engendré par M' , on a $M' = M \cap H'$.

En effet, soit (b_ι) une base de M' par rapport à K' ; (b_ι) est aussi une base de M par rapport à K , d'après la prop. 15. On a évidemment $M' \subset M \cap H'$; d'autre part, si $x \in M \cap H'$, on peut écrire $x = \sum_\iota \rho_\iota b_\iota$, avec $\rho_\iota \in K$; autrement dit, x et les b_ι forment un système lié par rapport à K ; comme ils appartiennent à H' , ils forment aussi un système lié par rapport à K' , d'après la prop.15 ; comme les b_ι forment un système libre par rapport à K' , x est égal à une combinaison linéaire des b_ι , à coefficients dans K' ; autrement dit, on a $\rho_\iota \in K'$, d'où $x \in M'$.

12. Bimodules. Soit E un ensemble muni d'une loi de groupe abélien et de deux lois externes dont les opérateurs sont respectivement deux anneaux A et B ; supposons que chacune de ces lois externes définisse (avec la structure de groupe de E) une structure de module sur E ; si en outre les deux lois externes sont permutables (chap.I, § 5), on dit qu'elles définissent sur E (avec la loi de groupe de E) une structure de bimodule par rapport aux anneaux A et B .

Si les structures de A-module et de B-module sur E ~~sont toutes deux des structures de A-module et de B-module sur E~~ sont toutes deux des structures de module à gauche, la permutabilité des lois externes s'exprime par l'identité $a(\beta x) = \beta(ax)$ quels que soient $a \in A$, $\beta \in B$, $x \in E$. Si au contraire E est par exemple un A-module à gauche et un B-module à droite, la permutabilité des lois externes s'exprime par l'identité $a(x\beta) = (ax)\beta$.

Exemples. 1) Supposons donnée sur un ensemble E une structure de module à gauche par rapport à un anneau A. Munissons également le groupe abélien E de la structure de module par rapport à $\mathbb{Z}$, dont la loi de composition externe est $(n,x) \to n.x$. Ces deux structures de module définissent sur E une structure de bimodule par rapport à A et $\mathbb{Z}$.

2) Sur un anneau A, l'addition, et les deux lois externes déduites par dédoublement (chap.I, § 5) de la multiplication, définissent une structure de bimodule par rapport à A lui-même.

Comme les modules, les bimodules sont des groupes abéliens à opérateurs particuliers ; toutes les propriétés générales de ces derniers leur sont donc applicables. Tout sous-groupe stable d'un bimodule E est un bimodule (dit sous-bimodule de E) ; tout groupe quotient (à opérateurs) de E par un sous-bimodule est un bimodule, dit bimodule quotient de E. Tout produit de bimodules est un bimodule. Nous laissons au lecteur le soin de transposer, pour les bimodules, les autres définitions et propriétés des modules données plus haut, en particulier les notions de somme directe, de bimodule simple et de bimodule complètement réductible.

Remarques. 1) On notera que, si E est un bimodule simple par rapport à deux anneaux A et B, il n'est pas en général un module simple quand on le considère seulement comme un A-module

ou un B-module. Par exemple, dans un anneau A, considéré comme bimodule par rapport à lui-même, les sous-bimodules sont les idéaux bilatères ; un idéal bilatère minimal n'est pas nécessairement un idéal à gauche minimal (ni un idéal à droite minimal ; voir chap.VII).

2) L'analogie qui apparaît entre les bimodules et les modules sera précisée au chap.III, §2, où on verra que, dans les cas les plus intéressants, on peut "assimiler" une structure de bimodule par rapport à deux anneaux A et B , à une structure de module par rapport à un troisième anneau C .

Exercices.- 1) Soit A un anneau n'ayant pas d'élément unité, A' l'anneau obtenu par adjonction à A d'un élément unité, suivant la méthode de l'exerc.3 du chap.I, §8 . Si E est un A-module quelconque, montrer que sa structure peut être considéré comme obtenue par restriction à A du domaine d'opérateurs d'un A'-module unitaire

2) Soit E un A-module, μ un élément central de A tel que $\mu x = \mu^2 x$ pour tout $x \in E$ (ce qui a lieu en particulier si μ est un idempotent (chap.I, §1,n°4) de A) ; montrer que E est somme directe du sous-module μE , et du sous-module M formé des $y \in E$ tels que $\mu y = 0$. En particulier, si ε est élément unité de A , E est somme directe du sous-module unitaire εE et d'un sous-module M tel que $aM = 0$ quel que soit $a \in A$.

3) Si E est un A-module quelconque, le sous-module monogène engendré par un élément $a \in E$ est identique à l'ensemble des éléments $n.a + \lambda a$, où n parcourt $\mathbb{Z}$, et λ parcourt A .

4) Soit M et N deux parties d'un A-module E , $\mathfrak{m}$ et $\mathfrak{n}$ leurs annulateurs ; montrer que l'annulateur de $M \cap N$ contient $\mathfrak{m} + \mathfrak{n}$; donner un exemple où il est distinct de $\mathfrak{m} + \mathfrak{n}$.

5) Dans un module produit $\prod_\iota E_\iota$, l'annulateur d'une partie F est l'intersection des annulateurs de ses projections.

6) La caractéristique d'un A-module unitaire est un diviseur de la caractéristique de A .

7) Si un A-module unitaire E admet une suite de Jordan-Hölder de longueur n , il existe un ensemble de n éléments engendrant E (remarquer que, si M et N sont deux sous-modules de E tels que M/N soit un module simple, il existe $a \in M$ tel que $M = N + Aa$) .

8) Si un A-module E admet une base <u>infinie</u> B , tout système de générateurs de E a une puissance au moins égale à celle de B (remarquer que si S est un système de générateurs de E , l'ensemble des éléments a_λ de B tels que le composant d'indice λ d'un élément au moins de S ne soit pas nul , est équipotent à S ; en déduire que si S était de puissance strictement inférieure à celle de B , il existerait un élément de B qui serait une combinaison linéaire des autres). En déduire que, si B' est une autre base de E , B et B' sont équipotentes.

9) a) Soit A un anneau ayant un élément unité, et tel que le A-module A_s admette une suite de Jordan-Hölder. Montrer que le module produit A_s^n ne peut être engendré par moins de n éléments (utiliser la prop.7 pour montrer que la somme de $m < n$ sous-modules monogènes de A_s^n est de longueur $\leqslant mp$, si p est la longueur de A_s) .

b) Soit B un sous-anneau de A ayant même élément unité que A .

Montrer de même que B_s^n ne peut être engendré par moins de n éléments (en considérant B_s^n comme une partie de A_s^n, montrer que dans le cas contraire, A_s^n serait aussi engendré par moins de n éléments). En déduire que si un B-module unitaire E admet une base régulière d'un nombre fini d'éléments, toute autre base régulière de E a le même nombre d'éléments.

10) Soit A un anneau sans diviseur de 0 et admettant un élément unité. Montrer que, pour $n>1$, le module A_s^n ne peut être monogène.

11) Soit A un anneau sans diviseur de 0 et admettant un élément unité. ~~Montrer que, pour n 1, le module A_s^n ne peut être monogène~~

~~14) Soit A un anneau sans diviseur de 0, ayant un élément unité.~~ Montrer que, si tout idéal à gauche de A est un A-module monogène, A admet un corps des quotients à gauche (chap.1, § 9, exerc.8) (utiliser l'exerc.10 et l'exerc.9 du chap.I, § 9).

12) Soit A un anneau sans diviseur de 0, ayant un élément unité.

a) Si A admet un corps des quotients à gauche K, et si E est un espace vectoriel sur K, M un A-module contenu dans E, montrer que toute partie de M qui est un système libre par rapport à l'anneau A est aussi un système libre par rapport à K (remarquer que, si a et b sont deux éléments $\neq 0$ de A, il existe deux éléments c,d de A tels que $ab^{-1}=c^{-1}d$).

b) Pour que dans le A-module A_s^n, il n'existe pas de système libre de plus de n éléments, il faut et il suffit que A admette un corps des quotients à gauche (pour voir que la condition est nécessaire, utiliser l'exerc.9 du chap.I, § 9 ; pour voir qu'elle est suffisante, utiliser a)).

13) Soit M un module simple par rapport à un anneau A.

Montrer que, ou bien on a $aM = \{0\}$ pour tout $a \in A$, et M a un nombre fini p d'éléments tel que p soit premier, ou bien pour tout $a \neq 0$ appartenant à M, on a $M = Aa$ (remarquer que, pour tout $x \in M$, $Ax \subset M$, et considérer le sous-module de M formé des $x \in M$ tels que $Ax = \{0\}$); dans le second cas, si $\mathfrak{a}$ est l'annulateur de a, $\mathfrak{a}$ est un idéal à gauche maximal de A, et M est isomorphe à $A/\mathfrak{a}$.

14) Soit E un A-module complètement réductible, somme directe d'une famille $(M_\iota)_{\iota \in I}$ de sous-modules simples. On dit que E est homogène si tous les M_ι sont isomorphes deux à deux. En général, si les M_ι sont quelconques, tout sous-module simple de E est isomorphe à un des M_ι (prop.12) ; si, pour chaque M_ι, on considère le sous-module G_ι de E, somme de tous les sous-modules simples de E isomorphes à M_ι, on dit que les G_ι sont les composants homogènes de E. Montrer que E est somme directe de ses composants homogènes distincts et que G_ι est la somme de tous les $M_\varkappa$ isomorphes à M_ι (utiliser la prop .5 et la prop.12).

15) a) Soit E un A-module complètement réductible homogène (exerc.14) somme directe d'une famille $(M_\iota)_{\iota \in I}$ de sous-modules simples deux à deux isomorphes. Si E est somme directe d'une seconde famille $(N_\varkappa)_{\varkappa \in K}$ de sous-modules simples, tous ces sous-modules sont isomorphes aux M_ι, et K est équipotent à I (distinguer deux cas d'après l'exerc.13, suivant que $A.E = \{0\}$, ou non ; dans le premier cas, considérer E comme un Z-module complètement réductible ; appliquer ensuite dans les deux cas l'exerc.8). Cas particulier des espaces vectoriels.

b) Soit E un A-module complètement réductible quelconque.

Si E est somme directe d'une famille $(M_\iota)_{\iota \in I}$ de sous-modules simples, et somme directe d'une seconde famille $(N_\kappa)_{\kappa \in K}$ de sous-modules simples, il existe une application biunivoque φ de I sur K telle que pour tout ι, $N_{\varphi(\iota)}$ soit isomorphe à M_ι (utiliser a) et l'exerc.14).

16) Soit K_0 un sous-corps d'un corps K tel que le rang de K par rapport à K_0 soit égal à 2 . Soit E un espace vectoriel à gauche par rapport à K , E_0 un sous-ensemble de E qui soit un espace vectoriel par rapport à K_0 . Soit V le plus grand sous-espace vectoriel de E (par rapport à K) contenu dans E_0 ; montrer que, si W_0 est un sous-espace vectoriel par rapport à K_0 , supplémentaire de V dans E_0 le sous-espace vectoriel W par rapport à K , engendré par W_0 , est tel que $V \cap W = \{0\}$ (autrement dit, la somme V+W est directe) (si $x_1, x_2, .., x_n$ est un système de points de W_0 , libre par rapport au corps K_0 , montrer qu'on ne peut avoir $\sum_{k=1}^{n} \lambda_k x_k \in E_0$ que si tous les λ_k appartiennent à K_0 ; on écrira les λ_k sous la forme $\rho_k + u\sigma_k$, où $u \in K$ et $\rho_k \in K_0$, $\sigma_k \in K_0$) .

Lorsque E a un nombre fini de dimensions par rapport à K , montrer que, si E_0 et E'_0 sont deux espaces vectoriels par rapport à K_0 , contenus dans E , V et V' les plus grands sous-espaces vectoriels de E (par rapport à K) contenus dans E_0 et E'_0 respectivement, pour qu'il existe un automorphisme de E transformant E_0 en E'_0 , il faut et il suffit que le nombre de dimensions de E_0 par rapport à K_0 soit égal à celui de E'_0 , et que le nombre de dimensions de V (par rapport à K) soit égal à celui de V' .

17) Soient E et F deux modules semi-simples isomorphes, V un sous-module de E , W un sous-module de F ; si V et W sont isomorphes,

E/V et F/W sont isomorphes. Montrer par un exemple que le résultat correspondant pour les modules complètement réductibles de longueure infinie est inexact.

18) Soit E un bimodule à gauche par rapport à un anneau A, à droite par rapport à un anneau B , les structures de A-module et de B-module de E étant unitaires. Montrer que, si $a \in E$, le sous-bimodule de E engendré par a est l'ensemble des sommes $\sum_i \alpha_i a \beta_i$, où (α_i) et (β_i) sont deux familles finies (ayant même nombres d'éléments, d'ailleurs quelconque) d'éléments de A et de B respectivement.

19) Si A et B sont deux anneaux dont les caractéristiques sont des nombres premiers entre eux, tout bimodule sur A et B est réduit à 0 .

§ 2. Fonctions linéaires. Dualité.

1. Fonctions linéaires. **Définition 1.** *Soient E et F deux modules par rapport au même anneau A . On appelle application linéaire de E dans F une représentation de E dans F* (chap.I, § 4) .

Autrement dit, une application linéaire u de E dans F est une application telle que $u(x+y)=u(x)+u(y)$ quels que soient $x \in E$, $y \in E$, et $u(\lambda x)=\lambda u(x)$ quels que soient $x \in E$ et $\lambda \in A$.

Remarque. Lorsque E et F sont deux groupes abéliens, considérés comme modules sur l'anneau $\mathbb{Z}$ (§ 1, n° 1), toute représentation u du groupe E dans le groupe F est aussi une application linéaire de E dans F , la relation $u(nx)=nu(x)$ étant une conséquence de l'identité $u(x+y) = u(x)+u(y)$.

Exemples. 1) La projection pr_J d'un produit $\prod_{\iota \in I} E_\iota$ d'une famille de modules sur un produit partiel $\prod_{\iota \in J} E_\iota$ est une application linéaire. De même, si un module E est somme directe d'une famille (M_ι) de sous-modules, et si $k_\iota(x)$ désigne le composant de $x \in E$ dans M_ι (§ 1, n° 7), k_ι est une application linéaire (§ 1, prop. 6).

2) Soit E un module à gauche sur un anneau A, a un élément de E ; l'application $\lambda \longrightarrow \lambda a$ du A-module A_s dans E est une application linéaire ; si on la désigne par θ_a, et si E est un module unitaire, on a (en désignant par ε l'élément unité de A), $\theta_a(\varepsilon)=a$.

Toutes les propriétés des représentations des groupes à opérateurs (chap. I, § 6) sont valables pour les applications linéaires ; nous les rappellerons brièvement :

Pour qu'une application d'un module E dans un module F soit un isomorphisme de E dans F, il faut et il suffit que ce soit une application linéaire biunivoque de E dans F.

Si u est une application linéaire de E dans F, u(E) est un sous-module de F ; $H=u^{-1}(0)$ est un sous-module de E, u(E) est isomorphe au module quotient E/H, u est composée d'un isomorphisme de E/H sur u(E) et de l'homomorphisme canonique de E sur E/H. Si M est un sous-module de E, u(M) est un sous-module de F, isomorphe aux modules quotients $M/(M \cap H)$ et $(M+H)/H$; en particulier, si la somme M+H est directe (c'est-à-dire si $M \cap H=\{0\}$), la restriction de u à M est un isomorphisme de M sur u(M).

Si M est un sous-module quelconque de E, la fonction u est compatible (Ens. R, § 5, n° 8) avec les relations de congruence $x \equiv y$ (M) dans E, $x' \equiv y'$ (u(M)) dans F ; par passage aux quotients, on en déduit une application $\dot{u}$ de E/M dans F/u(M), qui est une application linéaire de E/M sur u(E)/u(M) (chap. I, § 6) ; si φ est l'homomorphisme canonique de E

sur E/M, ψ celui de $u(E)$ sur $u(E)/u(M)$, on a $\mathring{u}\circ\varphi = \psi\circ u$.

Si M' est un sous-module de F, $u^{-1}(M')$ est un sous-module de E, contenant H ; le module quotient $u^{-1}(M')/H$ est isomorphe à $M'\cap u(E)$.

Si S est un système de générateurs du sous-module M de E, $u(S)$ est un système de générateurs de $u(M)$.

Enfin, si E,F,G sont trois modules sur un anneau A, u une application linéaire de E dans F, v une application linéaire de F dans G, la <u>composée</u> $v\circ u$ est une application linéaire de E dans G.

Nous désignerons par $\mathscr{L}(E,F)$ l'ensemble des applications linéaires d'un module E dans un module F. Si u et v sont deux telles applications, il est immédiat que $-u$ et $u+v$ sont encore des applications linéaires de E dans F ; donc $\mathscr{L}(E,F)$ est un <u>sous-groupe</u> additif du module produit F^E (ensemble des applications de E dans F) ; par contre, si A n'est pas commutatif, $w=au$ <u>n'est pas en général une application linéaire</u> de E dans F pour un $a\in A$; en effet on a $w(\lambda x)=au(\lambda x)=(a\lambda)u(x)$, et $\lambda w(x)=(\lambda a)u(x)$; on n'aura en général $w(\lambda x)=\lambda w(x)$ pour tout $\lambda\in A$ que si a appartient au <u>centre</u> C de A. En d'autres termes, $\mathscr{L}(E,F)$ n'est muni que d'une structure de module <u>par rapport à</u> C (et non par rapport à A).

<u>2. Applications linéaires d'espaces vectoriels</u>. Soient E et F deux espaces vectoriels sur un corps K, u une application linéaire de E dans F ; si $H=u^{-1}(0)$, $u(E)$ est isomorphe à l'espace vectoriel E/H ; donc, si G est un sous-espace vectoriel de E <u>supplémentaire</u> de H (§ 1, th. 5), $u(E)$ est <u>isomorphe à</u> G, et la restriction de u à G est un <u>isomorphisme</u> de G sur $u(G)=u(E)$. Si (a_ι) est une <u>base</u> de G (§ 1, n° 10), les éléments $u(a_\iota)$ forment donc une <u>base</u> de $u(E)$.

Définition 2. Si une application linéaire u d'un espace vectoriel E dans un espace vectoriel F est telle que $u(E)$ ait une dimension finie, cette dimension est appelée le rang de u, et se note $\rho(u)$.

Lorsque $u(E)$ a une dimension infinie, on dit encore que u est de rang infini.

Proposition 1. Soient E et F deux espaces vectoriels de dimensions respectives m et n ; pour toute application linéaire u de E dans F, on a

(1) $$\rho(u) \leqslant \mathrm{Min}(m,n) \quad ;$$

pour que $\rho(u)=m$, il faut et il suffit que u soit un isomorphisme de E dans F ; pour que $\rho(u)=n$, il faut et il suffit que u soit une application de E sur F.

Cela résulte aussitôt des remarques ci-dessus et du cor.1 du th.3 du § 1.

Corollaire. Soit E un espace vectoriel de dimension finie n ; pour qu'une application linéaire u de E dans lui-même soit un automorphisme de E, il faut et il suffit que l'une des trois conditions suivantes soit vérifiée :

a) u est de rang n ;

b) u est une application biunivoque de E dans E ;

c) u est une application de E sur E.

Au contraire, lorsque E est de dimension infinie, une application linéaire de E dans lui-même peut être biunivoque ou appliquer E sur lui-même, sans être un automorphisme de E (exerc. 15).

3. Applications linéaires d'un module quotient. Soit E un A-module, H un sous-module de E , φ l'application canonique de E sur le module quotient E/H . Si f est une application linéaire de E/H dans un A-module F , $f\circ\varphi$ est une application linéaire de E dans F , qui s'annule pour tout $x \in H$; réciproquement, si g est une application linéaire de E dans F ayant cette propriété, la relation $x \equiv y$ (mod.H) entraîne $g(x-y)=0$, c'est-à-dire $g(x)=g(y)$; g est donc compatible avec la relation $x \equiv y$ (mod.H) (Ens.R, § 5) et par suite est de la forme $f\circ\varphi$, où f est une application de E/H dans F ; on vérifie aussitôt que f est linéaire. En d'autres termes :

Proposition 2. Soient E et F deux A-modules, H un sous-module de E . Le module $\mathscr{L}(E/H,F)$ (par rapport au centre C de A) est isomorphe au sous-module de $\mathscr{L}(E,F)$ formé des applications linéaires de E dans F qui s'annulent dans H .

4. Applications linéaires d'une somme directe. Soient E et F deux modules sur un même anneau A , et supposons que E soit somme directe d'une famille (M_λ) de sous-modules. Pour tout $x \in E$, soit $h_\lambda(x)$ le composant de x dans M_λ ; on a $x = \sum_\lambda h_\lambda(x)$; si u est une application linéaire de E dans F , on peut écrire $u(x)=u(\sum_\lambda h_\lambda(x))=\sum_\lambda u(h_\lambda(x)) = \sum_\lambda u_\lambda(h_\lambda(x))$, en désignant par u_λ la restriction de u au sous-module M_λ . La valeur de u pour tout $x \in E$ est donc déterminée par la connaissance des restrictions de u aux M_λ . Inversement, donnons-nous, pour tout λ , une application linéaire u_λ de M_λ dans F ; si, pour tout $x \in E$, on pose $u(x)=\sum_\lambda u_\lambda(h_\lambda(x))$ (expression qui a un sens, puisque $h_\lambda(x)=0$, donc $u_\lambda(h_\lambda(x))=0$ sauf pour un nombre fini d'indices), il est immédiat que u est une application linéaire de E dans F, dont la restriction à M_λ est identique à u_λ . En résumé:

Proposition 3. Soient E et F deux modules sur un anneau A, tels que E soit somme directe d'une famille (M_λ) de sous-modules. Quelle que soit la famille (u_λ), où u_λ est une application linéaire de M_λ dans F, il existe une application linéaire u et une seule de E dans F, telle que la restriction de u à M_λ soit égale à u_λ pour tout λ.

Corollaire. Le module $\mathscr{L}(E,F)$ (par rapport au centre C de A) est isomorphe au module produit $\prod_\lambda \mathscr{L}(M_\lambda, F)$.

La prop.3 montre en particulier que si E est un module unitaire admettant une base (a_λ), toute application linéaire u de E dans F est entièrement déterminée par les valeurs des $u(a_\lambda)$. Mais en général, ces valeurs ne sont pas arbitraires dans F, car pour tout $\alpha \in A$ tel que $\alpha a_\lambda = 0$, on doit avoir $\alpha u(a_\lambda) = u(\alpha a_\lambda) = 0$; toutefois, si (a_λ) est une base régulière, et les b_λ des éléments arbitraires de F, il existe une application linéaire u (et une seule) de E dans F telle que $u(a_\lambda) = b_\lambda$ pour tout λ : c'est l'application qui à tout élément $\sum_\lambda \xi_\lambda a_\lambda$ fait correspondre $\sum_\lambda \xi_\lambda b_\lambda$. Cette remarque s'applique en particulier lorsque E et F sont des espaces vectoriels.

Reprenons les hypothèses de la prop.3, et supposons de plus que F soit aussi somme directe d'une famille (N_μ) de sous-modules. Pour tout $y \in F$, désignons par $k_\mu(y)$ le composant de y dans N_μ ; avec les notations précédentes, pour tout $x_\lambda \in M_\lambda$, on peut écrire $u_\lambda(x_\lambda) = \sum_\mu k_\mu(u_\lambda(x))$; si on pose $u_{\mu\lambda} = k_\mu \circ u_\lambda$, on voit que l'application u_λ est bien déterminée par la connaissance des applications linéaires $u_{\mu\lambda}$ de M_λ dans les N_μ ; mais cette famille d'applications linéaires n'est pas quelconque, car pour tout $x_\lambda \in M_\lambda$, il n'existe qu'un nombre fini d'indices μ tels que $u_{\mu\lambda}(x_\lambda) \neq 0$. Réciproquement, si pour chaque indice μ on se donne

une application linéaire $u_{\mu\lambda}$ de M_λ dans N_μ, ces applications satisfaisant à la condition précédente, et si, pour tout $x_\lambda \in M_\lambda$, on pose $u_\lambda(x_\lambda) = \sum_\mu u_{\mu\lambda}(x_\lambda)$ (expression qui a un sens en vertu de l'hypothèse), il est immédiat qu'on définit ainsi une application linéaire de M_λ dans F, telle que $k_\mu \circ u_\lambda = u_{\mu\lambda}$ pour tout indice μ. Tenant compte de la prop.3, on voit donc que si on se donne une famille $(u_{\mu\lambda})$, où $u_{\mu\lambda}$ désigne une application linéaire de M_λ dans N_μ, telle que, pour tout $x_\lambda \in M_\lambda$, il n'y ait qu'un nombre fini d'indices μ pour lesquels $u_{\mu\lambda}(x_\lambda) \neq 0$, il existe une application linéaire et une seule u de E dans F telle que, pour tout couple d'indices (λ, μ), et tout $x_\lambda \in M_\lambda$, on ait $k_\mu(u(x_\lambda)) = u_{\mu\lambda}(x_\lambda)$.

Soit G un troisième module sur A, somme directe d'une famille (P_ν) de sous-modules, et soit v une application linéaire de F dans G, $(v_{\nu\mu})$ la famille des applications linéaires qui lui correspond ($v_{\nu\mu}$ étant une application linéaire de N_μ dans P_ν); pour tout $x_\lambda \in M_\lambda$, on a

$$v(u_\lambda(x_\lambda)) = \sum_\mu v(u_{\mu\lambda}(x_\lambda)) = \sum_{\mu,\nu} v_{\nu\mu}(u_{\mu\lambda}(x_\lambda))$$

(la dernière somme ayant un sens puisque $u_{\mu\lambda}(x_\lambda) = 0$ sauf pour un nombre fini d'indices μ, et, pour ces derniers, $v_{\nu\mu}(u_{\mu\lambda}(x_\lambda)) = 0$ sauf pour un nombre fini d'indices ν). Désignons par $w_{\nu\lambda}$ l'application $x_\lambda \to \sum_\mu v_{\nu\mu}(u_{\mu\lambda}(x_\lambda))$ de M_λ dans P_ν; on écrit par abus de langage

$$w_{\nu\lambda} = \sum_\mu v_{\nu\mu} \circ u_{\mu\lambda} \qquad (2)$$

Il résulte de ce qui précède que la famille $(w_{\nu\lambda})$ ainsi définie correspond à l'application linéaire <u>composée</u> $v \circ u$.

5. <u>Endomorphismes d'un module</u>. Soit E un module sur un anneau A; conformément aux définitions générales (chap.I, § 4), un <u>endomorphisme</u> de E est une <u>application linéaire de</u> E <u>dans</u> E; l'ensemble de ces endomorphismes est

est donc l'ensemble que nous avons noté $\mathscr{L}(E,E)$; nous le noterons désormais $\mathscr{L}(E)$ pour abréger ; il est immédiat que c'est un anneau dont l'élément unité est l'application identique de E sur lui-même. La loi externe $(\gamma,u)\to\gamma u$ entre opérateurs γ appartenant au centre C de A, et endomorphismes u de E, définit sur $\mathscr{L}(E)$ une structure d'anneau à opérateurs (chap.I, § 8), car pour deux endomorphismes quelconques u,v de E, on a $(\gamma u)\circ v = u\circ(\gamma v) = \gamma(u\circ v)$.

L'anneau $\mathscr{L}(E)$ (sans opérateurs) est un sous-anneau de l'anneau $\mathscr{E}$ des endomorphismes du groupe additif (sans opérateurs) de E ; si, pour $a\in A$, u_a désigne l'homothétie $x\to ax$ de E, on sait que les u_a forment un sous-anneau A_1 de $\mathscr{E}$, isomorphe à l'anneau quotient $A/\mathfrak{a}$, où $\mathfrak{a}$ est l'annulateur de E. Le sous-anneau $\mathscr{L}(E)$ peut être défini comme formé des éléments de $\mathscr{E}$ permutables avec tous les éléments de A_1. On a déjà remarqué ci-dessus (n°1) qu'en général une homothétie quelconque de E n'est pas un endomorphisme du module E, autrement dit que $\mathscr{L}(E)$ ne contient pas A_1 en général

Les automorphismes d'un module E ne sont autres que les éléments inversibles de l'anneau $\mathscr{L}(E)$; ils forment un groupe, qu'on désigne par la notation $GL(E)$, et qu'on appelle groupe linéaire relatif au module E ; dans le cas où $E = A_s^n$, on écrit aussi $GL_n(A)$ au lieu de $GL(A_s^n)$.

6. Formes linéaires. Dual d'un module. Définition 3. Etant donné un module à gauche E sur un anneau A, on appelle forme linéaire sur E une application linéaire de E dans le A-module A_s (anneau A considéré comme module à gauche par rapport à lui-même).

L'ensemble $\mathscr{L}(E,A_s)$ des formes linéaires sur E forme un module par rapport au centre C de A. Mais en outre, pour toute forme linéaire u et tout $a\in A$, l'application $x\to u(x)a$ est encore une forme linéaire,

car pour tout $\beta \in A$, on a $u(\beta x)a = (\beta u(x))a = \beta(u(x)a)$; on désignera cette forme linéaire par ua , et on voit qu'on définit ainsi sur $\mathscr{L}(E,A_s)$ une structure de <u>module à droite</u> par rapport à A . Muni de cette structure, $\mathscr{L}(E,A_s)$ s'appelle le <u>module dual</u> (ou simplement le <u>dual</u>) de E ; nous le noterons désormais E' .

<u>Remarque</u>. Le fait qu'il existe une structure de A-module à droite sur l'ensemble des formes linéaires tient à ce qu'il existe, sur A , une structure de A-module à droite, dont la loi externe est <u>permutable</u> avec la loi externe du A-module à gauche A_s . De la même manière, il existera une structure de A-module à droite sur l'ensemble $\mathscr{L}(E,F)$, chaque fois que F sera un <u>bimodule</u> (à gauche et à droite) par rapport à A .

On définit de même manière le dual d'un A-module à droite ; c'est un A-module <u>à gauche</u>.

<u>Proposition 4</u>. <u>Si</u> A <u>est un anneau ayant un élément unité, le dual du module à gauche</u> A_s (resp. <u>du module à droite</u> A_d) <u>est isomorphe au module à droite</u> A_d (resp. <u>au module à gauche</u> A_s) .

En effet, si u est une forme linéaire sur A_s , et ε l'élément unité de A , on a pour tout $\lambda \in A$, $u(\lambda)=u(\lambda\varepsilon)=\lambda u(\varepsilon)=\lambda a$, en posant $a = u(\varepsilon)$; réciproquement, pour tout $a \in A$, $\lambda \longrightarrow \lambda a$ est une forme linéaire sur A_s ; l'application $u \rightarrow u(\varepsilon)$ est donc un isomorphisme du dual de A_s sur A_d . Démonstration analogue pour A_d .

En raison de cette isomorphie, on <u>identifie</u> d'ordinaire le dual de A_s (resp. A_d) à A_d (resp. A_s), une forme linéaire u étant identifiée à $u(\varepsilon)$.

<u>Remarque</u>. Il peut se faire que le dual d'un module non réduit à 0 soit <u>nul</u> ; par exemple, supposons que l'anneau A n'ait pas de diviseur de 0 , et soit E un A-module à gauche dont l'annulateur $\mathfrak{a}$ ne soit pas nul ; pour toute forme linéaire u sur E , tout élément

$x \in E$ et tout $a \in \mathfrak{a}$, on doit avoir $au(x)=u(ax)=u(0)=0$, et comme il existe des éléments $\neq 0$ dans $\mathfrak{a}$, on doit avoir $u(x)=0$ pour tout $x \in E$, c'est-à-dire $u=0$. En pareil cas, on considère souvent, au lieu du dual de E (qui ne présente alors aucun intérêt) le dual du <u>module normal associé</u> à E, qui, lui, n'est pas nul en général.

Soit E un A-module à gauche, E' son dual; à tout couple d'éléments $x \in E$, $x' \in E'$, correspond l'élément $x'(x) \in A$; on le désignera souvent par la notation $\langle x,x' \rangle$. L'application $(x,x') \longrightarrow \langle x,x' \rangle$ est appelée la <u>forme bilinéaire fondamentale</u> définie sur $E \times E'$ (cf. chap. III et VIII) ; on a identiquement

$$\langle x+y,x' \rangle = \langle x,x' \rangle + \langle y,x' \rangle \tag{3}$$

$$\langle x,x'+y' \rangle = \langle x,x' \rangle + \langle x,y' \rangle \tag{4}$$

$$\langle ax,x' \rangle = a\langle x,x' \rangle \tag{5}$$

$$\langle x,x'a \rangle = \langle x,x' \rangle a \quad . \tag{6}$$

Toute forme linéaire x' sur E peut donc être considérée comme l'application <u>partielle</u> (<u>Ens</u>. R, § 3, n° 13) $x \to \langle x,x' \rangle$ engendrée par la forme bilinéaire fondamentale.

De même, pour tout $x \in E$, l'application partielle $x' \to \langle x,x' \rangle$ est une <u>forme linéaire sur</u> E' ; si on la désigne par $\tilde{x}$, on voit que l'application $x \to \tilde{x}$ est une <u>application linéaire</u> (dite <u>canonique</u>) de E <u>dans</u> le <u>dual</u> E'' <u>de son dual</u> (qu'on appelle souvent le <u>bidual</u> de E).

Cette application n'est en général, ni une application de E <u>sur</u> E'', ni un <u>isomorphisme</u> de E <u>dans</u> E'' (cf. exerc. 9).

7. <u>Orthogonalité</u>. <u>Définition 4</u>. <u>Soit</u> E <u>un module</u>, E' <u>son dual ; on dit qu'un élément</u> $x \in E$ <u>et un élément</u> $x' \in E'$ <u>sont orthogonaux</u> (*) <u>si</u> $\langle x,x' \rangle = 0$.

On dit aussi que x est <u>orthogonal à</u> x', et x' <u>orthogonal à</u> x.

La déf. 4 exprime que x appartient au <u>sous-module</u> $^{-1}x'(0)$ de E.

On dit qu'une partie non vide M de E et une partie non vide M' de E' sont des ensembles <u>orthogonaux</u> si, quels que soient $x \in M$, $x' \in M'$, x et x' sont orthogonaux.

<u>Définition 5</u>. <u>Etant donnée une partie non vide quelconque</u> M (resp. M') <u>de</u> E (resp. E'), <u>on appelle sous-module totalement orthogonal à</u> M (resp. M') (ou simplement sous-module <u>orthogonal</u> à M (resp. M') par abus de langage, quand aucune confusion n'est à craindre) <u>l'ensemble des</u> $x' \in E'$ (resp. $x \in E$) <u>qui sont orthogonaux à tous les éléments de</u> M (resp. M') ; <u>on le note</u> $M^{\perp}$ (resp. $M'^{\perp}$).

Cette définition est justifiée, car si x' et y' sont orthogonaux à tous les $x \in M$, il en est de même de $x'+y'$ et de $x'a$ pour tout $a \in A$; de même pour les éléments de E orthogonaux à tous les éléments de M'.

Si M et N (resp. M' et N') sont deux parties de E (resp. E') telles que $M \subset N$ (resp. $M' \subset N'$), on a $N^{\perp} \subset M^{\perp}$ (resp. $N'^{\perp} \subset M'^{\perp}$). Si (M_ι) (resp. (M'_ι)) est une famille de parties de E (resp. E'), le sous-module orthogonal à la <u>réunion</u> des M_ι (resp. M'_ι) est l'<u>intersection</u> $\bigcap_\iota M_\iota^{\perp}$ (resp. $\bigcap_\iota M'^{\perp}_\iota$) ; ce sous-module est aussi le sous-module orthogonal au <u>sous-module</u> engendré par la réunion des M_ι (resp. M'_ι).

<u>Remarque</u>. Il n'existe pas d'élément $x' \in E'$ autre que 0 qui soit orthogonal à tous les $x \in E$, car la relation $\langle x,x' \rangle = 0$ pour tout $x \in E$ signifie $x'=0$; on a donc $E^{\perp} = \{0\}$. Par contre on peut avoir $E'^{\perp} \neq \{0\}$, c'est-à-dire qu'il peut exister des éléments $x \neq 0$ de E qui <u>annulent toutes les formes linéaires</u> sur E . Un élément $x \in E$ aura par exemple cette propriété si son annulateur contient un élément $a \in A$ qui n'est pas diviseur à gauche de 0 ; on a en effet, pour tout $x' \in E'$, $a\langle x,x' \rangle = \langle ax,x' \rangle = \langle 0,x' \rangle = 0$, ce qui entraîne $\langle x,x' \rangle = 0$ d'après l'hypothèse.

Pour toute partie non vide M de E , le sous-module $M^{\perp\perp}$ de E , orthogonal à $M^{\perp}$, est l'ensemble des $x \in E$ qui annulent toutes les formes linéaires s'annulant pour tous les éléments de M , ou encore l'intersection des sous-modules de la forme $^{-1}x'(0)$ qui contiennent M ; $M^{\perp\perp}$ contient donc le sous-module engendré par M , mais il peut en être distinct .

C'est ce qui se passe par exemple lorsque $E'^{\perp} = \{0\}$, et qu'on prend $M = \{0\}$.

De même, pour toute partie non vide M' de E' , $M'^{\perp\perp}$ est un sous-module contenant le sous-module engendré par M' , mais peut en être distinct (voir n° 9) .

8. Dual d'un module quotient. Dual d'une somme directe. Proposition 5. Le dual d'un module quotient E/M est isomorphe au sous-module $M^{\perp}$ de E' orthogonal à M .

Cette proposition n'est qu'un cas particulier de la prop.2. D'après la démonstration de la prop.2, on établit une isomorphie entre le dual de E/M et $M^{\perp}$ en faisant correspondre à toute forme linéaire u sur E/M la forme linéaire $u \circ \varphi$ sur E , où φ est l'homomorphisme canonique de E sur E/M .

Proposition 6. Si un module E est somme directe d'une famille (M_λ) de sous-modules, son dual E' est isomorphe au module produit $\prod_\lambda M'_\lambda$ des duals des M_λ .

C'est un cas particulier de la prop.3 : on y a vu qu'on établit une isomorphie entre E' et $\prod_\lambda M'_\lambda$ en faisant correspondre à toute forme linéaire x' sur E la famille (x'_λ) de ses restrictions aux M_λ .

Lorsque E est somme directe d'un nombre fini de sous-modules, la prop.6 se précise de la façon suivante :

Proposition 7. *Soit* E *un module somme directe d'une famille finie* $(M_i)_{1 \leqslant i \leqslant n}$ *de sous-modules ; pour tout indice* i *, soit* N_i *le sous-module* $\sum_{j \neq i} M_j$ *, supplémentaire de* M_i *. Le dual* E' *de* E *est somme directe des sous-modules* $N_i^\perp$ *orthogonaux aux* N_i *, et pour chaque indice* i *,* $N_i^\perp$ *est isomorphe au dual* M_i' *de* M_i *.*

Soit $h_i(x)$ le composant de $x \in E$ dans le sous-module M_i . On a $x = \sum_{i=1}^{n} h_i(x)$, et par suite, pour toute forme linéaire $x' \in E'$, $x'(x) = \sum_{i=1}^{n} x'(h_i(x))$, autrement dit $x' = \sum_{i=1}^{n} x' \circ h_i$. Pour $x \in N_i$, on a $h_i(x)=0$, donc $x' \circ h_i$ appartient au sous-module $N_i^\perp$, et on a bien $E' = \sum_{i=1}^{n} N_i^\perp$; d'autre part, cette somme est directe, car si une forme linéaire x' appartient à la fois à $N_i^\perp$ et à $\sum_{j \neq i} N_j^\perp$, on a $x'(x)=0$ pour $x \in N_i$ et $x'(x)=0$ pour $x \in M_i$, puisque M_i est contenu dans tous les N_j d'indice $\neq i$; comme M_i et N_i sont supplémentaires, on a $x'=0$. Pour établir la dernière partie de l'énoncé, il suffit d'appliquer la prop.5, en remarquant que M_i , supplémentaire de N_i , est isomorphe à E/N_i .

En raison de la prop.7, on identifie souvent le dual M_i' de M_i au sous-module $N_i^\perp$, en identifiant à toute forme linéaire u sur M_i la forme linéaire $x' \in N_i^\perp$ qui prolonge u sur E , et est bien déterminée en vertu de la prop.3 .

Corollaire 1. *Le sous-module* $M_i^\perp$ *, orthogonal à* M_i *, est égal à* $\sum_{j \neq i} N_j^\perp$.

En effet, comme M_i est contenu dans chacun des N_j d'indice $\neq i$, $M_i^\perp$ contient $\sum_{j \neq i} N_j^\perp$; d'autre part, la prop.7, appliquée à la décomposition de E en somme directe de M_i et N_i , montre que E' est somme directe de $M_i^\perp$ et $N_i^\perp$; comme E' est aussi somme directe de $\sum_{j \neq i} N_j^\perp$ et de $N_i^\perp$, on a $M_i^\perp = \sum_{j \neq i} N_j^\perp$.

Corollaire 2. *Si un sous-module* M *de* E *admet un supplémentaire, le dual de* M *est isomorphe au module quotient* $E'/M^\perp$.

C'est une conséquence immédiate de la prop.7, appliquée pour $n=2$.

2 Lorsque M n'admet pas de supplémentaire dans E, le corollaire précédent n'est plus exact en général (voir exerc. 8).

Un cas particulier important de la prop.7 est celui où E est un A-module à gauche unitaire admettant une <u>base régulière finie</u> $(a_i)_{1 \leqslant i \leqslant n}$. Comme E est alors isomorphe à A_s^n, il résulte des prop.4 et 7 que E' est isomorphe à A_d^n. De façon précise, pour tout $x = \sum_{i=1}^{n} \xi_i a_i$ désignons par $a_i'(x)$ la composante ξ_i de x ; a_i' est une forme linéaire sur E qu'on appelle <u>forme coordonnée d'indice i</u> (relative à la base (a_i)). Il est facile de voir que (a_i') est une <u>base régulière</u> du dual E' : en effet, pour toute forme linéaire $x' \in E'$, on a $x'(x) = \sum_{i=1}^{n} \xi_i x'(a_i) = \sum_{i=1}^{n} a_i'(x) x'(a_i)$, ou encore $x' = \sum_{i=1}^{n} a_i' . x'(a_i)$; inversement, pour toute forme linéaire $y' = \sum_{i=1}^{n} a_i' \beta_i$, on a $y'(a_j) = \beta_i$ puisque $a_i'(a_i) = \varepsilon$ (élément unité de A), et $a_j'(a_i) = 0$ pour $j \neq i$. Si on pose $M_i = A.a_i$, on voit (avec les notations de la prop.7) que $M_i^{\perp} = a_i'.A$. La base (a_i') est dite <u>base duale</u> de la base (a_i) ; elle est <u>caractérisée</u> (prop.3) par les relations

$$(7) \qquad \langle a_i, a_i' \rangle = \varepsilon , \qquad \langle a_i, a_j' \rangle = 0 \quad \text{pour} \quad j \neq i$$

Pour deux éléments $x = \sum_{i=1}^{n} \xi_i a_i$, $x' = \sum_{i=1}^{n} a_i' \xi_i'$, on a

$$(8) \qquad \langle x, x' \rangle = \sum_{i=1}^{n} \xi_i \xi_i' .$$

Les relations (7) prouvent que l'application $x \to \tilde{x}$ de E dans son bidual E" est un <u>isomorphisme de E sur E"</u> ; aussi <u>identifie-t-on</u> en général E et E" (à l'aide de l'isomorphisme canonique), ce qui permet de dire, d'après (7), que (a_i) est la <u>base duale</u> de (a_i').

Lorsque E admet une base régulière <u>infinie</u> $(a_\lambda)_{\lambda \in L}$, on sait (prop.6) que si on pose $M_\lambda = A.a_\lambda$, on peut identifier E' avec le produit $\prod_\lambda M_\lambda'$ (isomorphe à A_d^L), une forme linéaire x' étant identifiée avec la famille (x'_λ) de ses restrictions aux M_λ, ou, ce qui revient au même, avec la famille (ξ'_λ), où $\xi'_\lambda = x'(a_\lambda)$;

les ξ'_λ sont appelées les <u>coordonnées</u> de la forme linéaire x' (relativement à la base (a_λ) de E) ; si $x = \sum_\lambda \xi_\lambda a_\lambda$, on a $\langle x, x' \rangle = \sum_\lambda \xi_\lambda \xi'_\lambda$. On notera que, si M est un sous-module de E ayant pour base une sous-famille $(a_\lambda)_{\lambda \in J}$ de $(a_\lambda)_{\lambda \in L}$, le sous-module orthogonal $M^\perp$ est l'ensemble des formes linéaires dont les coordonnées d'indice $\lambda \in J$ sont nulles ; il est donc isomorphe à $\prod_{\lambda \in K} M'_\lambda$, où K désigne le complémentaire de J dans L .

On peut encore définir, pour tout indice λ , la <u>forme coordonnée</u> a'_λ , qui, à tout x , fait correspondre sa composante d'indice λ relative à la base (a_λ) (c'est-à-dire la forme dont toutes les coordonnées sont nulles, à l'exception de celle d'indice λ , égale à e). Le sous-module $a'_\lambda . A$ est identifié avec le sous-module <u>composant</u> d'indice λ du produit $\prod_\lambda M'_\lambda$ (§ 1, n°3) ; mais la somme (directe) des $a'_\lambda . A$ n'est plus identique à E'. En outre, l'application canonique $x \to \tilde{x}$ de E dans son bidual E" n'applique plus E <u>sur</u> E" (cf. n° 9) .

9. <u>Dualité dans les espaces vectoriels</u>. Tout espace vectoriel à gauche E sur un corps K est isomorphe à un espace vectoriel de la forme $K_s^{(L)}$ (§ 1, th.4) ; son dual E' est donc (prop.6) isomorphe à l'espace vectoriel à droite K_d^L . En particulier :

<u>Proposition 8</u>. <u>Le dual d'un espace vectoriel à gauche</u> E <u>de dimension</u> n <u>est un espace vectoriel à droite de dimension</u> n ; <u>l'application canonique</u> $x \to \tilde{x}$ <u>de</u> E <u>dans son bidual</u> E" <u>est un isomorphisme de</u> E <u>sur</u> E" .

Si K est <u>commutatif</u>, le dual E' d'un espace vectoriel E de dimension n est donc <u>isomorphe</u> à E .

Si au contraire l'ensemble d'indices L est infini, l'application canonique $x \to \tilde{x}$ de $E = K_s^{(L)}$ dans son bidual n'applique plus E <u>sur</u> E"

En effet, si (e_λ) est la base canonique de E , (e'_λ) la famille des formes coordonnées (n°8) correspondant à cette base, le sous-espace vectoriel H de E' engendré par les e'_λ n'est plus identique à E'. Il existe donc des formes linéaires sur E' qui sont nulles sur H sans être identiquement nulles (prop.3) ; une telle forme u ne peut être identique à une forme linéaire $x' \to \langle x, x' \rangle$, avec $x \in E$, car la condition $\langle x, e'_\lambda \rangle = 0$ pour tout $\lambda \in L$ signifie que $x=0$.

Tout sous-espace vectoriel M d'un espace vectoriel E admet un supplémentaire (§1, th.5) ; donc (prop.7), le dual de M est isomorphe à $E'/M^\perp$. En particulier, d'après la prop.8 :

Théorème 1. Si M est un sous-espace vectoriel de dimension p d'un espace vectoriel E , le sous-espace orthogonal $M^\perp$ admet dans le dual E' un supplémentaire de dimension p ; si M admet dans E un supplémentaire de dimension p , $M^\perp$ est de dimension p .

Corollaire. Soit E un espace vectoriel de dimension finie n ; si M est un sous-espace de E de dimension p , le sous-espace $M^\perp$ orthogonal à M est de dimension n-p .

Proposition 9. Si M et N sont deux sous-espaces vectoriels d'un espace vectoriel E , on a $(M \cap N)^\perp = M^\perp + N^\perp$.

En effet, M est somme directe de $M \cap N$ et d'un sous-espace M_1 ; N est somme directe de $M \cap N$ et d'un sous-espace N_1 . Si P désigne un sous-espace supplémentaire de $M+N$, E est somme directe des quatre sous-espaces $M \cap N$, M_1, N_1 et P . Désignons par A', B', C', D' les sous-espaces de E' respectivement orthogonaux à M_1+N_1+P , $(M \cap N)+N_1+P$, $(M \cap N)+M_1+P$ et $(M \cap N)+M_1+N_1$; E' est somme directe de A', B', C', D' ; d'après le cor.1 de la prop.7, on a $(M \cap N)^\perp = B'+C'+D'$.

$M_1^\perp = A'+C'+D'$, $N_1^\perp = A'+B'+D'$, donc, comme $M=(M\cap N)+M_1$, $M^\perp=(M\cap N)^\perp \cap M_1^\perp = C'+D'$, et de même $N^\perp = B'+D'$, d'où la proposition.

Définition 6. On appelle sous-espace vectoriel maximal d'un espace vectoriel E un élément maximal de l'ensemble des sous-espaces vectoriels différents de E , ordonné par inclusion.

Pour qu'un sous-espace vectoriel H de E soit maximal, il faut et il suffit que l'espace quotient E/H soit simple, c'est-à-dire de dimension un , puisqu'il y a correspondance biunivoque entre les sous-espaces vectoriels de E/H , distincts de $\{0\}$ et de E/H , et les sous-espaces vectoriels de E contenant H , distincts de H et de E (§ 1, prop. 1) . On peut donc dire que les sous-espaces maximaux de E sont les supplémentaires des espaces de dimension 1 de E .

En particulier, les sous-espaces de dimensx maximaux d'un espace de dimension n sont les espaces de dimension n-1 .

Proposition 10. Pour toute forme linéaire $x'\neq 0$ sur un espace vectoriel E , $^{-1}x'(0)$ est un sous-espace maximal de E ; réciproquement, pour tout sous-espace maximal H de E , il existe une forme linéaire $x'\neq 0$ sur E telle que $H = {}^{-1}x(0)$.

Soit $x'\neq 0$ une forme linéaire sur E , et soit $x_0 \in E$ tel que $x'(x_0)=a\neq 0$; si, pour un $x\in E$, on a $x'(x)=\lambda$, on a, pour tout scalaire μ , $x'(x-\mu x_0)=\lambda-\mu a$; en prenant $\mu = \lambda a^{-1}$, on a $x'(x-\mu x_0)=0$, donc $x-\mu x_0$ appartient au sous-espace vectoriel $H = {}^{-1}x'(0)$. Comme $x_0 \notin H$, cela prouve que E est somme directe de H et du sous-espace Kx_0 de dimension 1 , donc que H est maximal.

Réciproquement, si H est maximal, $H^\perp$ est de dimension 1 dans E' d'après le th. 1 ; pour tout $x'\neq 0$ appartenant à $H^\perp$, on a donc $H \subset {}^{-1}x'(0)$; mais comme H est maximal, $H = {}^{-1}x'(0)$, ce qui achève la démonstration.

Si H est un sous-espace maximal, pour tout $x' \neq 0$ de $H^{\perp}$, on dit que $x'(x)=0$ est une <u>équation</u> de H ; si $x'_0(x)=0$ est une équation de H, toute autre équation de H est de la forme $x'_0(x)\mu = 0$.

<u>Théorème 2</u>. <u>Tout sous-espace vectoriel M d'un espace vectoriel E est l'intersection des sous-espaces minimaux qui le contiennent</u>.

Il suffit de montrer que, pour tout $x \in \complement M$, il existe un sous-espace maximal contenant M et ne contenant pas x. Soit N un sous-espace supplémentaire de M, y le composant de x dans N ; par hypothèse $y \neq 0$. Soit (a_λ) une base de N ; il existe un indice μ tel que la composante d'indice μ de y soit $\neq 0$; si P est le sous-espace ayant pour base les a_λ d'indice $\neq \mu$, M+P est un sous-espace maximal, et ne contient pas x.

<u>Corollaire</u>. <u>Pour tout sous-espace vectoriel M d'un espace vectoriel E, on a</u> $M^{\perp\perp} = M$.

Cela signifie en effet que M est l'intersection de tous les sous-espaces de la forme $x'^{-1}(0)$ contenant M, et est donc équivalent au th.2, compte tenu de la prop.10.

<u>Proposition 11</u>. <u>Soient $x'_1, x'_2, \ldots, x'_p$ p formes linéaires sur un espace vectoriel E, formant un système libre dans E'. Il existe une base dans E telle que les p formes x'_i soient des formes coordonnées relatives à cette base</u>.

La proposition étant évidente pour p=0, nous la démontrerons par récurrence sur p. Par hypothèse, il existe donc une base de E formée de p-1 vecteurs $x_1, \ldots, x_{p-1}$, et d'une famille (a_ι), telle que $\langle x_i, x'_i \rangle = 1$ pour $1 \leqslant i \leqslant p-1$, $\langle x_i, x'_j \rangle = 0$ pour $1 \leqslant i \leqslant p-1$, $1 \leqslant j \leqslant p-1$ et $i \neq j$, et enfin $\langle x, x'_i \rangle = 0$ pour $1 \leqslant i \leqslant p-1$ et pour tout x appartenant au sous-espace vectoriel M ayant pour base la famille (a_ι). Montrons qu'il existe $u \in M$ tel que $\langle u, x'_p \rangle \neq 0$; sinon on aurait $x'_p \in M^{\perp}$, et $M^{\perp}$ a pour base $x'_1, \ldots, x'_{p-1}$; donc x'_p serait combinaison linéaire des x'_i

d'indice $\leqslant p-1$, contrairement à l'hypothèse. En multipliant u par un scalaire convenable, on en conclut qu'il existe $x_p \in M$ tel que $\langle x_p, x'_p \rangle = 1$. Soit d'autre part N le sous-espace maximal $\overset{-1}{x'_p}(0)$; E est somme directe de Kx_p et de N ; posons alors $x_i = y_i + \lambda_i x_p$, avec $y_i \in N$, pour $1 \leqslant i \leqslant p-1$; on a $\langle x_i, x'_i \rangle = \langle y_i, x'_i \rangle = 1$ et $\langle x_i, x'_j \rangle = \langle y_i, x'_j \rangle = 0$ pour $1 \leqslant i \leqslant p-1$, $1 \leqslant j \leqslant p-1$ et $j \neq i$. D'autre part M est somme directe de Kx_p et de $M \cap N$; si $(b_\varkappa)$ est une base de $M \cap N$, on voit que $y_1, y_2, \cdots, y_{p-1}, x_p$ et les $b_\varkappa$ forment une base de E pour laquelle les x'_i $(1 \leqslant i \leqslant p)$ sont p formes coordonnées.

Une conséquence immédiate de la prop.11 est le théorème suivant :

Théorème 3. Soit M' un sous-espace vectoriel, de dimension finie p , du dual E' d'un espace vectoriel E . Le sous-espace $M'^{\perp}$ de E , orthogonal à M' , a un supplémentaire de dimension p , et on a $M'^{\perp\perp} = M'$.

En effet, soit $(x'_i)_{1 \leqslant i \leqslant p}$ une base de M' ; $M'^{\perp}$ est identique à l'ensemble des $x \in E$ qui sont orthogonaux à tous les x'_i ; mais si on prend une base de E pour laquelle les x'_i sont p formes coordonnées et si x_i $(1 \leqslant i \leqslant p)$ sont les p vecteurs de cette base tels que $\langle x_i, x'_i \rangle = 1$, il est clair que $M'^{\perp}$ est engendré par les éléments de cette base distincts des x_i , d'où le théorème.

La seconde partie du théorème peut encore s'exprimer de la façon suivante : si V est, dans E , l'intersection d'un nombre fini de sous-espaces vectoriels maximaux $\overset{-1}{x'_i}(0)$, toute forme linéaire qui s'annule dans V est une combinaison linéaire des x'_i .

Remarques. 1) Lorsque E a un nombre fini de dimensions, le th.3 est une simple conséquence du th.1, appliqué au dual E' , E étant identifié avec son bidual.

2) Lorsque M' est un sous-espace de E' de dimension infinie on peut avoir $M'^{\perp\perp} \neq M'$. Prenons par exemple une base infinie (a_λ) de E , et soit M' le sous-espace de E' engendré par les formes coordonnées a'_λ correspondantes ; on a vu que M' est distinct de E' , mais on a $M'^{\perp} = \{0\}$ et $\{0\}^{\perp} = E'$.

10. Equations linéaires. Soit $(F_\iota)_{\iota \in I}$ une famille de modules à gauche sur un même anneau A , et, pour chaque ι , soit u_ι une application linéaire d'un A-module E dans F_ι , et y_ι un élément de F_ι ; par définition, le système d'équations linéaires (à gauche)

$$(9) \qquad u_\iota(x) = y_\iota \qquad (\iota \in I)$$

est la relation "quel que soit $\iota \in I$, $u_\iota(x) = y_\iota$ ". La variable x est appelée l'inconnue du système d'équations ; tout $x_0 \in E$ satisfaisant à cette relation est appelé une solution du système ; les y_ι sont dits les seconds membres du système. Un système quelconque (9) d'équations linéaires est équivalent à une seule équation linéaire : en effet, soit $F = \prod_\iota F_\iota$ le produit des modules F_ι ; posons $y = (y_\iota)$, et soit u l'application linéaire (u_ι) de E dans F ; le système (9) est équivalent à l'équation linéaire $u(x) = y$.

La théorie des équations linéaires est l'étude des deux problèmes suivants : 1° déterminer s'il existe des solutions d'un système (9) ; 2° dans l'affirmative, déterminer l'ensemble des solutions de ce système.

Lorsqu'il s'agit d'une seule équation $u(x) = y$, le premier de ces problèmes revient à chercher si $y \in u(E)$, le second à déterminer $u^{-1}(y)$. Ce dernier problème se ramène immédiatement au même problème pour l'équation "sans second membre" (dite aussi équation homogène) $u(x) = 0$, une fois connue une seule solution de $u(x) = y$; en effet, si $u(x_0) = y$, l'équation $u(x) = y$ équivaut à $u(x) = u(x_0)$, c'est-à-dire à $u(x - x_0) = 0$;

en d'autres termes, l'ensemble des solutions de $u(x)=y$ n'est autre que $x_0+{}^{-1}u(0)$. On remarquera que ${}^{-1}u(0)$, qui est un sous-module de E , n'est jamais vide, puisqu'il contient 0 (qui est appelé la solution nulle, ou solution triviale, de l'équation homogène $u(x)=0$) . Pour que l'équation $u(x)=y$ ait au plus une solution, il faut et il suffit que ${}^{-1}u(0)=\{0\}$, autrement dit, que la seule solution de l'équation sans second membre soit 0 , ou encore, que u soit un isomorphisme de E dans F .

Lorsque dans un système (9), les modules F_ι sont tous identiques à A_s , on dit qu'il s'agit d'un système scalaire d'équations linéaires : un tel système est donc de la forme

$$x'_\iota(x) = \eta_\iota \qquad (\iota \in I) \tag{10}$$

où les x'_ι sont des formes linéaires sur E , les η_ι des éléments de l'anneau A .

Lorsque F est un sous-module d'un module produit A_s^I , une équation linéaire $u(x)=y$, où $y \in F$, est équivalente au système scalaire

$$\mathrm{pr}_\iota(u(x))=\mathrm{pr}_\iota(y) \qquad (\iota \in I)$$

Si E est un A-module unitaire ayant une base régulière $(a_\lambda)_{\lambda \in L}$ et si on pose $x = \sum_\lambda \xi_\lambda a_\lambda$ pour tout $x \in E$, un système scalaire (10) est équivalent au système

$$\sum_{\lambda \in L} \xi_\lambda a_{\lambda\iota} = \eta_\iota \qquad (\iota \in I) \tag{11}$$

où $a_{\lambda\iota} = x'_\iota(a_\lambda)$. Inversement, tout système d'équations de la forme (11), où on suppose que $\xi_\lambda = 0$ sauf pour un nombre fini d'indices, peut s'écrire sous la forme (10), en prenant pour E la somme directe $A_s^{(L)}$, pour (a_λ) la base canonique de ce module. Les composantes ξ_λ de x sont encore appelées les inconnues du système (11), les $a_{\lambda\iota}$ ses coefficients.

Un système (11) est aussi équivalent, comme on vient de le voir, à une seule équation $u(x)=y$, où $y=(\eta_\iota)\in A_s^I$, et où u est l'application de E dans A_s^I définie par les conditions $u(a_\lambda)=(a_{\lambda\iota})_{\iota\in I}$; cette équation peut aussi s'écrire

$$\sum_{\lambda\in L} \xi_\lambda b_\lambda = y \tag{12}$$

où $b_\lambda = u(a_\lambda)$. Réciproquement, une relation de la forme (12), où $\xi_\lambda=0$ sauf pour un nombre fini d'indices, les b_λ et y étant des éléments de A_s^I , est équivalent au système (11) qu'on obtient en projetant sur les espaces facteurs de A_s^I .

Nous nous occuperons dans ce n° des systèmes scalaires.

Proposition 12. Pour qu'il existe une solution au moins du système scalaire (10), il faut que pour toute famille (ρ_ι) d'éléments de A (nuls sauf pour un nombre fini d'indices), telle que $\sum_\iota x'_\iota \rho_\iota = 0$, on ait $\sum_\iota \eta_\iota \rho_\iota = 0$.

La proposition est évidente à partir des définitions.

La condition nécessaire ainsi obtenue n'est pas suffisante en général pour que le système (10) admette une solution. Nous allons nous limiter, dans ce qui suit, au cas où E est un espace vectoriel sur un corps K (commutatif ou non), et au cas où le sous-espace du dual E' engendré par les formes linéaires x'_ι est de dimension finie r ; on dit alors que r est le rang du système (10).

Proposition 13. Pour qu'un système scalaire (10) d'équations linéaires sur un espace vectoriel E , de rang fini r , admette une solution, il faut et il suffit que, pour toute famille (ρ_ι) de scalaires (nuls sauf pour un nombre fini d'indices), telle que $\sum_\iota x'_\iota \rho_\iota = 0$, on ait $\sum_\iota \eta_\iota \rho_\iota = 0$. Si x_0 est une solution de (10), l'ensemble des solutions de (10) est de la forme x_0+V , où V est un sous-espace de E admettant un supplémentaire de dimension r .

En effet, il existe r des formes x'_ι, soient x'_{ι_k} $(1 \leqslant k \leqslant r)$ formant une base du sous-espace U' de dimension r du dual E', engendré par les x'_{ι_ν}. Pour tout indice ι distinct des ι_k, on a donc $x'_\iota = \sum_{k=1}^{r} x'_{\iota_k} \beta_{k,\iota}$; l'hypothèse entraîne qu'on a aussi $\eta_\iota = \sum_{k=1}^{r} \eta_{\iota_k} \beta_{k,\iota}$, et par suite, l'ensemble des solutions du système (10) est identique à l'ensemble des solutions du système partiel formé des r équations $x'_{\iota_k}(x) = \eta_{\iota_k}$ $(1 \leqslant k \leqslant r)$. D'après la prop. 11, il existe une base de E formée de r vecteurs a_k $(1 \leqslant k \leqslant r)$ et d'une famille (b_μ), telle que chacune des formes x'_{ι_k} soit égale à la forme coordonnée a'_k correspondant à a_k dans cette base. Il est clair alors que l'ensemble des solutions du système (10) est identique à l'ensemble des éléments $x = \sum_{k=1}^{r} \eta_{\iota_k} a_k + \sum_\mu \zeta_\mu b_\mu$, où les ζ_μ sont arbitraires (nuls sauf un nombre fini d'entre eux) ; ce qui achève la démonstration.

Un système (10) est toujours de rang fini r s'il n'a qu'un nombre fini m d'équations ; on a alors $r \leqslant m$; de même si E est de dimension finie n (ce qui, dans un système (11), correspond au cas où il n'y a que n inconnues), on a $r \leqslant n$.

En particulier :

Corollaire 1. Un système (10) sur un espace vectoriel, formé d'un nombre fini d'équations dont les premiers membres sont des formes linéairement indépendantes, admet toujours des solutions.

Corollaire 2. Un système (11) (à coefficients et seconds membres dans un corps K), formé de n équations à n inconnues, dont les premiers membres sont des formes linéairement indépendantes, admet une solution et une seule.

Remarques. 1) On peut compléter la prop.13 dans le cas (le plus important) d'un système de m équations à n inconnues

$$x'_j(x) = \sum_{i=1}^{n} \xi_i a_{ij} = \eta_j \qquad (1 \leqslant j \leqslant m)$$

Si (a'_i) est la base duale de la base (a_i) de E, on peut, par la méthode des "substitutions successives" (§ 1, n° 10), trouver une base de E' formée de r formes linéaires x'_{j_k} $(1 \leqslant k \leqslant r)$ et de $n-r$ formes coordonnées a'_{i_h} $(1 \leqslant h \leqslant n-r)$; pour tout indice j distinct des j_k, ce procédé donne l'expression $x'_j = \sum_{k=1}^{r} x'_{j_k} \beta_{k j}$ de x'_j. La condition nécessaire et suffisante pour que le système admette des solutions est donc $\eta_j = \sum_{k=1}^{r} \eta_{j_k} \beta_{k j}$ pour tout j distinct des j_k. D'autre part, le procédé des substitutions successives donne, pour tout indice i distinct des i_h, l'expression de a'_i à l'aide de la nouvelle base de E'

$$a'_i = \sum_{k=1}^{r} x'_{j_k} \gamma_{k i} + \sum_{h=1}^{n-r} a'_{i_h} \delta_{h i}$$

donc, si $x = \sum_{i=1}^{n} \xi_i a_i$ est solution du système, on a

$$\xi_i = \sum_{k=1}^{r} \eta_{j_k} \gamma_{k i} + \sum_{h=1}^{n-r} \xi_{i_h} \delta_{h i} \tag{13}$$

pour tout indice i distinct des i_h, et on obtiendra <u>toutes</u> les solutions du système, en donnant aux ξ_{i_h} des valeurs <u>arbitraires</u> dans ces formules.

Etant donné un système d'équations <u>explicitées</u>, on a donc toujours le moyen, par une suite explicitée d'additions et de multiplications dans K, de déterminer si ce système a des solutions, et dans l'affirmative d'obtenir une représentation paramètrique <u>explicitée</u> de l'ensemble des solutions.

2) Le critère suffisant de la prop. 13 n'est plus valable pour un système scalaire (10) de rang <u>infini</u> ; si on suppose par exemple que les x'_ι sont les formes <u>coordonnées</u> dans l'espace $E = K_s^{(I)}$, le critère est vérifié quels que soient les seconds membres, puisque les x'_ι sont indépendantes ; mais le système (10) n'admet de solutions que si les η_ι sont nuls à l'exception d'un nombre fini d'entre eux.

3) Si, dans un système quelconque (11), on remplace tous les $a_{\lambda\iota}$, dont l'indice λ appartient à une partie donnée J de L, par 0, il est clair que si le nouveau système a des solutions, à toute solution $(\zeta_\lambda)_{\lambda \in \complement J}$ de ce système correspondra une solution $(\xi_\lambda)_{\lambda \in L}$ du système (11), où $\xi_\lambda = \zeta_\lambda$ pour $\lambda \in \complement J$, $\xi_\lambda = 0$ pour $\lambda \in J$. Inversement, si (ξ_λ) est une solution de (11), comme il n'y a qu'un nombre <u>fini</u> d'indices λ tels que $\xi_\lambda \neq 0$, cette solution s'obtiendra par le procédé précédent à partir d'une solution du système obtenu en annulant tous les $a_{\lambda\iota}$ correspondant aux indices λ tels que $\xi_\lambda = 0$. Toute solution de (11) est donc solution d'un système de rang <u>fini</u> ; mais ce système dépend de la solution de (11) considérée.

<u>Proposition 14</u>. <u>Si les coefficients et les seconds membres d'un système (11) appartiennent à un sous-corps K' d'un corps K, et si le système admet une solution (ζ_λ) formée d'éléments de K, il admet aussi une solution (ζ'_λ) formée d'éléments de K'</u>.

D'après une remarque antérieure, on peut se limiter au cas d'un système à un nombre fini n d'inconnues ξ_i ; le système est alors équivalent à une relation de la forme

$$\sum_{i=1}^{n} \xi_i b_i = y$$

où y et les b_i appartiennent à $F = K_s^n$; d'après l'hypothèse, y et les b_i appartiennent en outre au sous-espace vectoriel <u>par rapport à K'</u> engendré par la base canonique de F ; ils forment par hypothèse un système <u>lié</u> par rapport à K, donc ils forment aussi un système lié par rapport à K' (§ 1, prop. 12).

La proposition en résulte si les b_i forment un système libre par rapport à K' ; dans le cas contraire, on peut exprimer les b_i par des combinaisons linéaires d'un certain nombre d'entre eux b_{i_h},

(formant un système libre), à coefficients dans $K' \subset K$; portant ces valeurs dans la relation $y = \sum_{i=1}^{n} \xi_i b_i$, on en déduit que y est combinaison linéaire des b_{i_h} , à coefficients dans K ; il est donc aussi combinaison linéaire des b_{i_h} à coefficients dans K' , ce qui démontre dans ce cas la proposition.

La méthode des substitutions successives conduit aussi à ce résultat ; en effet, dans les formules (13), les coefficients γ_{ki} et δ_{hi} appartiennent alors à K' ; il suffit de donner aux ξ_{i_h} des valeurs dans K' pour avoir une solution du système formée d'éléments de K' .

Corollaire. Si les coefficients et les seconds membres d'un système (11) appartiennent à un sous-corps K' d'un corps K , et si le système admet une seule solution formée d'éléments de K , ces éléments appartiennent à K' .

11. Transposée d'une application linéaire. Soient E et F deux modules sur un même anneau A , E' et F' leurs duals, u une application linéaire de E dans F . Pour toute forme linéaire $y' \in F'$, $x' = y' \circ u$ est une forme linéaire sur E .

Définition 7. On appelle transposée d'une application linéaire u d'un module E dans un module F , et on note u^* , l'application $y' \longrightarrow y' \circ u$ du dual de F dans le dual de E .

La transposée de u est donc définie par l'identité en x et y'

$$\langle u(x), y' \rangle = \langle x, u^*(y') \rangle \tag{14}$$

La transposée u^* est une application linéaire de F' dans E', car pour tout $\lambda \in A$, $(y'\lambda) \circ u = (y' \circ u)\lambda$.

Si u et v sont deux applications linéaires de E dans F , on a

$$(u+v)^* = u^* + v^* \quad \text{et} \quad (\lambda u)^* = u^* \lambda \tag{15}$$

Soit G un troisième module sur A , u une application linéaire de E dans F , v une application linéaire de F dans G ; d'après (14) on a identiquement, en $x \in E$ et $z' \in G'$

$$\langle v(u(x)), z' \rangle = \langle u(x), v^*(z') \rangle = \langle x, u^*(v^*(z')) \rangle$$

d'où la relation

(16) $$(v \circ u)^* = u^* \circ v^* .$$

Lorsque les applications canoniques de E et F dans leurs biduals respectifs E'' et F'' sont des isomorphismes de E et F sur E'' et F'' respectivement, et qu'on peut donc identifier E et E'' , F et F'' , la relation (14) prouve que la transposée $(u^*)^*$ de u^* est identique à u et que toute application linéaire de F' dans E' est transposée d'une application linéaire de E dans F . Il en est ainsi, en particulier, lorsque E et F sont deux modules unitaires admettant des bases régulières finies (et plus particulièrement, lorsque E et F sont des espaces vectoriels de dimension finie).

Définition 8. Soit u un isomorphisme d'un module E sur un module F , v l'isomorphisme réciproque ; on appelle contragrédiente de u et on note $\check{u}$ la transposée de l'isomorphisme v .

Proposition 15. La contragrédiente $\check{u}$ d'un isomorphisme u de E sur F est un isomorphisme de E' sur F', dont l'isomorphisme réciproque est la transposée u^* de u .

En effet, la relation $x' = y' \circ u$ entraîne $y' = x' \circ v$, donc u^* est un isomorphisme de F' sur E' , et $v^* = \check{u}$ est l'isomorphisme réciproque.

On voit donc que $\check{u}$ est définie par l'identité en $x \in E$ et $x' \in E'$

(17) $$\langle u(x), \check{u}(x') \rangle = \langle x, x' \rangle .$$

Etant donnée une application linéaire quelconque u de E dans F , l'identité (14) montre que, pour tout y' tel que $u^*(y') = 0$, on a

on a $\langle u(x), y' \rangle = 0$, autrement dit, y' est orthogonal au sous-module $u(E)$ de F ; réciproquement, si y' est orthogonal à $u(E)$, on a $\langle x, u^*(y') \rangle = 0$ pour tout $x \in E$, donc $u^*(y') = 0$; on peut donc écrire

(18) $$(u(E))^{\perp} = {}^{-1}u^*(0) .$$

On en déduit les conséquences suivantes :

Proposition 16. Si l'équation $u(x) = y_0$ admet une solution (au moins), y_0 est orthogonal au sous-module ${}^{-1}u^*(0)$ de F' .

Proposition 17. Si u est une application linéaire de E sur F , sa transposée u^* est un isomorphisme de F' dans E' .

En effet, on a alors ${}^{-1}u^*(0) = F^{\perp} = \{0\}$.

Les prop. 16 et 17 n'admettent pas de réciproque en général, car dire que y_0 est orthogonal à ${}^{-1}u^*(0)$ signifie d'après (18) qu'on a $y_0 \in (u(E))^{\perp\perp}$, et en général $(u(E))^{\perp\perp}$ est distinct de $u(E)$. Toutefois, on a $(u(E))^{\perp\perp} = u(E)$ si E et F sont des espaces vectoriels, (cor. du th. 2), donc :

Proposition 18. Soit u une application linéaire d'un espace vectoriel E dans un espace vectoriel F . Pour que l'équation $u(x) = y_0$ ait au moins une solution, il faut et il suffit que y_0 soit orthogonal à ${}^{-1}u^*(0)$.

Proposition 19. Pour qu'une application linéaire u d'un espace vectoriel E dans un espace vectoriel F soit une application de E sur F , il faut et il suffit que u^* soit un isomorphisme de F' dans E' .

Supposant toujours que E et F soient des espaces vectoriels, le dual du sous-espace $u(E)$ de F est isomorphe à $F'/(u(E))^{\perp}$, c'est-à-dire à $F'/({}^{-1}u^*(0))$ d'après (18) ; mais cet espace quotient est isomorphe à $u^*(F')$; donc :

Théorème 4. Si u est une application linéaire d'un espace vectoriel E dans un espace vectoriel F, le dual du sous-espace u(E) de F est isomorphe au sous-espace $u^*(F')$ de E'. En particulier, si u est de rang fini, u et u^* ont même rang.

12. Applications semi-linéaires. Soient A et B deux anneaux isomorphes, E un module sur A. Si $\lambda \to \lambda^\sigma$ est un isomorphisme de B sur A, on définit sur E une structure de B-module en posant, pour tout $\lambda \in B$ et tout $x \in E$, $\lambda x = \lambda^\sigma x$, la loi de groupe additif sur E restant inchangée ; on vérifie immédiatement que les axiomes des modules sont vérifiés pour cette nouvelle loi externe ; en outre, si E est un A-module unitaire, le B-module ainsi défini sur E, que nous noterons E_σ, est lui aussi unitaire. Si M est un sous-module du A-module E, c'est encore un sous-module du B-module E_σ, car pour tout $\lambda \in B$ et tout $x \in M$, on a $\lambda x = \lambda^\sigma x \in M$; en outre on a $E_\sigma/M = (E/M)_\sigma$, car pour toute classe $\dot{x} \in E/M$ et tout $\lambda \in B$, $\lambda^\sigma \dot{x}$ est précisément la classe de $\lambda^\sigma x$ pour tout $x \in \dot{x}$, c'est-à-dire la classe de l'élément λx, de E_σ, ou encore la classe $\lambda \dot{x}$ dans E_σ/M.

Soit x' une forme linéaire sur E ; pour tout $\lambda \in B$, on a $x'(\lambda x) = x'(\lambda^\sigma x) = \lambda^\sigma x'(x)$; on en conclut que l'application $x \to (x'(x))^{\sigma^{-1}}$ de E_σ dans B (σ^{-1} isomorphisme de A sur B, réciproque de σ), est une forme linéaire sur E_σ, qu'on note $x'^{\sigma^{-1}}$; inversement, si y' est une forme linéaire sur E_σ, y'^σ est une forme linéaire sur E ; l'application $x' \to x'^{\sigma^{-1}}$ est donc une application biunivoque du dual E' de E sur le dual $(E_\sigma)'$ de E_σ. On peut d'ailleurs définir sur E' une structure de B-module à droite, comme ci-dessus, en posant $x'\lambda = x'\lambda^\sigma$ pour tout $\lambda \in B$ et tout $x' \in E'$; si $(E')_\sigma$ est le B-module ainsi défini, l'application $x' \to x'^{\sigma^{-1}}$ est un isomorphisme de $(E')_\sigma$ sur $(E_\sigma)'$.

Considérons maintenant un B-module F ; on dit qu'une application u de F dans E est une application semi-linéaire relative à l'isomorphisme σ , si c'est une application linéaire de F dans le B-module E_σ ; il revient au même de dire que u vérifie les identités $u(x+y)=u(x)+u(y)$ et $u(\lambda x)=\lambda^\sigma u(x)$; on peut dire également que u est une application linéaire du A-module $(F)_{\sigma^{-1}}$ dans le A-module E . En tant que fonctions linéaires particulières, on peut appliquer aux fonctions semi-linéaires toutes les propriétés des fonctions linéaires démontrées ci-dessus ; nous nous bornerons à signaler seulement quelques particularités.

En premier lieu, une application semi-linéaire biunivoque de F sur E n'est autre qu'un di-isomorphisme de F sur E (chap.I, § 4). Soient E,F,G trois modules sur des anneaux isomorphes A,B,C, σ un isomorphisme de B sur A , τ un isomorphisme de C sur B ; si u (resp. v) est une application linéaire de F dans E (resp. de G dans F) relative à l'isomorphisme σ (resp. τ), l'application composée $u\circ v$ est une application semi-linéaire de G dans E , relative à l'isomorphisme $\tau\circ\sigma$ de C sur A .

Si u est une application semi-linéaire de F dans E , relative à l'isomorphisme σ , pour toute forme linéaire y' sur E_σ, $y'\circ u$ est une forme linéaire sur F , et l'application $y' \to y'\circ u$ est une application linéaire de $(E_\sigma)'$ dans F' , transposée de l'application linéaire u ; mais en vertu de l'isomorphie de $(E_\sigma)'$ et $(E')_\sigma$, on en déduit une application linéaire $x' \to x'^{\sigma^{-1}}\circ u$ de $(E')_\sigma$ dans F' , c'est-à-dire une application semi-linéaire de E' dans F', relative à l'isomorphisme σ^{-1} ; par abus de langage, c'est cette application qu'on appelle la transposée de u et qu'on note u^* ; la relation (14) est donc remplacée par

$$\langle u(x),y'\rangle = \langle x,u^*(y')\rangle^\sigma \tag{19}$$

En pratique, les applications semi-linéaires qu'on rencontre le plus souvent sont relatives, soit au cas où $B=A$ (et où σ est donc un automorphisme de A), soit au cas où $B=A^0$.

Exemple. Si A n'est pas commutatif, on a vu que pour un $a \in A$ n'appartenant pas au centre de A , l'homothétie $x \to ax$ n'est pas en général une application linéaire de E dans lui-même ; mais si a est inversible, c'est une application semi-linéaire relative à l'automorphisme intérieur $\xi \to a\xi a^{-1}$ car on a $a(\lambda x)=(a\lambda a^{-1})(ax)$

Exercices. 1) Soit u une application linéaire d'un espace vectoriel E de dimension m dans un espace vectoriel F de dimension n ; le sous-espace $H=u^{-1}(0)$ de E est de dimension $m-\rho(u)$. Si V est un sous-espace de E , de dimension p , et si $V \cap H$ est de dimension q , montrer que u(V) est de dimension p-q . Si W est un sous-espace de F tel que $W \cap u(E)$ soit de dimension r , montrer que $u^{-1}(W)$ est un sous-espace de E , de dimension $r+m-\rho(u)$.

2) Soient E,F,G trois espaces vectoriels de dimension finie sur un corps K , u une application linéaire de E dans F , v une application linéaire de F dans G . Montrer que $u(E) \cap v^{-1}(0)$ a une dimension égale à $\rho(u)-\rho(v \circ u)$; en déduire que, si F est de dimension n , on a

$$\mathrm{Max}(0,\rho(u)+\rho(v)-n) \leqslant \rho(v \circ u) \leqslant \mathrm{Min}(\rho(u),\rho(v))$$

et que $\rho(v \circ u)$ peut prendre toute valeur entière satisfaisant à ces inégalités.

Soit H un quatrième espace vectoriel de dimension finie sur K , w une application linéaire de G dans H . Montrer que $\rho(v \circ u)+\rho(w \circ v) \leqslant \rho(v)+\rho(w \circ v \circ u)$.

3) Montrer que, si E est un A-module, $F = \prod_{i \in I} F_i$ un produit de A-modules, le module (par rapport au centre de A) $\mathscr{L}(E,F)$ des applications linéaires de E dans F est isomorphe au module produit $\prod_{i \in I} \mathscr{L}(E,F_i)$.

4) Soient E et F deux modules monogènes unitaires sur un anneau A, a et b deux éléments engendrant respectivement E et F, $\mathfrak{a}$ et $\mathfrak{b}$ les annulateurs de a et b respectivement. Si G est le sous-groupe du groupe additif de A formé des éléments $\rho \in A$ tels que $\mathfrak{a}\rho \subset \mathfrak{b}$, montrer que le groupe additif $\mathscr{L}(E,F)$ des applications linéaires de E dans F est isomorphe au groupe quotient $G/\mathfrak{b}$.

En déduire que, si $\mathfrak{k}$ est l'annulateur à droite de $\mathfrak{a}$ dans A, le dual de E est isomorphe au A-module à droite $\mathfrak{k}$.

5) Soit A un anneau non commutatif sans diviseur de 0, ayant un élément unité. Pour tout idéal à gauche $\mathfrak{a} \neq (0)$ de A, considéré comme sous-module de A_s montrer que $\mathfrak{a}^\perp = \{0\}$. En déduire que si A ne peut être plongé dans un corps (*), il existe deux sous-modules M,N de A_s, tels que $(M \cap N)^\perp \neq M^\perp + N^\perp$ (utiliser l'exerc.9 du chap.I, § 9).

6) Soit E un espace vectoriel de dimension infinie. Montrer qu'il existe une famille infinie (M_i) de sous-espaces de E telle que $(\bigcap_i M_i)^\perp \neq \sum_i M_i^\perp$ (prendre pour les M_i des sous-espaces maximaux dont l'intersection se réduit à 0).

7) Soit E un espace vectoriel de dimension infinie. Montrer que si M' et N' sont deux sous-espaces de E', de dimension <u>finie</u>, on a $(M' \cap N')^\perp = M'^\perp + N'^\perp$, et qu'il existe des sous-espaces M',N' de E', de dimension infinie, tels que $(M' \cap N')^\perp \neq M'^\perp + N'^\perp$ (prendre M' et N' tels que $M' \cap N' = \{0\}$ et $M'^\perp = \{0\}$).

8) Soit M un sous-module d'un module E ; x'_M désignant la restriction à M d'une forme linéaire x' sur E , la relation $x'_M = y'_M$ équivaut à $x'-y' \in M^\perp$; en déduire que l'application $x' \to x'_M$ est une application linéaire de E' dans le dual M' de M , et que la représentation biunivoque associée de cette application est un isomorphisme de $E'/M^\perp$ dans M' . Lorsque M n'admet pas de supplémentaire, montrer que cet isomorphisme n'applique pas nécessairement $E'/M^\perp$ sur M' , en considérant le cas où $E=A_s$, A étant un anneau sans diviseur de 0 ayant un élément unité, et $M=A.a \neq A_s$ (a non diviseur de l'unité).

9) L'image réciproque de 0 par l'application canonique $x \to \tilde{x}$ d'un module E dans son bidual E'' est identique au sous-module $E'^\perp$.

10) Soit E un module somme directe de deux sous-modules M et N . Si M' et N' désignent les duals de M et N respectivement, montrer qu'on a $E'^\perp = M'^\perp + N'^\perp$, $M'^\perp = M \cap N^{\perp\perp}$, $N'^\perp = N \cap M^{\perp\perp}$, et $M^{\perp\perp} = M + N'^\perp = M + E'^\perp$.

Donner un exemple de module E tel que $E'^\perp = \{0\}$, mais où il existe des sous-modules M tels que $M^{\perp\perp} \neq M$ (cf. exerc.5) .

11) Soit (M_ι) une famille de sous-modules d'un module E , telle que $M_\iota^{\perp\perp} = M_\iota$ pour tout ι. Montrer que $(\bigcap_\iota M_\iota)^{\perp\perp} = \bigcap_\iota M_\iota$.

12) Soit u une application linéaire d'un module E dans un module F ; pour tout sous-module M de E et tout sous-module N' de F', on a $(u(M))^\perp = u^{*-1}(M^\perp)$ et $(u^*(N'))^\perp = u^{-1}(N'^\perp)$.

13) Soient E et F deux espaces vectoriels, u une application linéaire de E dans F . Si M est un sous-espace vectoriel de E , montrer que le dual de u(M) est isomorphe à $u^*(F')/(M^\perp \cap u^*(F'))$. De même, si N' est un sous-espace de F' tel que $u^*(N')$ ait un nombre fini de dimensions, $u^*(N')$ est isomorphe au dual de l'espace $u(E)/(N'^\perp \cap u(E))$.

14) Soit u une application linéaire d'un espace vectoriel E dans un espace vectoriel F . Pour que u soit un isomorphisme de E dans F , il faut et il suffit que u^* soit une application de F' sur E' (pour voir que la condition est nécessaire, montrer que, si x' est une forme linéaire quelconque sur E et (e_λ) une base de E , il existe une forme linéaire $y' \in F'$ telle que $\langle e_\lambda , x' \rangle = \langle e_\lambda , u^*(y') \rangle$ pour tout λ .)

15) Soit E un espace vectoriel ayant une base dénombrable (e_n). Montrer qu'il existe des isomorphismes de E dans lui-même et des applications linéaires de E sur E , qui ne sont pas des automorphismes de E (définir une application linéaire u de E dans lui-même en se donnant $u(e_n)$ pour chaque n).

16) Soit $x'_\iota(x) = \eta_\iota$ $(\iota \in I)$ un système scalaire d'équations dans un espace vectoriel E (sur un corps K). Pour que le système soit de rang r , il faut et il suffit que l'application $x \longrightarrow (x'_\iota(x))$ de E dans K_s^I soit de rang r .

17) Soit M un A-module à gauche simple.

a) Si $aM = \{0\}$ pour tout $a \in A$, et si M a p éléments (p premier, cf. §1, exerc. 13), le dual de M est isomorphe à l'idéal à droite de A formé des éléments d'ordre p de l'annulateur à droite de A .

b) Si $M = Aa$ pour un $a \in M$ (cf. §1, exerc. 13), et si $\mathfrak{a}$ est l'annulateur de a , le dual de M est l'isomorphe à l'annulateur à droite $\mathfrak{b}$ de $\mathfrak{a}$. Pour que $\mathfrak{b} \neq (0)$, il faut et il suffit qu'il existe des idéaux à gauche de A isomorphes à M . Dans ce cas, on a $M'^{\perp} = \{0\}$.

18) Montrer que les th. 2, 4 et les prop. 18 et 19 s'étendent aux modules complètement réductibles tels que le dual d'aucun de leurs sous-modules simples ne se réduise à 0 .

19) Soit L un ensemble d'indices infini, K un corps quelconque. Montrer que toute base de l'espace vectoriel produit K_s^L a une puissance au moins égale à celle de $\mathfrak{P}(L)$ (soit $(a_\mu)_{\mu \in M}$ la famille des éléments distincts de K_s^L dont toutes les coordonnées sont égales à 0 ou à 1 , E le sous-espcace de K_s^L engendré par cette famille, N une partie de M telle que $(a_\mu)_{\mu \in N}$ soit une base de E (§ 1,th.4) ; pour tout indice $\mu \in \complement N$, soit $a_\mu = \sum_{\nu \in N} \lambda_{\mu\nu} a_\nu$; en projetant cette relation sur les espaces facteurs de K_s^L , montrer que les $\lambda_{\mu\nu}$ appartiennent au sous-corps K_0 de K engendré par les éléments 0 et 1 , par application du cor. de la prop. 14 ; en remarquant que K_0 est dénombrable, montrer que N et M sont équipotents ; conclure en utilisant le th.5 du § 1 et l'exerc. 15 du § 1).

Si la puissance de K est au plus égale à celle de $\mathfrak{P}(L)$, montrer que toute base de K_s^L est équipotente à $\mathfrak{P}(L)$.

Montrer qu'un espace vectoriel sur un corps commutatif ayant une base infinie n'est jamais isomorphe à son dual.

20) Soient E et F deux modules sur un anneau A , u une application linéaire de E dans F . Montrer que l'application $(x,y) \longrightarrow (x,y-u(x))$ du module produit $E \times F$ dans lui-même est un <u>automorphisme</u> de $E \times F$. En déduire que, si v est une application linéaire de F dans E , et si a est un élément de E tel que $v(u(a))=a$, il existe un automorphisme w de $E \times F$ tel que $w(a,0)=(0,u(a))$.

21) a) Soit E un espace vectoriel sur un corps K . Toute application f de E dans E permutable avec tous les <u>automorphismes</u> de E (c'est-à-dire telle que $f(u(x))=u(f(x))$ pour tout $x \in E$ et tout automorphisme u) est de la forme $x \longrightarrow ax$ (a scalaire constant).

b) Soit f une application de $E \times E$ dans E , telle que, pour tout automorphisme u de E , on ait identiquement $f(u(x),u(y))=u(f(x,y))$. Montrer que, dans l'ensemble des couples (x,y) linéairement indépendants d'éléments de E , on a $f(x,y)=\alpha x+\beta y$, où α et β sont deux scalaires constants et qu'on a $f(\lambda x, \mu x)=\varphi(\lambda,\mu)x$, φ étant une application arbitraire de $K \times K$ dans K . Si en outre on a $f(u(x),u(y))=u(f(x,y))$ pour tout endomorphisme u de E , on a $f(x,y)=\alpha x+\beta y$ quels que soient x et y . Généraliser aux applications de E^n dans E .

§ 3. Matrices sur un anneau

1. Définition des matrices. Définition 1. On appelle matrice sur un anneau A (commutatif ou non) toute famille $(a_{\lambda\mu})_{(\lambda,\mu)\in L\times M}$ d'éléments de A, dont l'ensemble d'indices est le produit de deux ensembles non vides L, M . Pour tout $\lambda \in L$, la famille $(a_{\lambda\mu})_{\mu\in M}$ est appelée la ligne d'indice λ de la matrice ; pour tout $\mu \in M$, la famille $(a_{\lambda\mu})_{\lambda\in L}$ est appelée la colonne d'indice μ de la matrice. Une matrice est dite finie si elle a un nombre fini de lignes et de colonnes (autrement dit, si les ensembles d'indices L et M sont finis).

Les dénominations de "ligne" et de "colonne" proviennent de ce que, dans le cas (de beaucoup le plus intéressant) d'une matrice finie $(a_{ij})_{1\leqslant i\leqslant m,\,1\leqslant j\leqslant n}$, on imagine les éléments de la matrice disposés dans les "cases" d'un tableau rectangulaire ayant m lignes (rangées horizontales) et n colonnes (rangées verticales) :

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

Une sous-famille $(a_{\lambda\mu})_{(\lambda,\mu)\in H\times K}$ d'une matrice $(a_{\lambda\mu})_{(\lambda,\mu)\in L\times M}$ dont l'ensemble d'indices est le produit d'une partie H de L et d'une partie K de M, est dite <u>sous-matrice</u> de la matrice considérée ; on dit qu'elle s'obtient en <u>supprimant</u> les lignes d'indice $\lambda\in\complement H$ et les colonnes d'indice $\mu\in\complement K$; inversement, on dit que la matrice $(a_{\lambda\mu})_{(\lambda,\mu)\in L\times M}$ s'obtient en <u>bordant</u> la sous-matrice $(a_{\lambda\mu})_{(\lambda,\mu)\in H\times K}$ par les lignes d'indice $\lambda\in\complement H$ et les colonnes d'indice $\mu\in\complement K$.

On désigne d'ordinaire les matrices par des majuscules italiques. L'ensemble des matrices sur un anneau A, correspondant à des ensembles d'indices L,M donnés, n'est autre que le produit $A^{L\times M}$; on peut donc le munir de la structure de <u>groupe additif</u> produit des structures de groupe additif des facteurs A ; la <u>somme</u> de deux matrices $\underline{X}=(\xi_{\lambda\mu})_{(\lambda,\mu)\in L\times M}$ et $\underline{Y}=(\eta_{\lambda\mu})_{(\lambda,\mu)\in L\times M}$ est donc la matrice $\underline{X}+\underline{Y}=(\xi_{\lambda\mu}+\eta_{\lambda\mu})_{(\lambda,\mu)\in L\times M}$.

La somme de deux matrices $\underline{X}$, $\underline{Y}$ n'est donc définie que si les ensembles d'indices des lignes et des colonnes sont les <u>mêmes</u> pour ces deux matrices.

On peut de même munir $A^{L\times M}$ de la structure de A-<u>module à gauche</u> (resp. de la structure de A-<u>module à droite</u>) produit des structures correspondantes des facteurs ; le produit $\rho\underline{X}$ (resp. $\underline{X}\rho$) d'un opérateur $\rho\in A$ et d'une matrice $\underline{X}=(\xi_{\lambda\mu})$ est la matrice $(\rho\,\xi_{\lambda\mu})$ (resp. $(\xi_{\lambda\mu}\rho)$). Ces deux structures définissent d'ailleurs sur $A^{L\times M}$ une structure de <u>bimodule</u> (§1,n°12) par rapport à A.

Considérons en particulier le cas où A possède un élément unité ϵ, et où $L=[1,m]$ et $M=[1,n]$ sont finis ; soit $\underline{E}_{ij}$ la matrice (a_{hk})

telle que $a_{hk}=0$ pour $(h,k)\neq(i,j)$, et $a_{ij}=\varepsilon$; lorsqu'on munit l'ensemble $A^{L\times M}$ des matrices à m lignes et n colonnes sur A de l'une des structures de module précédentes, les mn matrices E_{ij} forment une <u>base régulière</u> de ces deux modules, qu'on appelle leur <u>base canonique</u>.

<u>2. Matrices et applications linéaires</u>. Soient A un anneau ayant un élément unité, L et M deux ensembles d'indices quelconques ; considérons les deux A-modules <u>à droite</u> $E=A_d^{(L)}$, $F=A_d^{(M)}$; soient $(e_\lambda)_{\lambda\in L}$, $(f_\mu)_{\mu\in M}$ les <u>bases canoniques</u> (§ 1, n°9) de ces deux modules. On sait (§ 2, prop. 3) qu'une application linéaire u de E dans F est déterminée par la donnée des éléments $y_\lambda = u(e_\lambda)$ de F, et qu'inversement, toute famille $(y_\lambda)_{\lambda\in L}$ d'éléments de F détermine une application linéaire u de E dans F par les conditions $u(e_\lambda)=y_\lambda$. On a $u(e_\lambda) = \sum_{\mu\in M} f_\mu a_{\mu\lambda}$ avec, pour tout $\lambda\in L$, $a_{\mu\lambda}=0$ sauf pour un nombre fini d'indices μ (ces indices dépendant de λ) ; les $a_{\mu\lambda}$ sont bien déterminés par la donnée de u, et inversement déterminent les $u(e_\lambda)$, donc u. Désignons par $\underline{M}(u)$ la matrice $(a_{\mu\lambda})_{(\mu,\lambda)\in M\times L}$ qu'on fait ainsi correspondre à u : la <u>colonne</u> d'indice λ de cette matrice est donc formée des composantes $a_{\mu\lambda}$ de $u(e_\lambda)$ relativement à la base canonique de F, et n'a qu'un nombre fini d'éléments non nuls. Nous dirons qu'une matrice n'ayant qu'un nombre fini d'éléments $\neq 0$ dans chaque colonne est une matrice <u>semi-finie</u> ; on voit donc que l'application $u \to \underline{M}(u)$ est un <u>isomorphisme</u> de la structure de groupe additif de l'ensemble $\mathscr{L}(E,F)$ des applications linéaires de E dans F, sur celle de l'ensemble des matrices semi-finies, ayant M comme ensemble d'indices des lignes, L comme ensemble d'indices des colonnes (ensemble qui est évidemment un sous-groupe du groupe additif $A^{M\times L}$ de toutes les matrices sur A ayant ces ensembles d'indices).

Cette application est même un isomorphisme de la structure de A-module à gauche de $\mathscr{L}(E,F)$ (structure dont l'existence provient de ce que $A_d^{(M)}$ est muni d'une structure de bimodule ; cf. § 2, n°6) sur la structure de A-module à gauche de l'ensemble des matrices semi-finies.

Il résulte de la définition de l'isomorphisme précédent que, lorsqu'on se donne la matrice $\underline{M}(u)=(a_{\mu\lambda})$ correspondant à une application linéaire u de E dans F, les composantes η_μ de u(x) dans F, pour tout $x=\sum_{\lambda\in L} e_\lambda \xi_\lambda$, sont données par les formules

$$\eta_\mu = \sum_{\lambda\in L} a_{\mu\lambda}\,\xi_\lambda \quad . \tag{1}$$

Remarques. 1) Lorsque l'anneau A n'a pas d'élément unité, les formules (1) font encore correspondre à tout élément (ξ_λ) de la somme directe $A_d^{(L)}$ (considérée comme sous-module du module produit A_d^L) un élément (η_μ) de $A_d^{(M)}$, et il est immédiat que cette application est linéaire ; mais plusieurs matrices distinctes peuvent alors définir de cette manière la même application linéaire, et d'autre part, il peut exister des applications linéaires de $A_d^{(L)}$ dans $A_d^{(M)}$ qui ne peuvent s'obtenir de cette façon.

2) Soit A un anneau ayant un élément unité, et considérons les applications linéaires du module somme directe $E=A_d^{(L)}$ dans le module produit $G=A_d^M$; une telle application u est déterminée par les éléments $u(e_\lambda)=y_\lambda$ de G ; si on pose $y_\lambda=(a_{\mu\lambda})_{\mu\in M}$, on fait correspondre à u la matrice $\underline{M}(u)=(a_{\mu\lambda})$ qui cette fois est une matrice quelconque de $A^{M\times L}$; on définit ainsi un isomorphisme de la structure de A-module à gauche de $\mathscr{L}(E,G)$ sur celle de $A^{M\times L}$; lorsqu'on se donne la matrice $\underline{M}(u)=(a_{\mu\lambda})$ correspondant à une application linéaire u de E dans G, les coordonnées η_μ de u(x) sont encore données en fonction des composantes ξ_λ de x par les formules (1).

3. Produit de deux matrices. Soient L,M,N trois ensembles d'indices, A un anneau ayant un élément unité, u une application linéaire du module à droite $E=A_d^{(L)}$ dans $F=A_d^{(M)}$, v une application linéaire de F dans $G=A_d^{(N)}$. Si $\underline{M}(u)=(\alpha_{\mu\lambda})_{(\mu,\lambda)\in M\times L}$, $\underline{M}(v)=(\beta_{\nu\mu})_{(\nu,\mu)\in N\times M}$ sont les matrices semi-finies correspondant respectivement à u et v, cherchons les éléments de la matrice $\underline{M}(w)=(\gamma_{\nu\lambda})_{(\nu,\lambda)\in N\times L}$ qui correspond à l'application composée $w=v\circ u$. Avec les notations du n°2, et en désignant par $(g_\nu)_{\nu\in N}$ la base canonique de G, on a

$$w(e_\lambda)=v(u(e_\lambda))=v\Big(\sum_{\mu\in M} f_\mu \alpha_{\mu\lambda}\Big)=\sum_{\mu\in M} v(f_\mu)\alpha_{\mu\lambda}=\sum_{\mu\in M}\Big(\Big(\sum_{\nu\in N} g_\nu \beta_{\nu\mu}\Big)\alpha_{\mu\lambda}\Big)=$$
$$=\sum_{\nu\in N} g_\nu \Big(\sum_{\mu\in M}\beta_{\nu\mu}\alpha_{\mu\lambda}\Big)$$

d'où la formule

$$\gamma_{\nu\lambda}=\sum_{\mu\in M}\beta_{\nu\mu}\alpha_{\mu\lambda} \qquad (2)$$

(qui a un sens puisque les matrices $\underline{M}(u)$ et $\underline{M}(v)$ sont semi-finies).

On dit que la matrice $\underline{M}(w)$ dont les éléments sont définis par (2) est le produit de la matrice $\underline{M}(v)$ et de la matrice $\underline{M}(u)$, et on la note $\underline{M}(v)\underline{M}(u)$; définition qui permet d'écrire la formule

$$\underline{M}(v\circ u)=\underline{M}(v)\underline{M}(u) \qquad (3)$$

Remarques. 1) Le produit d'une matrice $\underline{Y}=(\eta_{\nu\mu})_{(\nu,\mu)\in N\times M}$ et d'une matrice $\underline{X}=(\xi_{\mu\lambda})_{(\mu,\lambda)\in M\times L}$ n'est donc défini que si l'ensemble des indices des colonnes de Y est identique à l'ensemble des indices des lignes de X ; en particulier, si $L\neq N$, le produit XY n'a aucun sens. Dans la formule (2) figurent les éléments d'une même ligne de $\underline{M}(v)$ multipliés à droite par les éléments d'une même colonne de $\underline{M}(u)$: on dit que la multiplication de deux matrices se fait "lignes par colonnes".

2) Lorsque A est un anneau sans élément unité, on peut encore définir le produit de deux matrices semi-finies sur A par la formule (2) qui garde un sens ; on vérifie aussitôt que

que l'application linéaire de $A_d^{(L)}$ dans $A_d^{(N)}$ qui correspond à cette matrice produit est encore la composée des applications correspondant aux matrices facteurs.

3) Si on prend pour module G , non la somme directe, mais le produit A_d^N , les formules (2) gardent un sens et donnent encore les éléments de la matrice $\underline{M}(v \circ u)$; on dit encore que cette matrice est le <u>produit</u> de la matrice quelconque $\underline{M}(v)$ et de la matrice semi-finie $\underline{M}(u)$. On notera par contre que les formules (2) n'ont plus de sens si les matrices $(a_{\mu\lambda})$ et $(\beta_{\lambda\mu})$ sont toutes deux quelconques, la somme du second membre comportant alors une infinité de termes non nuls en général.

Toute propriété relative à la somme ou au composé d'applications linéaires se <u>traduit</u> en propriétés relatives à la somme ou au produit de matrices semi-finies, grâce à la formule (3) et aux formules $\underline{M}(u+v)=\underline{M}(u)+\underline{M}(v)$, $\underline{M}(au)=a\underline{M}(u)$. En particulier, on a les règles de <u>distributivité</u> et d'<u>associativité</u>

$$\underline{X}(\underline{Y}+\underline{Z}) = \underline{XY}+\underline{XZ}$$

$$(\underline{X}+\underline{Z})\underline{X} = \underline{YZ}+\underline{ZX}$$

$$\underline{X}(\underline{YZ}) = (\underline{XY})\underline{Z}$$

$$a(\underline{XY}) = (a\underline{X})\underline{Y}$$

valables chaque fois que les opérations qui y figurent ont un sens.

En traduisant de la même manière la formule (2) du § 2, n°4, qui donne la composée de deux applications linéaires de modules décomposés en sommes directes, on obtient une intéressante formule pour le calcul du produit de deux matrices.

Soit en effet $\underline{X}$ une matrice semi-finie correspondant à une application linéaire u de $A_d^{(L)}$ dans $A_d^{(M)}$. Soit (L_i) une <u>partition</u>

de L en p ensembles, (M_j) une partition de M en q ensembles, et soit E_i (resp. F_j) la somme (directe) des modules composants de $A_d^{(L)}$ (resp. $A_d^{(M)}$) dont l'indice appartient à L_i (resp. M_j). Aux décompositions de $A_d^{(L)}$ et $A_d^{(M)}$ en somme directe des E_i et des F_j respectivement, il correspond (§ 2, n°4) une famille (u_{ji}) d'applications linéaires, où u_{ji} est une application linéaire de E_i dans F_j, définie par la condition que, pour tout $x \in E_i$, $u_{ji}(x)$ est le composant dans F_j de $u(x)$. Il résulte de cette définition que la matrice $\underline{M}(u_{ji})$ n'est autre que la sous-matrice $\underline{X}_{ji}$ de $\underline{X}$ obtenue par suppression des lignes d'indice $\mu \in \complement M_j$, et des colonnes d'indice $\lambda \in \complement L_i$; la matrice $\underline{X}$ peut donc s'imaginer comme un "tableau de matrices" à q "lignes et p "colonnes" :

$$\begin{pmatrix} \underline{X}_{11} & \underline{X}_{12} & \cdots & \underline{X}_{1p} \\ \underline{X}_{21} & \underline{X}_{22} & \cdots & \underline{X}_{2p} \\ \cdots & \cdots & \cdots & \cdots \\ \underline{X}_{q1} & \underline{X}_{q2} & \cdots & \underline{X}_{qp} \end{pmatrix}$$

Considérons maintenant une application linéaire v de $A_d^{(M)}$ dans $A_d^{(N)}$, et soit $\underline{Y}$ la matrice $\underline{M}(v)$. Si on considère la même partition (M_j) de M, et une partition (N_k) de N en r ensembles, la matrice $\underline{Y}$ est de même mise sous forme d'un tableau à r lignes et q colonnes, formé des sous-matrices $\underline{Y}_{kj} = \underline{M}(v_{kj})$, où (v_{kj}) est la famille d'applications linéaires qui correspond à v et aux partitions (M_j) et (N_k). Si maintenant on traite de même l'application composée $w = v \circ u$ pour les partitions (L_i) et (N_k), la matrice produit $\underline{Z} = \underline{Y}\underline{X}$ qui lui correspond apparait comme un tableau de r lignes et p colonnes de sous-matrices $\underline{Z}_{ki}$, correspondant à la famille (w_{ki}) d'applications linéaires déterminée par w. Mais, d'après la

la formule (2) du § 2,n°4, on a $w_{ki}=\sum_{j=1}^{q} v_{kj}\circ u_{ji}$; donc

(4) $$\underline{Z}_{ki} = \sum_{j=1}^{q} \underline{Y}_{kj}\underline{X}_{ji}$$

En d'autres termes, <u>le tableau des Z_{ki} s'obtient en formant le "produit" du tableau des Y_{kj} par celui des X_{ji} comme si ces tableaux étaient des matrices dont les Y_{kj} et X_{ji} seraient respectivement les éléments</u> ; c'est ce qu'on appelle effectuer le produit $\underline{YX}$ "<u>par blocs</u>" .

La formule (1) qui donne les composantes de $u(x)$, peut s'interpréter à l'aide de la notion de produit de matrices, de la manière suivante : tout élément $x=\sum_{\lambda\in L} e_\lambda \xi_\lambda$ de $E=A_d^{(L)}$ détermine une application linéaire $\xi \longrightarrow x\xi$ (que nous avons désignée par θ_x au § 2,n°1) de A_d dans $A_d^{(L)}$; à cette application correspond la <u>matrice à une colonne</u> $\underline{M}(\theta_x)=(\xi_\lambda)_{\lambda\in L}$. De même $u(x)=\sum_{\mu\in M} f_\mu \eta_\mu$ détermine l'application linéaire $\theta_{u(x)}$ de A_d dans $A_d^{(M)}$, à laquelle correspond la matrice à une colonne $\underline{M}(\theta_{u(x)})=(\eta_\mu)_{\mu\in M}$; or, on a $u(x\xi)=u(x)\xi$, autrement dit $\theta_{u(x)}=u\circ\theta_x$; en traduisant cette relation en matrices, on obtient les relations (1). Le plus souvent, lorsqu'aucune confusion n'en peut résulter, on identifie l'élément $x\in E$ à la matrice à une colonne $\underline{M}(\theta_x)$ (formée des <u>composantes</u> de x) qui lui correspond ; avec cette convention, les formules (1) peuvent donc s'écrire

(5) $$u(x)=\underline{M}(u).x \quad .$$

4. <u>Matrices carrées</u>. <u>Définition 2</u>. <u>On appelle matrice carrée une matrice dont les lignes et les colonnes ont même ensemble d'indices</u>.

On dit qu'une matrice carrée <u>finie</u> ayant n lignes et n colonnes est une matrice d'<u>ordre</u> n .

Soit L un ensemble d'indices quelconque, A un anneau ayant un élément unité ε ; pour tout <u>endomorphisme</u> u du module $\widetilde{E=}A_d^{(L)}$, la matrice correspondante $\underline{M}(u)$ est une matrice carrée semi-finie ayant L comme ensemble des indices des lignes et des colonnes ; en outre, ces matrices forment un <u>anneau</u> et l'application $u \to \underline{M}(u)$ est un <u>isomorphisme</u> de l'anneau $\mathcal{L}(E)$ des endomorphismes de E , sur l'anneau de ces matrices. L'élément unité de ce dernier est la matrice $\underline{I}=(\delta_{\lambda\mu})$, où $\delta_{\lambda\mu}=0$ pour $\lambda \neq \mu$, et $\delta_{\lambda\lambda}=\varepsilon$ pour tout $\lambda \in L$; lorsqu'il s'agit de l'anneau des matrices carrées <u>finies</u> d'ordre n , cet élément unité (dit aussi <u>matrice unité</u> d'ordre n) se note parfois $\underline{I}_n$, lorsqu'on veut éviter toute confusion.

D'une façon générale, dans une matrice carrée $\underline{X}=(\xi_{\lambda\mu})$, les éléments $\xi_{\lambda\lambda}$ dont les deux indices sont égaux, sont appelés <u>éléments diagonaux</u>, et la famille $(\xi_{\lambda\lambda})_{\lambda \in L}$ est appelée la <u>diagonale</u> de $\underline{X}$.

Une matrice dont les éléments non diagonaux sont nuls est dite matrice <u>diagonale</u> ; la matrice unité $\underline{I}$ est évidemment une matrice diagonale, ainsi que tout multiple $\rho\underline{I}=\underline{I}\rho$ de cette matrice par un scalaire ρ (matrice dont tous les éléments diagonaux sont égaux à ρ) ; on notera que, pour toute matrice carrée $\underline{X}$, on a $(\rho\underline{I})\underline{X} = \rho\underline{X}$ et $\underline{X}(\rho\underline{I}) = \underline{X}\rho$.

Il est immédiat que, si $\underline{X}$ et $\underline{Y}$ sont deux matrices diagonales, dont (ξ_λ) et (η_λ) sont les diagonales respectives, le produit $\underline{XY}$ est la matrice diagonale, ayant pour diagonale $(\xi_\lambda \eta_\lambda)$; les matrices diagonales forment donc un <u>sous-anneau</u>, isomorphe à l'anneau produit A^L , de l'anneau des matrices carrées semi-finies sur A , ayant pour ensemble d'indices des lignes et des colonnes l'ensemble L ; les matrices $\rho\underline{I}$ forment un sous-anneau, isomorphe à A , de l'anneau des matrices diagonales.

Plus généralement, considérons une partition (L_i) de l'ensemble L en p ensembles, et mettons toute matrice carrée semi-finie $(\xi_{\lambda\mu})(\lambda,\mu)\in L\times L$ sous forme d'un "tableau carré de matrices" correspondant à la même partition (L_i) de l'ensemble L pour les lignes et les colonnes

$$\begin{pmatrix} \underline{X}_{11} & \underline{X}_{12} & \cdots & \underline{X}_{1p} \\ \underline{X}_{21} & \underline{X}_{22} & \cdots & \underline{X}_{2p} \\ \cdots & \cdots & \cdots & \cdots \\ \underline{X}_{p1} & \underline{X}_{p2} & \cdots & \underline{X}_{pp} \end{pmatrix}$$

Chacune des matrices $\underline{X}_{ii}$ est une matrice carrée dont les lignes et les colonnes ont pour ensemble d'indices L_i .

Cela étant, celles des matrices carrées semi-finies pour lesquelles le tableau précédent est un tableau <u>diagonal</u>, c'est-à-dire tel que $\underline{X}_{ij}=0$ pour $i\neq j$, forment un <u>anneau</u>, comme le montre le produit "par blocs" de deux matrices mises sous la forme précédente ($n^o 3$). Si V_i désigne la somme (directe) des modules composants de $A_d^{(L)}$, dont l'indice appartient à L_i , ces matrices correspondent aux endomorphismes u de $A_d^{(L)}$, tels que $u(V_i)\subset V_i$ pour $1\leqslant i\leqslant p$.

2. <u>Transposée d'une matrice finie</u>. Jusqu'à la fin de ce paragraphe, nous ne considérerons plus, en principe, que des matrices <u>finies</u> sur un anneau A ayant un élément unité ϵ ; les matrices à m lignes et n colonnes sur A correspondent donc biunivoquement aux applications linéaires de A_d^n dans A_d^m .

En particulier, les <u>formes linéaires</u> sur $E=A_d^n$ correspondent biunivoquement aux matrices à <u>une ligne</u> et n colonnes. De façon précise, si $(e_i)_{1\leqslant i\leqslant n}$ est la base canonique de E , à la forme linéaire x' correspond la matrice à une ligne $\underline{M}(x')=(\xi'_i)$, où $\xi'_i=x'(e_i)=\langle e_i,x'\rangle$

On sait que le dual E' de E peut être identifié au module à gauche A_s^n, la base canonique (e'_i) de ce module étant <u>base duale</u> de (e_i) (§ 2, n°8) ; la matrice à une ligne $\underline{M}(x')$ est alors formée des <u>composantes</u> de la forme x' ; on sait que, si $x = \sum_{i=1}^{n} e_i \xi_i$, on a $\langle x,x' \rangle = \sum_{i=1}^{n} \xi'_i \xi_i$; en identifiant comme d'ordinaire x à la matrice à une colonne (ξ_i), cette relation s'écrit encore (cf. formule (5))

(6) $$\langle x,x' \rangle = \underline{M}(x').x \quad .$$

Remarquons maintenant que tout A-module à gauche peut être considéré comme un module <u>à droite</u> sur l'anneau A^o, <u>opposé</u> de A . En particulier, si $E=A_d^n$, $F=A_d^m$, nous considèrerons les <u>duals</u> respectifs $E'=A_s^n$, $F'=A_s^m$ de ces modules, comme les A^o-modules à droite $(A_d^o)^n$ et $(A_d^o)^m$ respectivement. Si u est une application linéaire de E dans F, sa <u>transposée</u> u^* est une application linéaire du A^o-module à droite F' dans le A^o-module à droite E'. Cherchons la relation entre la matrice $\underline{M}(u)$ (à éléments dans A) et la matrice $\underline{M}(u^*)$ (à éléments <u>dans</u> A^o). Si $(e_i),(f_j)$ sont les bases canoniques de E et F, (e'_i) et (f'_j) celles de E' et F' respectivement, l'élément β_{ij} de $\underline{M}(u^*)$ appartenant à la ligne d'indice i et la colonne d'indice j est égal à la composante sur e'_i de $u^*(f'_j)$, c'est-à-dire à $\langle e_i, u^*(f'_j) \rangle = \langle u(e_i), f'_j \rangle$; mais $\langle u(e_i), f'_j \rangle$ n'est autre que la composante de $u(e_i)$ sur f_j, donc l'élément a_{ji} appartenant à la ligne d'indice j et la colonne d'indice i de $\underline{M}(u)$. D'une façon générale, si $\underline{X}=(\xi_{ji})$ est une matrice à m lignes et n colonnes sur l'anneau A, nous désignerons par $\underline{X}^*$ et nous appellerons <u>transposée</u> de la matrice $\underline{X}$ la matrice (ξ'_{ij}), à n lignes et m colonnes, <u>sur l'anneau</u> A^o, telle que $\xi'_{ij} = \xi_{ji}$ pour $1 \leqslant i \leqslant n$, $1 \leqslant j \leqslant m$; on dit aussi que $\underline{X}^*$ se déduit de $\underline{X}$ en <u>échangeant les lignes et les colonnes</u> de cette matrice. Avec cette notation, on a donc

(7) $$\underline{M}(u^*) = (\underline{M}(u))^* \quad .$$

Il est immédiat que $(\underline{X}^*)^*=\underline{X}$; en outre, si $\underline{Y}$ est une matrice à n lignes et p colonnes sur A , il résulte de la formule (16) du § 2, donnant la transposée de la composée de deux applications linéaires, qu'on a

$$(8) \qquad (\underline{XY})^* = \underline{Y}^* . \underline{X}^*$$

en tenant compte que les produits qui figurent dans les éléments de la matrice du second membre doivent être pris dans l'anneau A^o.

En particulier, la transposée de la forme linéaire x' est l'application linéaire de A_d^o dans $E'=(A_d^o)^n$, que nous avons désignée ci-dessus par $\theta_{x'}$; on retrouve ainsi le fait que la transposée de la matrice $\underline{M}(x')$ est la matrice à une colonne dont les éléments sont les composantes, ξ_i' de x' sur la base (e_i') (ces composantes étant considérées comme des éléments de A^o) ; comme, suivant la convention générale, cette matrice à une colonne est identifiée à x' , on voit que la relation (6) peut encore s'écrire

$$(9) \qquad \langle x,x' \rangle = x'^* . x \quad .$$

D'après la formule(5), pour toute forme linéaire $y' \in F'$, on a $u^*(y')=\underline{M}(u^*).y'$; d'après (7),(8) et (9), on a donc

$$\langle x,u^*(y') \rangle = y'^* . \underline{M}(u).x$$

et la formule fondamentale (14) du § 2 prend l'aspect de la règle d'associativité du produit de matrices

$$y'^* . (\underline{M}(u).x) = (y'^* . \underline{M}(u)).x \quad .$$

Dans le cas particulier où m=n , et où la matrice carrée $\underline{X}$ est inversible, c'est-à-dire correspond à un automorphisme u de $E=A_d^n$, l'application contragrédiente $\check{u}$ (§ 2,n°11) est un automorphisme de $E'=(A_d^o)^n$, réciproque de la transposée u^* de u , et identique à la transposée de l'automorphisme réciproque de u ; il correspond donc à u la matrice $(\underline{X}^{-1})^* =(\underline{X}^*)^{-1}$; on la note $\check{\underline{X}}$ et on l'appelle la contragrédien

te

de la matrice $\underline{X}$; d'après (8), pour deux matrices carrées inversibles et de même ordre $\underline{X}$, $\underline{Y}$ sur l'anneau A , on a

(10) $\overset{\vee}{\underline{XY}} = \overset{\vee}{\underline{X}}.\overset{\vee}{\underline{Y}}$

(le produit étant relatif à l'anneau A^0).

6. Matrices finies sur un corps. Une matrice $\underline{X}$ à m lignes et n colonnes sur un corps K correspond à une application linéaire u de K_d^n dans K_d^m ; le rang $\rho(u)$ de cette application est par définition le rang de la matrice $\underline{X}$; comme c'est le nombre de dimensions de $u(K_d^n)$, il revient au même (en identifiant les colonnes de $\underline{X}$ aux images par u de la base canonique de K_d^n) de donner la définition suivante :

Définition 3. On appelle rang d'une matrice $\underline{X}$ à m lignes et n colonnes sur un corps K , et on note $\rho(\underline{X})$, le nombre de dimensions du sous-espace de K_d^m engendré par les n colonnes de $\underline{X}$.

On peut dire aussi que le rang de $\underline{X}$ est le nombre maximum des colonnes de $\underline{X}$ linéairement indépendantes. On a évidemment, d'après la définition 3 , $\rho(\underline{X}) \leqslant \mathrm{Min}(m,n)$. Pour toute sous-matrice $\underline{Y}$ de $\underline{X}$, on a $\rho(\underline{Y}) \leqslant \rho(\underline{X})$.

Le th.4 du §2, et la définition de la transposée d'une matrice, montrent que :

Proposition 1. Le rang d'une matrice finie $\underline{X}$ sur un corps, est égal au rang de sa transposée $\underline{X}^*$.

Les matrices carrées d'ordre n sur K correspondent aux endomorphismes de K_d^n ; elles forment un anneau isomorphe à l'anneau $\mathcal{L}(K_d^n)$ des endomorphismes de K_d^n . Aux automorphismes de K_d^n correspondent les matrices carrées inversibles ; par suite (§ 2, cor.de la prop.1) :

Proposition 2. Pour qu'une matrice carrée d'ordre n sur un corps soit inversible, il faut et il suffit que son rang soit égal à n .

7. Application aux équations linéaires. Soit A un anneau ayant un élément unité ; considérons un système de m équations linéaires (à droite) à n inconnues, à coefficients dans A

$$(11) \qquad \sum_{j=1}^{n} a_{ij}\,\xi_j = \beta_i \qquad (1 \leqslant i \leqslant m)$$

Si (e_i) désigne la base canonique de A_d^m, (f_j) celle de A_d^n, si on pose $x = \sum_{j=1}^{n} f_j\,\xi_j$, $y = \sum_{i=1}^{m} e_i\beta_i$, et si u désigne l'application linéaire de A_d^n dans A_d^m, définie par $u(f_j) = \sum_{i=1}^{m} e_i a_{ij}$, on a vu (§2, n°10) que le système (11) est équivalent à l'équation $u(x)=y$, ou encore à

$$(12) \qquad \sum_{j=1}^{n} u(f_j)\,\xi_j = y$$

La matrice $\underline{A}=\mathbb{M}(u)=(a_{ij})$, à m lignes et n colonnes, qui correspond à u, est dite la matrice du système (11) ; dire que le système (11) a une solution revient, d'après (12), à dire que la matrice à une colonne $y=(\beta_i)$ est une combinaison linéaire des n colonnes de la matrice $\underline{A}$.

Considérons en particulier le cas d'un système (11) sur un corps K. Alors, l'interprétation précédente, et la définition du rang d'une matrice, prouvent que :

Proposition 3. Pour qu'un système (11) d'équations linéaires sur un corps K ait une solution, il faut et il suffit que la matrice B obtenue en bordant la matrice $\underline{A}=(a_{ij})$ du système par une $(n+1)^{\text{ème}}$ colonne (β_i) formée des seconds membres de (11), ait même rang que la matrice $\underline{A}$.

Cette condition est toujours remplie lorsque m=n, et que $\underline{A}$ est une matrice inversible, c'est-à-dire de rang n. En outre, si on identifie comme d'ordinaire x et y aux matrices à une colonne (ξ_j) et (β_i) respectivement, et qu'on écrit l'équation $u(x)=y$ sous la forme $\underline{A}.x=y$ (formule (5)), on voit que l'unique solution du système (11) est donnée

par la formule

(13) $$x = \underline{A}^{-1}.y$$

8. Changements de bases. Soit A un anneau ayant un élément unité. Au n°2, nous avons défini une correspondance biunivoque entre applications linéaires de A_d^n dans A_d^m, et matrices à m lignes et n colonnes sur A. Plus généralement, soient E et F deux A-modules à droite unitaires admettant respectivement des bases régulières finies (§ 1, n°8), $(a_i)_{1 \leqslant i \leqslant n}$ et $(b_j)_{1 \leqslant j \leqslant m}$; à toute application linéaire u de E dans F correspond biunivoquement la famille des éléments $u(a_i) = \sum_{j=1}^{m} b_j a_{ji}$ et par suite aussi la matrice (a_{ji}) à m lignes et n colonnes. Nous dirons que cette matrice correspond à l'application u, rapportée aux bases (a_i) et (b_j) (prises dans cet ordre), et, lorsqu'il y aura lieu d'éviter toute ambiguité, nous la désignerons par $\underline{M}(u;(a_i),(b_j))$.

Soit G un troisième A-module à droite unitaire, ayant une base régulière $(c_k)_{1 \leqslant k \leqslant p}$; si v est une application linéaire de F dans G, le même raisonnement qu'au n°3 prouve que

(14) $$\underline{M}(v \circ u;(a_i),(c_k)) = \underline{M}(v;(b_j),(c_k))\underline{M}(u;(a_i),(b_j))$$

En particulier, si on identifie tout élément $x = \sum_{i=1}^{n} a_i \xi_i$ de E avec la matrice à une colonne (ξ_i) de ses composantes sur la base (a_i), et de même tout élément $y = \sum_{j=1}^{m} b_j \eta_j$ de F avec la matrice à une colonne (η_j), on a la formule analogue à (5)

(15) $$u(x) = \underline{U}.x$$

$\underline{U}$ étant la matrice correspondant à u, rapportée aux bases (a_i) et (b_j).

Soient E' et F' les modules duals de E et F respectivement, considérés comme des modules à droite sur l'anneau A^0 opposé de A. Soient (a_i') et (b_j') les bases duales de (a_i) et (b_j) respectivement ; le même raisonnement qu'au n°5 montre que la matrice $\underline{M}(u^*;(b_j'),(a_i'))$

de la transposée u^* de u , rapportée aux bases (b'_j) et (a'_i), est identique à la transposée de la matrice $\underline{M}(u;(a_i),(b_j))$.

Considérons à présent dans E une deuxième base régulière $(\bar{a}_i)$ ayant même nombre d'éléments n que la base (a_i) (ce qui sera toujours le cas, par exemple, si E est un espace vectoriel, d'après le th.6 du § 1 ; cf. § 1, exerc.9) . Soit $\bar{a}_i = \sum_{j=1}^{n} a_j a_{ji}$; la matrice carrée $\underline{P}=(a_{ji})$ est appelée la matrice de passage de la base (a_i) à la base $(\bar{a}_i)$. On peut dire que $\underline{P}$ est la matrice de l'application identique e de E sur lui-même, rapportée aux bases $(\bar{a}_i)$ et (a_i) (dans cet ordre) ; comme e est un automorphisme de E , $\underline{P}$ est une matrice inversible, et son inverse $\underline{P}^{-1}$ n'est autre que la matrice de passage de la base $(\bar{a}_i)$ à la base (a_i), d'après (14).

Réciproquement, si on se donne une matrice inversible $\underline{P}=(a_{ji})$ d'ordre n , les n éléments $\bar{a}_i = \sum_{j=1}^{n} a_j a_{ji}$ forment une base régulière de E ; en effet, si on pose $u(a_i)=\bar{a}_i$ $(1 \leqslant i \leqslant n)$, l'endomorphisme u de E ainsi défini est un automorphisme, car $\underline{P}$ n'est autre que la matrice $\underline{M}(u;(a_i),(a_i))$.

Soient (a'_i), $(\bar{a}'_i)$ les bases duales de (a_i) et $(\bar{a}_i)$ respectivement dans le dual E' de E (considéré comme module à droite sur A^0) ; comme la transposée de l'application identique de E est l'application identique de E' , la matrice $\underline{M}(e^*;(a'_i),(\bar{a}'_i))$ est la transposée de la matrice $\underline{M}(e;(\bar{a}_i),(a_i))=\underline{P}$; cela signifie que la matrice de passage de la base (a'_i) à la base $(\bar{a}'_i)$ est la contragrédiente $\overset{\vee}{P}$ de la matrice de passage $\underline{P}$ de la base (a_i) à la base $(\bar{a}_i)$. Revenant à la structure de A-module à gauche sur E' , on a donc

(16) $$a'_i = \sum_{j=1}^{n} a_{ij} \bar{a}'_j$$

d'où, si $x = \sum_{i=1}^{n} a_i \xi_i = \sum_{i=1}^{n} \bar{a}_i \bar{\xi}_i$, en remarquant que $\xi_i = \langle x, a'_i \rangle$ et $\bar{\xi}_i = \langle x, \bar{a}'_i \rangle$,

(17) $$\xi_i = \sum_{j=1}^{n} a_{ij}\,\overline{\xi}_j \qquad (1 \leqslant i \leqslant n)$$

formules dites du <u>changement de coordonnées</u> ; on remarquera qu'elles expriment les composantes de x sur la base (a_i) en fonction des composantes de x sur la base $(\overline{a}_i)$ et des éléments de P , c'est-à-dire de la matrice des composantes des $\overline{a}_i$ sur la base (a_i) : on dit que les composantes de x se transforment de façon <u>contravariante</u> (ou <u>contragrédiente</u>) par un changement de base. Les formules analogues exprimant les $\overline{\xi}_i$ en fonction des ξ_i sont

(18) $$\overline{\xi}_i = \sum_{j=1}^{n} \overline{a}_{ij}\,\xi_j \qquad (1 \leqslant i \leqslant n)$$

où $(\overline{a}_{ji}) = P^{-1}$. Si on désigne par x et $\overline{x}$ les matrices à une colonne (ξ_i) et $(\overline{\xi}_i)$ respectivement, les formules (17) et (18) équivalent aux deux formules (équivalentes)

(19) $$\begin{cases} x = P.\,\overline{x} \\ \overline{x} = P^{-1}.\,x \end{cases}$$

On peut d'ailleurs démontrer directement les formules (17) en remplaçant les $\overline{a}_i$ par leurs valeurs dans l'identité $\sum_{i=1}^{n} a_i\,\xi_i = \sum_{i=1}^{n} \overline{a}_i\,\overline{\xi}_i$ et identifiant les coefficients des a_i aux deux membres ; on peut aussi obtenir ces formules sous la forme (19) en appliquant la formule (15) au cas où u est l'automorphisme identique de E , rapporté aux bases $(\overline{a}_i)$ et (a_i) (dans cet ordre).

On voit de même que, si x' est une forme linéaire sur E , ξ'_i ses composantes sur la base (a'_i) , $\overline{\xi}'_i$ ses composantes sur la base $(\overline{a}'_i)$, on a

(20) $$\overline{\xi}'_i = \sum_{j=1}^{n} \xi'_j\,a_{ji} \qquad (1 \leqslant i \leqslant n)$$

On dit que les composantes d'une forme linéaire sur E se transforment de façon <u>covariante</u> (ou <u>corrédiente</u>) par changement de base ; si x' et $\overline{x}'$ sont les matrices à une colonne (ξ'_i) et $(\overline{\xi}'_i)$, dont les élément doivent

être considérés comme appartenant à A^0, on peut écrire ces formules

$$\overline{x}' = \underline{P}^* x'$$

la multiplication se faisant dans A^0 ; ou encore, en revenant aux matrices à éléments dans A

(21) $$\overline{x}'^* = x'^* . \underline{P} \quad .$$

9. Matrices équivalentes. Soient E et F deux A-modules unitaires à droite, ayant respectivement les bases régulières finies $(a_i)_{1 \leqslant i \leqslant n}$ et $(b_j)_{1 \leqslant j \leqslant m}$; soit u une application linéaire de E dans F , $\underline{U}$ la matrice correspondant à u , rapportée aux bases (a_i) et (b_j). Soit maintenant $(\overline{a}_i)$ (resp. $(\overline{b}_j)$) une autre base régulière de E (resp. F) ayant même nombre d'éléments que (a_i) (resp. (b_j)); soit $\underline{P}$ (resp. $\underline{Q}$) la matrice de passage de (a_i) à $(\overline{a}_i)$ (resp. de (b_j) à $(\overline{b}_j)$), et soit $\underline{U}'$ la matrice correspondant à u , rapportée aux bases $(\overline{a}_i)$ et $(\overline{b}_j)$. Si on pose $x = \sum_{i=1}^{n} a_i \xi_i = \sum_{i=1}^{n} \overline{a}_i \overline{\xi}_i$ et $u(x) = \sum_{j=1}^{m} b_j \eta_j = \sum_{j=1}^{m} \overline{b}_j \overline{\eta}_j$, on a, d'après les formules (15) et (19)

$$\underline{Q}.(\overline{\eta}_j) = \underline{UP}.(\overline{\xi}_i) \qquad \text{et} \qquad (\overline{\eta}_j) = \underline{U}'.(\overline{\xi}_i)$$

ce qui donne l'expression de $\underline{U}'$

(22) $$\underline{U}' = \underline{Q}^{-1}\underline{UP}$$

Définition 4. On dit que deux matrices $\underline{X}, \underline{X}'$, à m lignes et n colonnes, sur un anneau A ayant un élément unité, sont équivalentes, s'il existe une matrice carrée inversible P d'ordre m et une matrice carrée inversible Q d'ordre n , telles que

(23) $$\underline{X}' = \underline{PXQ} \quad .$$

Avec cette définition, on peut donc dire que lorsqu'on change de base dans deux modules E,F (ayant des bases régulières finies), la matrice d'une application linéaire de E dans F , rapportée aux nouvelles bases, est équivalente à la matrice de cette même application, rapportée aux anciennes bases.

Une autre interprétation consiste à considérer, comme au n°2, les applications linéaires u,u' de A_d^n dans A_d^m qui correspondent aux matrices $\underline{X},\underline{X}'$ respectivement, et les automorphismes φ et ψ de A_d^m et A_d^n, qui correspondent respectivement à $\underline{P}$ et $\underline{Q}$; alors la relation (23) équivaut à $u' = \varphi \circ u \circ \psi$.

Avec l'une ou l'autre interprétation, il est clair que la relation "$\underline{X}$ et $\underline{X}'$ sont équivalentes" est bien une relation d'équivalence dans l'ensemble des matrices à m lignes et n colonnes sur A , ce qui justifie la terminologie adoptée.

Exemples de matrices équivalentes. 1) On dit que deux matrices $\underline{X}=(\xi_{ij})$ et $\underline{X}'=(\xi'_{ij})$, à m lignes et n colonnes, "ne diffèrent que par l'ordre des lignes", s'il existe une permutation σ de l'intervalle $[1,m]$ de $\mathbb{N}$ telle que pour $1 \leqslant i \leqslant m$, $1 \leqslant j \leqslant n$, on ait $\xi'_{ij} = \xi_{\sigma(i),j}$. S'il en est ainsi les matrices $\underline{X}$ et $\underline{X}'$ sont équivalentes ; en effet, avec les notations précédentes, et en désignant par $(e_j)_{1 \leqslant j \leqslant n}$, $(f_i)_{1 \leqslant i \leqslant m}$ les bases canoniques de A_d^n et A_d^m respectivement, on a $u'=\varphi \circ u$, où φ est l'automorphisme de A_d^m défini par les relations $\varphi(f_i)=f_{\sigma(i)}$ pour $1 \leqslant i \leqslant m$; d'où $\underline{X}'=\underline{P}\underline{X}$, où $\underline{P}$ est la matrice dont la ligne d'indice i est identique à la ligne d'indice $\sigma(i)$ de la matrice unité $\underline{I}_m$.

On dit de même que $\underline{X}$ et $\underline{X}'$ ne diffèrent que par lbrdre des colonnes", s'il existe une permutatica τ de $[1,n]$ telle que $\xi'_{ij}= \xi_{i,\tau(j)}$ pour tout couple d'indices (i,j) . On montre que dans ce cas $\underline{X}$ et $\underline{X}'$ sont équivalentes, et que de façon plus précise, on a $\underline{X}'=\underline{X}\underline{Q}$, où $\underline{Q}$ est la matrice dont la colonne d'indice j $(1 \leqslant j \leqslant n)$ est identique à la colonne d'indice $\tau(j)$ de la matrice $\underline{I}_n$.

2) Supposons maintenant que, pour un indice j déterminé, on ait, pour $1 \leqslant i \leqslant m$, $\xi'_{ij} = \xi_{ij} + \xi_{ik}\mu$, où k est un indice $\neq j$, et μ un élément quelconque de A : on dit alors que $\underline{X}'$ se déduit de $\underline{X}$ en ajoutant à la colonne d'indice j de $\underline{X}$ la colonne d'indice k multipliée à droite par μ . Montrons encore que dans ce cas $\underline{X}$ et $\underline{X}'$ sont équivalentes ; en effet, avec les mêmes notations, on a $u'(e_j) = u(e_j) + u(e_k)\mu = u(e_j + e_k\mu)$, donc $u' = u \circ \psi$, où ψ est l'automorphisme de A_d^n défini par $\psi(e_j) = e_j + e_k\mu$, $\psi(e_h) = e_h$ pour $h \neq j$ (il s'agit bien d'un automorphisme, car l'application linéaire ψ' définie par $\psi'(e_j) = e_j - e_k\mu$, $\psi'(e_h) = e_h$ pour $h \neq j$, est bien réciproque de ψ). On a par suite $\underline{X}' = \underline{X}\underline{Q}$, où $\underline{Q}$ est la matrice qu'on obtient en ajoutant à la colonne d'indice j de $\underline{I}_n$ la colonne d'indice k de cette matrice, multipliée à droite par μ .

On a un résultat analogue quand $\underline{X}'$ se déduit de $\underline{X}$ en ajoutant à la ligne d'indice i de $\underline{X}$ la ligne d'indice $h \neq i$, multipliée à gauche par un élément quelconque $\lambda \in A$; cette fois on a $\underline{X}' = \underline{P}\underline{X}$, où P se déduit de $\underline{I}_m$ en ajoutant à la ligne d'indice i de cette matrice la ligne d'indice h multipliée par λ (*) .

Proposition 4. Pour que deux matrices à m lignes et n colonnes sur un corps K soient équivalentes, il faut et il suffit qu'elles aient même rang.

Il est immédiat que la condition est nécessaire, car si $\underline{X}$ et $\underline{X}'$ sont équivalentes, et si u et u' sont les applications linéaires de K_d^n dans K_d^m qui leur correspondent, on a $u' = \varphi \circ u \circ \psi$, où φ est un automorphisme de K_d^m et ψ un automorphisme de K_d^n ; il en résulte que $u(K_d^n)$ et $u'(K_d^n)$ ont même dimension.

Pour voir que la condition est suffisante, nous allons voir que toute matrice $\underline{X}$ de rang r $(r \leqslant \mathrm{Min}(m,n))$ est équivalente à la matrice $\underline{U} = (\mu_{ij})$ où $\mu_{ii} = e$ (élément unité de K) pour $1 \leqslant i \leqslant r$, et $\mu_{ij} = 0$ pour tout autre couple d'indices.

Pour cela, nous montrerons que, si u est l'application linéaire de K_d^n dans K_d^m qui correspond à $\underline{X}$, il existe une base (a_j) de K_d^n et une base (b_i) de K_d^m telles que la matrice de u, rapportée à ces nouvelles bases, soit identique à $\underline{U}$.

En effet, $H = {}^{-1}u(0)$ est un sous-espace à n-r dimensions de K_d^n ; soit G un supplémentaire de H dans K_d^n, et prenons une base (a_j) de K_d^n telle que, pour $1 \leqslant j \leqslant r$, les a_j forment une base de G, et pour $r+1 \leqslant j \leqslant n$, une base de H (§1, th.5). Alors les vecteurs $u(a_j)$ forment une base de $u(K_d^n)$ pour $1 \leqslant j \leqslant r$; on peut donc trouver une base (b_i) de K_d^m dont les vecteurs d'indice $i \leqslant r$ soient identiques aux $u(a_j)$. Il est clair alors que $\underline{U}$ est bien la matrice de u, rapportées aux deux bases ainsi construites.

La matrice $\underline{U}$ est appelée <u>matrice canonique de rang r</u>, à m lignes et n colonnes, sur le corps K.

10. <u>Matrices carrées semblables</u>. Soit E un module unitaire sur un anneau A, ayant deux bases régulières (a_i) et $(\bar{a}_i)$ de n éléments. Soit u un endomorphisme de E, $\underline{U}$ et $\underline{U}'$ les matrices carrées correspondant à u, rapportée respectivement aux bases $(a_i),(a_i)$ et aux bases $(\bar{a}_i),(\bar{a}_i)$; si $\underline{P}$ est la matrice de passage de la base (a_i) à la base $(\bar{a}_i)$, il résulte de la formule (22) qu'on a

(24) $$\underline{U}' = \underline{P}^{-1}\underline{U}\underline{P} \quad .$$

<u>Définition 5</u>. <u>On dit que deux matrices carrées $\underline{X},\underline{X}'$ d'ordre n sur un anneau A ayant un élément unité sont semblables, s'il existe une matrice carrée inversible $\underline{P}$ d'ordre n, telle que</u>

(25) $$\underline{X}' = \underline{P}\underline{X}\underline{P}^{-1}$$

Avec cette définition, on peut donc dire que, lorsqu'on rapporte un endomorphisme de E à la <u>même</u> base dans les deux sens, la matrice correspondante se transforme en une matrice <u>semblable</u> pour tout changement de base.

Une autre interprétation consiste à considérer les endomorphismes u et u' de A_d^n qui correspondent respectivement aux matrices $\underline{X},\underline{X}'$, et l'automorphisme φ de A_d^n qui correspond à la matrice $\underline{P}$; la relation (25) équivaut alors à $u'=\varphi\circ u\circ\varphi^{-1}$.

Il est clair, ici encore, que la relation "$\underline{X}$ et $\underline{X}'$ sont semblables" est une relation d'équivalence dans l'ensemble des matrices carrées d'ordre n sur A .

Remarques. 1) Si on échange deux lignes (ou deux colonnes) dans une matrice carrée $\underline{X}$, on obtient une matrice équivalente à $\underline{X}$, mais non semblable à $\underline{X}$ en général. On obtient une matrice semblable à $\underline{X}=(\xi_{ij})$ si on effectue la même permutation σ sur les lignes et les colonnes, c'est-à-dire si on prend la matrice $\underline{X}'=(\xi'_{ij})$, où $\xi'_{ij}=\xi_{\sigma(i),\sigma(j)}$ pour tout couple d'indices.

2) Deux matrices carrées semblables sur un même corps K ont évidemment même rang, puisqu'elles sont équivalentes. Mais ici cette condition nécessaire n'est plus suffisante pour que deux matrices sur K soient semblables ; au chap.V, nous donnerons des conditions nécessaires et suffisantes lorsque K est un corps commutatif.

3) Soient $\underline{X},\underline{X}'$ deux matrices carrées d'ordre n , qui s'écrivent sous forme de "tableaux diagonaux" de matrices carrées :

$$\underline{X}=\begin{pmatrix} \underline{X}_1 & 0 & \dots & 0 \\ 0 & \underline{X}_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \underline{X}_p \end{pmatrix} \qquad \underline{X}'=\begin{pmatrix} \underline{X}'_1 & 0 & \dots & 0 \\ 0 & \underline{X}'_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \underline{X}'_p \end{pmatrix}$$

correspondant à la même partition de l'ensemble d'indices $[1,n]$ pour $\underline{X}$ et $\underline{X}'$. Si, pour $1 \leqslant i \leqslant p$, $\underline{X}_i$ et $\underline{X}'_i$ sont semblables, $\underline{X}$ et $\underline{X}'$ sont semblables, car si $\underline{X}'_i = \underline{P}_i \underline{X}_i \underline{P}_i^{-1}$, on a $\underline{X}' = \underline{P}\underline{X}\underline{P}^{-1}$, avec

$$\underline{P} = \begin{pmatrix} \underline{P}_1 & 0 & \dots & 0 \\ 0 & \underline{P}_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \underline{P}_p \end{pmatrix}$$

comme il résulte de la formation du produit "par blocs".

11. Matrice d'une application semi-linéaire. Soient A et B deux anneaux isomorphes, ayant un élément unité, et soit $a \longrightarrow a^\sigma$ un isomorphisme de B sur A. Pour toute matrice $\underline{X} = (\xi_{\lambda\mu})$ sur B, on désigne par $\underline{X}^\sigma$ la matrice $(\xi_{\lambda\mu}^\sigma)$ sur A ; il est immédiat qu'on a $(\underline{X}+\underline{Y})^\sigma = \underline{X}^\sigma + \underline{Y}^\sigma$, $(\underline{X}\underline{Y})^\sigma = \underline{X}^\sigma . \underline{Y}^\sigma$, $(a\underline{X})^\sigma = a^\sigma . \underline{X}^\sigma$ et $(\underline{X}a)^\sigma = \underline{X}^\sigma . a^\sigma$ (les opérations écrites étant supposées avoir un sens).

Soient E un A-module unitaire à droite ayant une base régulière $(a_i)_{1 \leqslant i \leqslant m}$, F un B-module unitaire à droite ayant une base régulière $(b_j)_{1 \leqslant j \leqslant n}$. Soit u une application semi-linéaire (§2, n°12) de F dans E, relative à l'isomorphisme σ ; si on pose $u(b_j) = \sum_{i=1}^{m} a_i a_{ij}$, il correspond à u la matrice à m lignes et n colonnes (a_{ij}), à éléments dans A ; on dit encore que c'est la matrice correspondant à u, rapportée aux bases (b_j) et (a_i), et on la note parfois $\underline{M}(u;(b_j),(a_i))$.

Si on identifie comme d'ordinaire un élément $x \in F$ (resp. $y \in E$) avec la matrice à une colonne formée de ses composantes sur la base (b_j) (resp. (a_i)), on a ici

$$u(x) = \underline{U}.x^\sigma \tag{26}$$

$\underline{U}$ étant la matrice correspondant à u, rapportée aux bases (b_j) et (a_i).

Soit C un troisième anneau isomorphe à B et à A, $\beta \longrightarrow \beta^\tau$ un isomorphisme de C sur B, G un C-module à droite, ayant une base régulière

$(c_k)_{1 \leqslant k \leqslant p}$. Soit v une application semi-linéaire de G dans F correspondant à l'isomorphisme τ ; si $\underline{V}$ est la matrice correspondant à v , rapportée aux bases (c_k) et (b_j) (matrice dont les éléments appartiennent donc à B), la matrice qui correspond à l'application semi-linéaire composée u.v (relative à l'isomorphisme $\sigma \circ \tau$), rapportée aux bases (c_k) et (a_i) , est la matrice $\underline{U}.\underline{V}^{\sigma}$, comme il résulte de (26).

Soient (a'_i), (b'_j) les <u>bases duales</u> de (a_i) et (b_j) respectivement dans E' et F' ; on sait que la <u>transposée</u> u^* de u est une application semi-linéaire de E' dans F' , relative à l'isomorphisme σ^{-1} ; de la formule (19) du § 2 on déduit aisément que la matrice correspondant à u^* , rapportée aux bases (a'_i) et (b'_j) est la matrice $(\underline{U}^{\sigma^{-1}})^*$, <u>transposée</u> de la matrice $\underline{U}^{\sigma^{-1}}$, $\underline{U}$ étant la matrice qui correspond à u , rapportée aux bases (b_j) et (a_i) .

Enfin, si $(\overline{a}_i)$ est une seconde base régulière de m éléments de E , $(\overline{b}_j)$ une seconde base régulière de n éléments de F , $\underline{P}$ (resp. $\underline{Q}$) la matrice de passage de (a_i) à $(\overline{a}_i)$ (resp. de (b_j) à $(\overline{b}_j)$), la matrice correspondant à u , rapportée aux nouvelles bases $(\overline{b}_j)$ et $(\overline{a}_i)$ est la matrice

$$\underline{U}' = \underline{P}^{-1}\underline{U}\underline{Q}^{\sigma} \quad ,$$

comme il résulte des formules (19) et (26) .

<u>Exercices</u>. 1) Soit A un anneau ayant un élément unité, (L_i) $(1 \leqslant i \leqslant p)$ une partition de l'intervalle $[1,n]$ de $\mathbb{N}$. On met toute matrice carrée $\underline{X}$ d'ordre n sur A , sous la forme d'un tableau carré de matrices $(\underline{X}_{ij})$ correspondant à la même partition (L_i) de l'ensemble commun des indices des lignes et des colonnes.

a) Montrer que les matrices $\underline{X}$ pour lesquelles le tableau $(\underline{X}_{ij})$ <u>n'a que des zéros au-dessus de la diagonale</u> (c'est-à-dire que $\underline{X}_{ij}=0$ pour $i<j$) forment un <u>sous-anneau</u> de l'anneau des matrices

matrices carrées d'ordre n sur A . Comment peut-on caractériser les endomorphismes du module A_d^n auxquels correspondent ces matrices?

b) Si chacune des matrices diagonales $\underline{X}_{ii}$ d'une telle matrice $\underline{X}$ est inversible, montrer que $\underline{X}$ est inversible, et que $\underline{X}^{-1}$ est encore un tableau de matrices n'ayant que des zéros au-dessus de la diagonale. Lorsque A est un corps, montrer que cette condition suffisante pour que $\underline{X}$ soit inversible est aussi nécessaire.

2) Soit $\underline{X}$ une matrice à m lignes et n colonnes sur un corps K ; montrer que le rang $\rho(\underline{X})$ est le plus grand des rangs des sous-matrices carrées de $\underline{X}$ (soit $\rho(\underline{X})=r$; si $a_1,..,a_r$ sont r colonnes de $\underline{X}$ formant un système libre dans K_d^m , et si on complète ces r éléments par m-r des vecteurs de la base canonique $(e_i)_{1\leqslant i\leqslant m}$ de K_d^m , montrer que les composantes de $a_1,a_2,\ldots,a_r$ sur les r autres vecteurs de la base canonique forment une matrice carrée inversible d'ordre r).

3) Soient $\underline{X},\underline{X}',\underline{Y},\underline{Y}'$ quatre matrices carrées d'ordre n sur un anneau ayant un élément unité ; on suppose en outre que $\underline{X}$ soit inversible. Pour qu'il existe deux matrices carrées inversibles $\underline{P},\underline{Q}$ telles que $\underline{X}'=\underline{PXQ}$ et $\underline{Y}'=\underline{PYQ}$, il faut et il suffit que $\underline{X}'$ soit inversible, et que les matrices $\underline{YX}^{-1}$ et $\underline{Y}'\underline{X}'^{-1}$ soient semblables.

§4. Algèbres.

1. Définition d'une algèbre. Définition 1. Etant donné un anneau commutatif A, ayant un élément unité ε , on appelle algèbre (ou système hypercomplexe) sur A , un anneau à opérateurs E , dont la loi externe a l'anneau A pour ensemble d'opérateurs, et définit, avec l'addition dans E , une structure de A-module unitaire sur E .

En d'autres termes, une algèbre sur A est un anneau E muni d'une loi externe (notée multiplicativement à gauche), ayant A comme domaine d'opérateurs, et satisfaisant aux identités suivantes :

(1) $\alpha(x+y)=\alpha x + \alpha y$

(2) $(\alpha+\beta)x = \alpha x + \beta x$

(3) $(\alpha\beta)x = \alpha(\beta x)$

(4) $\varepsilon x = x$

(5) $\alpha(xy) = (\alpha x)y = x(\alpha y)$

($\alpha \in A$, $\beta \in A$, $x \in E$, $y \in E$)

On en déduit la formule générale de distributivité

(6) $$(\sum_i \alpha_i x_i)(\sum_j \beta_j y_j) = \sum_{i,j} (\alpha_i \beta_j)(x_i y_j)$$

($\alpha_i \in A$, $\beta_j \in A$, $x_i \in E$, $y_j \in E$) .

Exemples. 1) Tout anneau E ayant un élément unité peut être muni d'une structure d'algèbre par rapport à son centre A , le composé d'un opérateur $z \in A$ et d'un élément $x \in E$ étant le produit zx ($=xz$) pour la multiplication de l'anneau.

2) Si, sur un anneau quelconque E , on considère la structure d'anneau à opérateurs définie par la loi externe $(n,x) \longrightarrow n.x$, où $n \in Z$ (chap.I, § 8), cette structure est une structure d'algèbre par rapport à l'anneau Z .

Sur une algèbre E , la structure d'anneau à opérateurs opposée à celle de E est encore une structure d'algèbre ; on dit que E , muni de cette structure, est l'algèbre opposée à l'algèbre donnée.

Si on restreint la loi externe d'une algèbre E sur un anneau A , à un sous-anneau B de A (ayant même élément unité que A), cette loi définit (avec la structure d'anneau de E) une nouvelle structure d'algèbre sur l'ensemble E , structure qu'on aura soin de distinguer de la structure d'algèbre ayant A comme domaine d'opérateurs.

Remarques. 1) Nous aurons plus tard à considérer des structures algèbriques définies, sur un ensemble E, par la donnée de deux lois internes et d'une loi externe ayant un anneau commutatif comme ensemble d'opérateurs, tous les axiomes des algèbres étant vérifiés, à l'exception de l'associativité de la multiplication dans E ; par extension, un ensemble muni d'une telle structure sera dit "algèbre non associative".

2) On pourrait tenter de généraliser la déf.1 en supprimant la restriction de commutativité faite sur l'anneau d'opérateurs A ; mais en fait, si on se borne au cas (le plus intéressant en pratique) où tout élément de E est égal à un produit de deux éléments de E (autrement dit, le cas où $E.E=E$, ce qui a toujours lieu, en particulier, lorsque E possède un élément unité), cette généralisation ne serait qu'apparente. En effet, pour $\alpha \in A$, $\beta \in A$, $x \in E$, $y \in E$, on a, d'après (3) et (5)

$$(\alpha\beta)(xy) = \alpha(\beta(xy)) = \alpha(x(\beta y)) = (\alpha x)(\beta y)$$

et d'autre part

$$(\beta\alpha)(xy) = \beta(\alpha(xy)) = \beta((\alpha x)y) = (\alpha x)(\beta y)$$

d'où $(\alpha\beta-\beta\alpha)(xy)=0$. Comme par hypothèse, tout élément de E se met sous la forme xy, on voit que l'idéal bilatère $\mathfrak{b}$ de A engendré par les éléments $\alpha\beta-\beta\alpha$, est contenu dans l'annulateur $\mathfrak{a}$ du A-module E ; or, il est clair que $A/\mathfrak{b}$ est commutatif, donc il en est de même de l'anneau $A/\mathfrak{a} = (A/\mathfrak{b})/(\mathfrak{a}/\mathfrak{b})$; si on passe de la structure de A-module sur E à sa structure normale associée, on obtient sur E une structure d'algèbre par rapport à $A/\mathfrak{a}$, qu'on peut assimiler à la structure donnée.

Il arrivera souvent qu'on ait à considérer, sur une algèbre E, une structure de module à gauche par rapport à un sous-anneau non commutatif B de E ; on se gardera de croire que E soit une algèbre sur l'anneau B.

2. Bases d'une algèbre. Table de multiplication. Les algèbres les plus intéressantes sont celles qui, considérées comme modules par rapport à leur anneau d'opérateurs A, admettent une base régulière par rapport à A (§ 1, n° 8) ; c'est toujours le cas pour les algèbres sur un corps, qui sont celles qu'on rencontre le plus fréquemment.

Dans une algèbre E ayant une base régulière par rapport à son anneau d'opérateurs A, la multiplication est bien déterminée si on connaît, d'une part la multiplication dans l'anneau A, et d'autre part les produits deux à deux des éléments d'une base régulière de E : cela résulte de la formule (6). Si $(a_\lambda)_{\lambda \in L}$ est une base régulière de E par rapport à A, tout élément de E s'écrit d'une seule manière sous forme d'une combinaison linéaire $\sum_\lambda a_\lambda a_\lambda$; le calcul du produit de deux éléments de E est ramené à celui des produits $a_\lambda a_\mu$, et comme on peut écrire

$$a_\lambda a_\mu = \sum_\rho \gamma_{\lambda\mu\rho} a_\rho \tag{7}$$

la connaissance des éléments $\gamma_{\lambda\mu\rho} \in A$ qui figurent dans ces relations détermine complètement la multiplication dans E ; on dit que les relations (7) constituent la table de multiplication de la base régulière (a_λ) considérée.

Ce nom vient de ce que, dans le cas où l'ensemble d'indices L est un intervalle $[1,n]$ de $\mathbb{N}$, on imagine les relations (7) écrites en disposant les seconds membres de ces relations en un tableau carré

	a_1	a_2	...	a_j	...	a_n
a_1						
a_2						
:						
a_i				$\sum_k \gamma_{ijk} a_k$		
:						
a_n						

étant entendu que l'élément qui figure dans la ligne de a_i et la colonne de a_j est la valeur du produit $a_i a_j$.

Les éléments $\gamma_{\lambda\mu\nu}$ qui figurent dans les relations (7) ne sont pas arbitraires, car on doit avoir les relations d'associativité

(8) $$(a_\lambda a_\mu) a_\rho = a_\lambda (a_\mu a_\rho)$$

quels que soient les indices λ , μ , ρ ; d'après (7), ces relations équivalent à

(9) $$\sum_\nu \gamma_{\lambda\mu\nu}\gamma_{\nu\rho\sigma} = \sum_\nu \gamma_{\lambda\nu\sigma}\gamma_{\mu\rho\nu}$$

quels que soient les indices λ , μ , ρ , σ .

Réciproquement, supposons donnés un A-module unitaire E , une base régulière (a_λ) de E , et une famille $(\gamma_{\lambda\mu\nu})$ d'éléments de A satisfaisant aux relations (9) ; on peut alors définir une multiplication sur E en posant, pour $x = \sum_\lambda \xi_\lambda a_\lambda$, $y = \sum_\lambda \eta_\lambda a_\lambda$, $xy = \sum_{\lambda,\mu,\nu} \xi_\lambda \eta_\mu \gamma_{\lambda\mu\nu} a_\nu$; la vérification de la distributivité de cette loi par rapport à l'addition dans E est immédiate ; les conditions (9) entraînent son associativité, et par suite cette loi et l'addition dans E définissent sur E une structure d'anneau ; enfin, il est clair que la loi externe sur E définit, avec cette structure d'anneau, une structure d'algèbre par rapport à A . Ce mode de définition d'une algèbre est fréquemment employé.

On notera que les éléments $\gamma_{\lambda\mu\nu}$ dépendent de la base régulière (a_λ) choisie ; en général, la table de multiplication change de forme quand on change de base.

Si l'algèbre E est définie de la manière précédente, on définira sur E la structure <u>opposée</u> en prenant, pour la même base (a_λ), la table de multiplication dont les constantes sont $\gamma'_{\lambda\mu\nu} = \gamma_{\mu\lambda\nu}$. En particulier, pour que E soit <u>commutative</u>, il faut et il suffit que $\gamma_{\mu\lambda\nu} = \gamma_{\lambda\mu\nu}$ quels que soient λ, μ, ν.

En d'autres termes, la table de multiplication de l'algèbre opposée de E (par rapport à la même base) s'obtient en prenant la <u>symétrique</u> de la table de multiplication de E par rapport à sa "diagonale principale"; une algèbre commutative est caractérisée par le fait que sa table de multiplication est <u>symétrique</u> par rapport à sa diagonale.

De même, pour qu'un élément $a_\varkappa$ de la base régulière considérée soit <u>élément unité</u> de E, il faut et il suffit que $a_\varkappa a_\lambda = a_\lambda a_\varkappa = a_\lambda$ quel que soit λ, c'est-à-dire que $\gamma_{\varkappa\lambda\mu} = \gamma_{\lambda\varkappa\mu} = 0$ pour $\mu \neq \lambda$, et $\gamma_{\varkappa\lambda\lambda} = \gamma_{\lambda\varkappa\lambda} = \varepsilon$, quel que soit λ.

Une algèbre E par rapport à un <u>corps</u> K est un <u>espace vectoriel</u> par rapport à K ; lorsque E a un nombre fini de dimensions par rapport à K, ce nombre se note $[E:K]$, et s'appelle le <u>rang</u> de l'algèbre E par rapport à K ; lorsque E a une infinité de dimensions, on dit encore que son rang est infini.

Si K' est un <u>sous-corps</u> de K, E est aussi une algèbre par rapport à K' ; si (a_λ) est une base de E par rapport à K, (ρ_μ) une base de K par rapport à K', $(\rho_\mu a_\lambda)$ est une base de E par rapport à K' (§1, prop.11) ; en particulier :

Proposition 1. *Si les rangs* $[E:K]$ *et* $[K:K']$ *sont finis, il en est de même de* $[E:K']$, *et on a*

(10) $$[E:K'] = [E:K][K:K']$$

Réciproquement si $[E:K']$ *est fini, il en est de même de* $[E:K]$ *et* $[K:K']$, *et on a la relation* (10).

3. Sous-algèbres. Idéaux. Algèbres quotients. Soit E une algèbre par rapport à un anneau A. Il est immédiat que, sur un *sous-anneau* quelconque F de l'anneau à opérateurs E (chap.I, § 8, n° 4)(*), la structure induite par la structure d'algèbre de E est encore une structure d'algèbre par rapport à A ; muni de cette structure, F est appelé une *sous-algèbre* de E. Si M est une partie quelconque de E, l'ensemble N des éléments de E permutables avec tous les éléments de M, est une sous-algèbre de E (chap.I, § 8, prop.2) ; en particulier, le *centre* de E est une sous-algèbre de E.

Il n'y a pas à revenir sur la notion d'idéal (à gauche, à droite ou bilatère) dans une algèbre : elle a été définie plus généralement pour un anneau à opérateurs quelconque (chap.I, § 8, n° 5).

Si $\mathfrak{a}$ est un idéal bilatère d'une algèbre E (par rapport à un anneau A) la structure d'anneau à opérateurs du quotient $E/\mathfrak{a}$ est une structure d'algèbre par rapport à A, comme on le vérifie aussitôt ; on dit que $E/\mathfrak{a}$ est l'*algèbre quotient* de E par $\mathfrak{a}$.

4. Représentations. Soient E et F deux algèbres par rapport au *même* anneau A ; on a déjà défini (chap.I, § 8, n° 8) les *représentations* de E dans F : rappelons qu'une application u de E dans F est une représentation si elle vérifie les identités

$$u(x+y)=u(x)+u(y)\ ,\quad u(xy)=u(x)u(y)\ ,\quad u(ax)=au(x)\quad (a\in A, x\in E, y\in E)$$

On peut donc encore dire que u est une représentation de E dans F si elle est une application linéaire du A-module E dans le A-module F, et une représentation pour les multiplications dans E et dans F.

Toutes les propriétés des représentations d'anneaux à opérateurs s'appliquent en particulier aux représentations des algèbres : si u est une représentation de E dans F, $u(E)$ est une sous-algèbre de F ; $\mathfrak{a} = u^{-1}(0)$ est un idéal bilatère de E, $u(E)$ est isomorphe à l'algèbre quotient $E/\mathfrak{a}$, et u est composée d'un isomorphisme de $E/\mathfrak{a}$ sur $u(E)$ et de l'homomorphisme canonique de E sur $E/\mathfrak{a}$; si G est une sous-algèbre de E, $u(G)$ est une sous-algèbre de F, isomorphe à l'algèbre quotient $G/(G \cap \mathfrak{a})$ et aussi à l'algèbre quotient $(G+\mathfrak{a})/\mathfrak{a}$.

Si E admet une base régulière (e_λ), une représentation f de E dans F est entièrement déterminée par les éléments $f(e_\lambda)$ (§ 2, prop. 3); inversement, la donnée de ces éléments détermine une application linéaire f du A-module E dans le A-module F ; pour que cette application soit une représentation de l'algèbre E dans l'algèbre F, il faut et il suffit, d'après la formule de distributivité (6), qu'on ait identiquement $f(e_\lambda e_\mu) = f(e_\lambda) f(e_\mu)$ pour tout couple (λ, μ) d'indices.

Lorsque E possède un élément unité e, l'application $a \to ae$ est une représentation h de l'anneau A dans l'algèbre E (A étant considéré comme algèbre par rapport à lui-même) ; si $ae = 0$, on a, pour tout $x \in E$, $ax = a(ex) = (ae)x = 0$, donc l'idéal bilatère $\mathfrak{a} = h^{-1}(0)$ de A n'est autre que l'annulateur (§ 1, n° 4) de E, et $h(A)$ est une sous-algèbre de E, isomorphe à $A/\mathfrak{a}$. Lorsque la structure de A-module de E est normale (§ 1, n° 4), ce qui est le cas le plus fréquent dans les applications, on a $\mathfrak{a} = (0)$ et $h(A)$ est isomorphe à A ; comme $ax = (ae)x$, il n'y a pas lieu de faire de distinction entre la structure d'algèbre de E relative à A et celle relative à $h(A)$; aussi identifie-t-on d'ordinaire A et $h(A)$,

considérant donc l'anneau d'opérateurs A comme une sous-algèbre de E , contenue dans le centre de E et ayant même élément unité que E . Quand on peut faire cette identification, on notera que tout idéal de l'anneau E (sans opérateur) est aussi un idéal de l'algèbre E (par contre un sous-anneau de l'anneau E sans opérateur n'est pas nécessairement une sous-algèbre de E).

Remarque. On a déjà signalé (chap.I, § 8) que lorsqu'on considère sur un ensemble E plusieurs structures d'anneau à opérateurs (et en particulier plusieurs structures d'algèbre) ayant même structure d'anneau sous-jacente, il y a lieu de distinguer soigneusement les sous-algèbres, idéaux, représentations, etc., relatifs à ces diverses structures. En particulier, considérons sur un anneau E , deux structures d'algèbre par rapport à des sous-anneaux distincts A,B de son centre, et soit a un élément de A n'appartenant pas à B ; pour toute représentation f de E , considérée comme algèbre sur A , on doit avoir $f(ax)=af(x)=f(a)f(x)$ quels que soit $x \in E$; au contraire, si g est une représentation de E , considérée comme algèbre sur B , on aura $g(ax)=g(a)g(x)$, mais en général $g(ax) \neq ag(x)$.

5. Produits et sommes directes d'algèbres. Soit (E_ι) une famille d'algèbres sur un même anneau A ; il est immédiat que l'anneau à opérateurs $E=\prod_\iota E_\iota$, produit des E_ι (chap.I, § 8, n° 10) est encore une algèbre sur A , qu'on appelle l'algèbre produit des algèbres E_ι ; toutes les propriétés des produits d'anneaux à opérateurs s'appliquent en particulier aux produits d'algèbres.

Soit F une algèbre sur A , (F_ι) une famille de sous-algèbres de A , telle que F , considéré comme A-module, soit somme directe (§ 1, n° 7)

des sous-modules F_ι ; par abus de langage, on dit encore que l'algèbre F est <u>somme directe des sous-algèbres</u> F_ι . Mais, il faut distinguer soigneusement cette notion de celle de <u>produit</u> d'algèbres : même lorsque l'ensemble d'indices est <u>fini</u>, l'algèbre F n'est isomorphe au produit des sous-algèbres F_ι que lorsqu'elle est leur <u>composée directe</u> (chap.I, § 8, n° 11), ce qui n'a lieu que lorsque les F_ι sont toutes des <u>idéaux bilatères</u> de F , ou, ce qui revient au même, lorsque $F_\iota . F_\varkappa = \{0\}$ pour tout couple d'indices distincts (chap.I, § 8, prop.7). Il en résulte que, si les F_ι ne sont pas tous des idéaux bilatères de F , la loi multiplicative dans F <u>n'est pas entièrement déterminée</u> par les lois multiplicative de chacune des sous-algèbres F_ι : pour la déterminer il faut savoir en outre comment se multiplient deux éléments appartenant à deux F_ι distincts.

6. <u>Exemples d'algèbres : I. Anneaux d'endomorphismes</u>. Soit E un module à droite sur un anneau A ayant un élément unité ; nous avons vu (§ 3) que l'ensemble $\mathcal{L}(E)$ des endomorphismes de E est muni d'une structure d'anneau et d'une loi externe $u \longrightarrow \gamma u$ ayant pour domaine d'opérateurs le <u>centre</u> C de l'anneau A ; comme cette loi externe et l'addition dans $\mathcal{L}(E)$ définissent une structure de module unitaire, et que d'autre part, on a $\gamma(u \circ v) = (\gamma u) \circ v = u \circ (\gamma v)$ quels que soient $\gamma \in C$ et les endomorphismes u et v , on voit que $\mathcal{L}(E)$ est ainsi muni d'une structure d'<u>algèbre</u> par rapport à C , ayant pour élément unité l'application identique de E sur lui-même.

Le cas le plus important est celui où E est un module à droite unitaire ayant une base régulière de n éléments ; alors $\mathcal{L}(E)$ est isomorphe à <u>l'anneau des matrices carrées d'ordre n</u> sur l'anneau A que nous désignerons par $\mathcal{M}_n(A)$. Lorsque A est commutatif, $\mathcal{M}_n(A)$ admet une base régulière de n^2 éléments par rapport à A , formée des matrices E_{ij} ,

où E_{ij} désigne la matrice carrée dont tous les éléments sont nuls à l'exception de l'élément appartenant à la ligne d'indice i et la colonne d'indice j , qui est égal à l'élément unité ε de A . On dit que cette base est la base canonique de $\mathcal{M}_n(A)$. Sa table de multiplication est donnée par

$$(11) \qquad \begin{cases} E_{ij}E_{hk} = 0 & \text{si } j \neq h \\ E_{ij}E_{jk} = E_{ik} \end{cases}$$

L'élément unité I_n de $\mathcal{M}_n(A)$ est égal à $\sum_{i=1}^{n} E_{ii}$; l'anneau A peut être identifié au sous-anneau des matrices aI_n $(a \in A)$.

7. Exemples d'algèbres : II. Extensions quadratiques d'un anneau. Soit A un anneau commutatif ayant un élément unité. On appelle extension quadratique de A une algèbre E par rapport à A ayant une base régulière formée de deux éléments, dont l'un est l'élément unité de E ; on identifie donc A à un sous-anneau de E , l'élément unité de E étant identifié avec l'élément unité de A , que nous noterons 1 . Si u est le second élément de la base régulière considérée, tout élément de E s'écrit donc d'une seule manière sous la forme $a+bu$, où $a \in A$ et $b \in A$. Comme $1.u=u.1=u$ par hypothèse, E est commutatif, et la table de multiplication de la base (1,u) est entièrement définie par la donnée de u^2 , c'est-à-dire la relation

$$(12) \qquad u^2 = au+\beta \qquad (\alpha \in A,\ \beta \in A)$$

qui définit u^2 ; les conditions d'associativité sont remplies quels que soient α et β , qui peuvent donc être pris arbitrairement dans A .

Etudions la structure de E lorsque A est un corps de caractéristique $\neq 2$; si on remarque que

$$(a+bu)^2 = (ba+2a)(a+bu)+b^2\beta-aba-a^2$$

en faisant $b=1$, $a=-\alpha/2$ dans cette formule, on voit qu'on peut prendre comme nouvelle base de E les éléments 1 et $v=u-\frac{\alpha}{2}$, avec $v^2=\gamma$, où $\gamma \in A$. Cela étant, distinguons plusieurs cas :

1° γ n'est pas un carré dans A . Alors E est un corps ; en effet, si $a+bv\neq 0$, on a $(a+bv)(a-bv)=a^2-b^2\beta\neq 0$ par hypothèse, donc $\frac{a}{a^2-b^2\beta} - \frac{b}{a^2-b^2\beta} v$ est inverse de $a+bv$.

Lorsque A est le corps des nombres réels, -1 n'est pas un carré dans A ; les éléments de l'extension quadratique E correspondant à $\gamma=-1$ sont appelés nombres complexes (cf.chap.VI et Top.gén., chap.V).

2° γ est un carré $\mu^2\neq 0$; prenons alors comme nouvelle base de E les éléments $e_1=\frac{1}{2}+\frac{v}{2\mu}$, $e_2=\frac{1}{2}-\frac{v}{2\mu}$; on a $e_1^2=e_1$, $e_2^2=e_2$, $e_1e_2=e_2e_1=0$; E est donc composé direct des deux corps Ae_1 , Ae_2 isomorphes à A .

3° $\gamma=0$; l'ensemble $\mathfrak{n}=Av$ est alors un idéal dans E , tel que $\mathfrak{n}\cdot\mathfrak{n}=(0)$, et l'algèbre quotient $E/\mathfrak{n}$ est isomorphe au corps A .

Lorsque A est le corps des nombres réels R, les éléments de l'algèbre E sur R ayant pour base 1,v tels que $v^2=0$ sont appelés nombres duaux.

8. Exemples d'algèbres : III. Quaternions. Soit A un anneau commutatif ayant un élément unité, E une algèbre sur A ayant une base régulière de quatre éléments, dont le premier est élément unité de E , qu'on identifie avec l'élément unité 1 de A , et dont les trois autres notés j,k, ℓ , se multiplient d'après la table :

$$j^2=k^2=\ell^2=-1$$
$$jk=-kj=\ell$$
$$k\ell=-\ell k=j \qquad (14)$$
$$\ell j=-j\ell=k$$

On vérifie sans peine que cette table de multiplication satisfait aux conditions d'associativité ; l'algèbre E ainsi définie, qui est non commutative si A n'est pas de caractéristique 2 , est appelée l'algèbre des quaternions sur A . La base $(1,j,k,\ell)$ de E est appelée la base canonique de E .

L'algèbre des quaternions E est isomorphe à l'algèbre opposée E^0 sur A . Pour tout quaternion $x=a+bj+ck+d\ell$, désignons en effet par $\bar{x}$ le quaternion $a-bj-ck-d\ell$, qu'on appelle le quaternion conjugué de x ; l'application $x \to \bar{x}$ est évidemment une application linéaire biunivoque de E sur E^0 , et on a $\overline{jk} = \bar{\ell} = -\ell = +kj = \bar{k}.\bar{j}$, et on voit de même que $\overline{k\ell} = \bar{\ell}.\bar{k}$, $\overline{\ell j} = \bar{j}.\bar{\ell}$. Donc $x \to \bar{x}$ est un isomorphisme de E sur E^0 , qu'on peut aussi considérer comme un isomorphisme de E^0 sur E ; on dit aussi que c'est un antiautomorphisme de E , et en tant qu'application de E sur E , il est identique à son application réciproque. En outre, on a $x+\bar{x} = 2a \in A$, et $x\bar{x}=\bar{x}x=a^2+b^2+c^2+d^2 \in A$; le produit $x\bar{x}$ est aussi appelé la norme du quaternion x , et noté parfois $N(x)$.

Considérons en particulier le cas où A est un corps, dans lequel la relation $x^2+y^2+z^2+t^2=0$ entraîne $x=y=z=t=0$ (c'est ce qui a lieu par exemple dans le corps $\mathbb{Q}$ des nombres rationnels, ou le corps $\mathbb{R}$ des nombres réels ; voir chap.VI) ; alors l'algèbre des quaternions E sur A est un corps non commutatif, car les relations $x\bar{x}=\bar{x}x=N(x)\neq 0$ pour tout $x\neq 0$ dans E , montrent que x admet un inverse $x^{-1}=\frac{\bar{x}}{N(x)}$ dans E .

On notera que les éléments $a+bj$ (resp. $a+ck$, $a+d\ell$) de E forment alors un sous-corps commutatif, extension quadratique de A correspondant à $\alpha=0$, $\beta=-1$ dans (12) .

9. Exemples d'algèbres : IV. Algèbre d'un groupe. Soient A un anneau commutatif ayant un élément unité, S un monoïde (chap.I, § 1), que nous noterons multiplicativement. Considérons, dans le A-module $E=A^{(S)}$ somme directe d'une famille $(A_u)_{u\in S}$ de modules identiques à A, la base canonique (e_u) $(u\in S)$; on définit sur E une structure d'algèbre par rapport à A en prenant pour table de multiplication de la base (e_u)

(15) $$e_u e_v = e_{uv}$$

En effet, les conditions d'associativité sont satisfaites, car on a $(e_a e_b)e_c = e_{ab}e_c = e_{abc} = e_a(e_b e_c)$ d'après l'associativité de la multiplication dans S. L'algèbre ainsi définie est appelée l'algèbre du monoïde S relative à l'anneau A.

L'application $u \to e_u$ de S dans $A^{(S)}$ (muni de la multiplication seule) est évidemment un isomorphisme ; aussi identifie-t-on S avec la base canonique (e_u) ; autrement dit, tout élément de l'algèbre $A^{(S)}$ s'écrit d'une manière et d'une seule sous la forme $\sum_{s\in S} a_s.s$ $(a_s \in A)$. Si S est commutatif, il en est de même de l'algèbre $A^{(S)}$; si S admet un élément unité e, e est également élément unité de l'algèbre $A^{(S)}$. Si T est une partie stable du monoïde S, l'ensemble des éléments de $A^{(S)}$ de la forme $\sum_{s\in T} a_s.s$ est une sous-algèbre de $A^{(S)}$, isomorphe à l'algèbre $A^{(T)}$ du monoïde T, et qu'on identifie avec cette dernière.

Toute représentation f d'un monoïde S dans un monoïde S' peut être prolongée d'une manière et d'une seule en une représentation de l'algèbre $A^{(S)}$ dans l'algèbre $A^{(S')}$, en posant $f(\sum_{s\in S} a_s.s) = \sum_{s\in S} a_s f(s)$

Si maintenant g est une représentation de l'anneau A sur un anneau commutatif B, on définit une représentation h de la structure d'anneau (sans opérateur) de l'algèbre $A^{(S)}$ du monoïde S relative à l'anneau A, sur la structure d'anneau de l'algèbre $B^{(S)}$ du même monoïde S relative à l'anneau B, en posant $h(\sum_{s\in S} a_s.s) = \sum_{s\in S} g(a_s).s$.

Si S admet un élément unité, de sorte que A puisse être considéré comme sous-anneau de $A^{(S)}$, la représentation h est un <u>prolongement</u> de la représentation g .

Les algèbres de monoïdes les plus importantes sont les algèbres de <u>groupes</u> (relatives à un <u>corps</u>) ; nous les étudierons au chapitre VII.

<u>Exercices</u>.- 1) Soit K un corps de caractéristique 2 , E une extension quadratique de K , ayant pour base 1 et u , avec $u^2=\alpha u+\beta$. Montrer que, si l'équation $x^2-\alpha x-\beta=0$ n'a pas de racines dans K , E est un corps ; si elle a deux racines distinctes, E est composé direct de deux corps isomorphes à K ; enfin, si elle a une seule racine (ce qui n'est possible que pour $\alpha=0$), E est isomorphe à l'algèbre ayant pour base 1 et v , avec $v^2=0$.

2) Si A est un anneau commutatif ayant un élément unité, et de caractéristique $\neq 2$, le centre de l'algèbre des quaternions sur A est identique à A .

3) Soit K un corps commutatif, de caractéristique $\neq 2$, et dans lequel -1 est le carré d'un élément $i \in K$; montrer que l'algèbre des quaternions sur K est isomorphe à l'algèbre des matrices d'ordre 2 sur K (considérer la base équivalente à $(1,j,k,\ell)$ formée des éléments $\frac{1}{2}(1+ij)$, $\frac{1}{2}(1-ij)$, $\frac{1}{2}(k+i\ell)$, $\frac{1}{2}(k-i\ell)$) .

4) Soit A un anneau commutatif de caractéristique 2 , ayant un élément unité. Montrer que l'algèbre des quaternions sur A est commutative et possède une base $(1,e_1,e_2,e_3)$ telle que $e_1^2=e_2^2=e_3^2=0$, $e_1e_2=e_3$, $e_1e_3=e_2e_3=0$.

5) Soit K un corps commutatif de caractéristique $\neq 2$; soit E l'algèbre sur K ayant une base de quatre éléments $1,j,k,\ell$ (1 élément unité commun de K et E), avec la table de multiplication

$j^2=k^2=1$, $\ell^2=-1$, $jk=-kj=\ell$, $k\ell=-\ell k=-j$, $\ell j=-j\ell=-k$.

Montrer que E est isomorphe à l'algèbre des matrices d'ordre 2 sur K (considérer la nouvelle base $\frac{1}{2}(1+j)$, $\frac{1}{2}(1-j)$, $\frac{1}{2}(k+\ell)$, $\frac{1}{2}(k-\ell)$) .

6) Soit K un corps commutatif de caractéristique $\neq 2$: soit E l'algèbre sur K ayant une base de quatre éléments 1,j,k (1 élément unité commun de K et E), avec la table de multiplication

$j^2=k^2=\ell^2=1$, $jk=kj=\ell$, $k\ell=\ell k=j$, $\ell j=j\ell=k$.

Montrer que E est composé direct de quatre corps isomorphes à K (considérer la base de E formée des éléments $(1+\varepsilon j)(1+\varepsilon' k)$, où ε et ε' sont égaux à $+1$ ou -1) .

L'algèbre E est l'algèbre (relative à K) du produit de deux groupes cycliques d'ordre 2 . Généraliser à l'algèbre du groupe produit de n groupes cycliques d'ordre 2 .

7) Le <u>groupe quaternionique</u> Q (chap.I, § 6, exerc.20) est isomorphe au groupe des huit quaternions ± 1 , $\pm j$, $\pm k$, $\pm \ell$ dans une algèbre de quaternions sur un corps de caractéristique $\neq 2$. Montrer que l'algèbre E du groupe Q sur un corps K de caractéristique $\neq 2$ est composée directe de quatre corps isomorphes à K et de l'algèbre des quaternions sur K (si c est l'élément de Q qui correspond à -1 dans l'isomorphie précédente, les éléments de Q peuvent s'écrire $e,j,k,\ell,c,cj,ck,c\ell$; considérer la base de E formée des éléments $\frac{1}{2}(e+c)$, $\frac{1}{2}(e-c)$, $\frac{1}{2}(e-c)j$, $\frac{1}{2}(e+c)k$, $\frac{1}{2}(e-c)k$, $\frac{1}{2}(e+c)\ell$, $\frac{1}{2}(e-c)\ell$) .

8) Montrer que l'algèbre E du <u>groupe diédral</u> $\mathfrak{D}_8$ d'ordre 8 (chap.I, § 6, exerc.20) sur un corps commutatif K de caractéristique $\neq 2$, est composé direct de quatre corps isomorphes à K et de l'algèbre des matrices d'ordre 2 sur K (si a et b sont les deux

les deux générateurs de $\mathcal{D}_8$, les éléments de $\mathcal{D}_8$ sont de la forme $a^i b^j$ $(0 \leqslant i \leqslant 3$, $0 \leqslant j \leqslant 1)$; considérer la base de E formée des éléments $\frac{1}{2}(e+a^2)$, $\frac{1}{2}(e-a^2)$, $\frac{1}{2}(a+a^3)$, $\frac{1}{2}(a-a^3)$, et de ces quatre éléments multipliés à droite par b ; utiliser l'exerc.5).

Montrer de même que l'algèbre F du groupe diédral $\mathcal{D}_6$ d'ordre 6 sur un corps K de caractéristique $\neq 2$ et $\neq 3$, est composé direct de deux corps isomorphes à K et de l'algèbre de matrices d'ordre 2 sur K (considérer ici la base de E formée des éléments $e+a+a^2$, $a+a^2-2e$, $a-a^2$, et de ces trois éléments multipliés à droite par b)

9) Soit G un groupe, H un sous-groupe distingué de G. Montrer que l'algèbre de groupe $A^{(G/H)}$ du groupe quotient G/H relative à un anneau A , est isomorphe à l'algèbre quotient $A^{(G)}/\mathfrak{a}$, où $\mathfrak{a}$ est l'idéal bilatère de l'algèbre de groupe $A^{(G)}$, engendré par les éléments de la forme ts-s , où t parcourt H et s parcourt G

*10) Soit E la sous-algèbre de l'algèbre des matrices d'ordre n sur un anneau A (ayant un élément unité), formée des matrices (a_{ij}) telles que $a_{ij}=0$ pour $i<j$, et $a_{i+h,j+h} = a_{ij}$ pour tout couple d'indices tel que $i \geqslant j$, et tout entier h (tel que $i+h \leqslant n$ et $j+h \leqslant n$) . Montrer que E est isomorphe à l'algèbre quotient de l'algèbre $A[x]$ des polynomes d'une indéterminée sur A , par l'idéal principal (x^n) de $A[x]$. *