LIVRE II
ALGEBRE
CHAPITRE II (ETAT 5)
ALGEBRE LINEAIRE

Rédaction n° 038

Nombre de pages : 124

Nombre de feuilles : 124

Delsarte - Schwartz

A 38

LIVRE II

ALGEBRE

CHAPITRE II (Etat 5)

ALGEBRE LINEAIRE

Sommaire

LIVRE II

ALGEBRE

CHAPITRE II (Etat 5)

ALGEBRE LINEAIRE

§ 1. Modules.

1. Définition des modules.

DEFINITION 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 par la donnée :

1° d'une loi de groupe abélien dans E (notée additivement) ;

2° d'une loi de composition externe partout définie $(\alpha,x)\to\alpha\top x$ dont le domaine d'opérateurs est l'anneau A, et qui satisfait aux axiomes suivantes :

(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, n°1) de A, tout module à droite sur l'anneau A est un module à gauche sur l'anneau A^0.

Il en résulte qu'on peut exposer les propriétés des modules en se bornant systématiquement, soit aux modules à gauche, soit aux modules à droite, la remarque précédente permettant de traduire aussitôt tout résultat relatif aux uns en un résultat relatif aux autres ; sauf au § 6 (où, pour des raisons de commodité de notation, tous les modules que nous considérerons seront des modules à droite), nous n'étudierons en principe que les modules <u>à gauche</u>, et lorsque nous parlerons de <u>module</u> (sans préciser) il s'agira d'un module à gauche, dont la loi externe sera notée multiplicativement.

Lorsque l'anneau A est <u>commutatif</u>, il n'y a pas lieu de distinguer les notions de module à droite et de module à gauche par rapport à A .

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

L'axiome (M_{II}) signifie de même que cette loi externe est <u>distributive</u> par rapport à l'ensemble des deux lois additives dans A et dans E ; l'axiome (M_{III}) enfin, qu'elle est <u>associative</u> par rapport à la multiplication dans A (chap.I, § 5).

Au § 7, n° 9, nous verrons comment l'étude des groupes abéliens à opérateurs quelconques peut se ramener à celle des modules.

Les applications $x \to ax$ d'un module E dans lui-même s'appellent les <u>homothéties</u> de E (chap.I, § 6, n° 9) ; ce sont des endomorphismes de la structure de groupe abélien (<u>sans opérateur</u>) 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 par rapport à un anneau A , et si B est un <u>sous-anneau</u> quelconque de A , la loi de

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 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 $(n,x) \to n.x$ (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 $\mathcal{E}$ 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 $(f,x) \to f(x)$ entre opérateurs $f \in \mathcal{E}$ et éléments $x \in G$ définit sur G une structure de module à gauche par rapport à l'anneau $\mathcal{E}$.

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 $ax=0$ pour tout $a \in A$ et tout $x \in G$.

2. Modules unitaires. Espaces vectoriels.

DEFINITION 2. On dit qu'un A-module 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 $\varepsilon x = x$ pour tout $x \in E$) .

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_g et A_d sont unitaires ; les modules définis dans les exemples 2 et 3 du n°1 sont unitaires.

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

DEFINITION 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. Par abus de langage, on emploie aussi parfois cette terminologie pour des modules quelconques.

Exemples. 1) Un corps est à la fois espace vectoriel à gauche et à droite par rapport à un quelconque de ses sous-corps.

* 2) L'espace numérique à 3 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 et d'une telle fonction f étant la fonction numérique $x \longrightarrow tf(x)$. *

Dans un espace vectoriel E sur un corps K , toute homothétie $x \longrightarrow ax$ 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 $x = a^{-1}(ax) = a^{-1}y$.

3. Sous-modules et modules quotients.

Soit E un A-module ; 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 A-module de E , est une structure de A-module ; 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 espace vectoriel E est un espace vectoriel, qu'on appelle encore sous-espace vectoriel de E (ou simplement sous-espace de E , si aucune confusion n'en résulte).

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

2) Soit A un anneau. Les sous-modules de A_s (resp. A_d) ne sont autres que les idéaux à gauche (resp. idéaux à droite) de l'anneau A .

3) Soit E un A-module, 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 $\mathbb{Z}$ (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 , telle que $ax = 0$ quels que soient $a \in A$ et $x \in G$.

Remarque. 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 sous-module B_s du B-module A_s n'est pas un A-module si $B \neq A$.

Soit E un A-module. Toute relation d'équivalence <u>compatible</u> (chap.I, § 4, n° 3) avec la structure de A-module de E est de la forme $x-y \in M$, où M est un sous-groupe stable de E (chap.I, § 6, n°11), c'est-à-dire un <u>sous-module</u> 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, n°11) est une structure de A-module ; muni de cette structure, E/M est appelé <u>module quotient</u> 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 a fortiori toute classe mod.M . En particulier, tout module quotient d'un <u>espace vectoriel</u> E est un espace vectoriel, module quotient d'un <u>espace vectoriel</u> E est un espace vectoriel, qu'on appelle <u>espace vectoriel quotient</u> de E .

<u>Exemple</u>. Tout idéal à gauche $\mathfrak{a}$ dans un anneau A définit un module quotient $A_s/\mathfrak{a}$ du A-module A_s ; ce module quotient se note souvent, pour abréger, $A/\mathfrak{a}$, mais, lorsque $\mathfrak{a}$ est un idéal <u>bilatère</u>, il faut se garder de confondre la structure d'<u>anneau quotient</u> 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. <u>Soit M un sous-module d'un module E , f l'application canonique de E sur le module quotient E/M = E'</u> .

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 $(E/M)/(N/M)$.

4. Produit de modules.

Soit $(E_\iota)_{\iota \in I}$ une famille de modules sur un même anneau A. On vérifie immédiatement que, sur l'ensemble produit $E = \prod_{\iota \in I} E_\iota$, le produit des structures de module des E_ι (chap.I, § 4, n°5) est une structure de A-module. 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, la partie $M = \prod_{\iota \in I} M_\iota$ est un sous-module de 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 réduit à un seul indice $\varkappa$, le sous-module E'_J se note encore $E'_\varkappa$, et s'appelle le sous-module composant d'indice $\varkappa$ de E ; il est isomorphe à $E_\varkappa$, auquel on l'identifie souvent.

De même, si N est un sous-module quelconque de E, le sous-module N'_ι de E'_ι, formé des éléments dont les coordonnées d'indice $\neq \varkappa$ sont

sont nulles, et la coordonnée d'indice ι égale à $pr_\iota x$, où x parcourt M, est appelé le module <u>composant</u> d'indice ι de M ; il est isomorphe à la <u>projection</u> de M sur E_ι, avec laquelle on l'identifie souvent.

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

Un exemple important de produit de modules est celui où tous les modules facteurs E_ι sont identiques au module A_s ; on le désigne par la notation A_s^I, ou simplement A^I quand aucune confusion n'est à craindre ; les éléments de ce module sont les <u>applications de</u> I <u>dans</u> A.

<u>5. Annulateurs</u>.

DEFINITION 4. <u>On appelle annulateur d'une partie</u> F <u>d'un</u> A-<u>module</u> E, <u>l'ensemble des éléments</u> $a \in A$ <u>tels que</u> $ax=0$ <u>pour tout</u> $x \in F$.

Si deux parties F, G de E sont telles que $F \subset G$, l'annulateur de G est contenu dans celui de F. Si (F_ι) est une famille de parties de E, l'annulateur de la réunion $\bigcup_\iota F_\iota$ est l'intersection des annulateurs des F_ι. En particulier, l'annulateur d'une partie F est l'intersection des annulateurs des éléments de F.

Il est immédiat que l'annulateur d'une partie quelconque F de E est un <u>idéal à gauche</u> de A. L'annulateur d'un <u>sous-module</u> M de E est un <u>idéal bilatère</u> de A : en effet, si $ax=0$ pour tout $x \in M$, on a aussi $a(\beta x)=0$ pour tout $x \in M$ et tout $\beta \in A$, donc $a\beta$ appartient à l'annulateur de M pour tout $\beta \in A$. En particulier l'annulateur $\mathfrak{a}$ du module E est un idéal bilatère de A.

Pour tout $a \in A$, désignons par u_a l'homothétie $x \longrightarrow ax$ produite par l'opérateur a ; considérons l'application $a \longrightarrow u_a$ de A dans l'anneau

des endomorphismes $\mathscr{E}$ du groupe abélien (sans opérateur) E ; les axiomes (M_{II}) et (M_{III}) montrent que cette application est une <u>représentation</u> de l'anneau A dans l'anneau $\mathscr{E}$; l'image réciproque de 0 , dans cette représentation, est précisément l'<u>annulateur</u> $\mathfrak{a}$ de E ; donc l'image de A par l'application $\alpha \longrightarrow u_\alpha$, est isomorphe à l'anneau quotient $A/\mathfrak{a}$.

On dit que le module E est <u>normal</u> si son annulateur $\mathfrak{a}$ est <u>nul</u>. Si E n'est pas normal, et si $\dot{\alpha}$ est un élément quelconque de l'anneau quotient $A/\mathfrak{a}$, pour un $x \in E$ quelconque, l'élément αx est le même pour tous les $\alpha \in \dot{\alpha}$; si on le désigne par $\dot{\alpha}x$, on voit aussitôt que l'application $(\dot{\alpha},x) \longrightarrow \dot{\alpha}x$ définit sur E une structure de module <u>normal</u> par rapport à l'anneau quotient $A/\mathfrak{a}$; muni de cette structure, on dit que E est le <u>module normal associé</u> au A-module E . On observera que tout sous-module d'un A-module E est aussi un sous-module du module normal associé, et réciproquement.

6. Combinaisons linéaires. Modules monogènes.

Soit I un ensemble d'indices quelconque, $(x_\iota)_{\iota \in I}$ une famille d'éléments d'un A-module E , pour laquelle l'ensemble J des indices ι tels que $x_\iota \neq 0$ soit <u>fini</u> ; on convient de désigner par $\sum_{\iota \in I} x_\iota$ et d'appeler <u>somme</u> de la famille $(x_\iota)_{\iota \in I}$ la somme $\sum_{\iota \in J} x_\iota$. On peut encore dire que la somme de la famille $(x_\iota)_{\iota \in I}$ est la valeur commune des sommes $\sum_{\iota \in H} x_\iota$ pour toute partie finie H de I telle que $x_\iota = 0$ pour $\iota \in \complement H$; lorsque I est fini, on retrouve bien la notion de somme d'une famille finie (définie au chap.I).

Bien entendu, la notation $\sum_{\iota \in I} x_\iota$ n'a pas de sens pour une famille $(x_\iota)_{\iota \in I}$ telle que $x_\iota \neq 0$ 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 chapitre, nous emploierons cette notation, il sera toujours sous-entendu, sauf mention expresse du contraire, que $x_\iota = 0$ sauf pour un nombre fini d'indices.

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) $$a . \sum_{\iota \in I} x_\iota = \sum_{\iota \in I} a x_\iota \qquad \text{pour } a \in A .$$

DEFINITION 5. On dit qu'un élément x d'un A-module E est une combinaison linéaire, à coefficients dans A, d'une famille $(a_\iota)_{\iota \in I}$ d'éléments de E, s'il existe une famille $(\lambda_\iota)_{\iota \in I}$ d'éléments de A, telle que $\lambda_\iota = 0$ sauf pour un nombre fini d'indices, et que l'on ait $x = \sum_{\iota \in I} \lambda_\iota a_\iota$. Toute famille $(\lambda_\iota)_{\iota \in I}$ ayant ces propriétés est appelée famille de coefficients de la combinaison linéaire x (relativement à la famille (a_ι)).

En général, il existe plusieurs familles de coefficients distinctes satisfaisant à la relation $x = \sum_\iota \lambda_\iota a_\iota$ (voir n° 8).

On notera que 0 est combinaison linéaire de la famille vide d'éléments de E (d'après la convention du chap.I, § 2, n° 1).

PROPOSITION 2. Dans un A-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).

En effet, tout sous-module de E contenant tous les a_ι contient les combinaisons linéaires des a_ι ; inversement, les formules (1) et (2) prouvent que l'ensemble des combinaisons linéaires des a_ι est un sous-module M de E ; comme $a_\iota = \varepsilon a$ (ε élément unité de A), M contient tous les a_ι, donc est le plus petit sous-module de E contenant les a_ι.

DEFINITION 6. On dit qu'un module est monogène s'il est engendré par un seul élément.

La prop.2 montre que si E est un A-module monogène unitaire, il est identique à l'ensemble A.a des éléments λa, où λ parcourt A, pour tout élément a engendrant E.

Exemples. 1)Tout groupe monogène étant abélien, est un $\mathbb{Z}$-module monogène.

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

Si E est un A-module monogène unitaire, a un élément engendrant E, l'application $\lambda \longrightarrow \lambda a$ est une représentation du A-module A_g sur E, en vertu des axiomes (M_{II}) et (M_{III}) ; l'image réciproque de 0 par cette représentation est l'annulateur $\mathfrak{a}$ de a ; donc E est isomorphe au module quotient $A_g/\mathfrak{a}$. Réciproquement, si A est un anneau ayant un élément unité ε, et $\mathfrak{a}$ un idéal à gauche quelconque de A, le module quotient $A_g/\mathfrak{a}$ est un module monogène engendré par la classe $\dot{\varepsilon} = \varepsilon + \mathfrak{a}$ de ε, car la classe $\dot{\mu} = \mu + \mathfrak{a}$ d'un élément quelconque $\mu \in A$ peut s'écrire $\mu\dot{\varepsilon}$. Ainsi :

PROPOSITION 3. Soit A un anneau ayant un élément unité. Tout A-module monogène unitaire est isomorphe à un module quotient $A_g/\mathfrak{a}$, où $\mathfrak{a}$ est un idéal à gauche quelconque de A ; réciproquement, tout module quotient de A_g est un module monogène unitaire.

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 $\mathfrak{b} \supset \mathfrak{a}$; tout module quotient de E est isomorphe à un module quotient $A/\mathfrak{b}$, donc est lui-même monogène.

Il ne faudrait pas croire par contre 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 lesquels il existe des idéaux non principaux

7. Somme et somme directe de sous-modules.

PROPOSITION 4. Le sous-module engendré par la réunion d'une famille $(M_\iota)_{\iota\in I}$ de sous-modules d'un module E, 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 $x_\iota = 0$ sauf pour un nombre fini d'indices et $x_\iota \in M_\iota$ pour tout $\iota \in I$.

En effet, tout sous-module de E contenant la réunion $\bigcup_{\iota\in I} M_\iota$ contient toutes ces sommes, et d'autre part, les formules (1) et (2) montrent que l'ensemble de ces sommes est un sous-module de E.

Lorsque I est fini, le sous-module engendré par la réunion des M_ι n'est autre que leur somme $\sum_{\iota\in I} M_\iota$ (chap.I, § 1). Par extension, on pose la définition suivante :

DEFINITION 7. 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 de E engendré par la réunion de cette famille.

DEFINITION 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 $\sum_{\iota\in I} x_\iota$ (avec $x_\iota \in M_\iota$ pour tout ι, et $x_\iota = 0$ sauf pour un nombre fini d'indices).

La déf.8 généralise la définition de la somme directe déjà donnée au chap.I, § 6, n°6, lorsque I est fini. Elle signifie que la relation $\sum_{\iota\in I} x_\iota = \sum_{\iota\in I} y_\iota$, où $x_\iota \in M_\iota$, $y_\iota \in M_\iota$ pour tout ι, entraîne $x_\iota = y_\iota$ pour tout ι, ou encore (en vertu de (1), et du fait que les M_ι sont

sont des sous-modules) que la relation $\prod_{\iota \in I} z_\iota = 0$, où $z_\iota \in M_\iota$ pour tout ι , entraîne $z_\iota = 0$ pour tout ι .

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 d'indice $\iota \neq \varkappa$ se réduise à 0 .

La condition est évidemment nécessaire ; 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 $x_\iota \in M_\iota$ pour tout ι et $x = \sum_\iota x_\iota$; 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 $a \in A$

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

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

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.8 entraîne donc (3) quel que soit ι . Démonstration analogue pour (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 composant de N dans M_ι .

Etant donnée une famille quelconque $(M_\iota)_{\iota \in I}$ de A-modules, on peut définir un A-module qui est somme directe d'une famille de sous-modules respectivement isomorphes aux M_ι ; il suffit de prendre, dans le module produit $\prod_{\iota \in I} M_\iota$, le module M' , somme des modules composants M'_ι (n°4), cette somme étant évidemment directe ; par abus de langage, on dira

(lorsqu'aucune confusion n'en peut résulter) que M' est la somme directe de la famille $(M_\iota)_{\iota \in I}$; si I est fini, M' est identique au module produit $\prod_{\iota \in I} M_\iota$. Lorsque tous les M_ι sont identiques à un même module M , leur somme directe se note $M^{(I)}$.

PROPOSITION 7. Soit (M_ι) une famille de sous-modules d'un module E ; le sous-module N de E , somme des M_ι , est isomorphe à un module quotient du module M , somme directe de la famille (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 N , on définit une représentation de M sur N en vertu des formules (1) et (2), d'où la proposition.

DEFINITION 9. 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 M_2 .

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 $M_1 \cap M_2 = \{0\}$.

PROPOSITION 8. Si M_1 et M_2 sont deux sous-modules supplémentaires dans un module E , l'application qui, à tout $x \in M_2$, fait correspondre sa classe mod. M_1 , est un isomorphisme de M_2 sur E/M_1 .

En effet, cette application est une représentation de M_2 dans E/M_1 , puisque c'est la restriction à M_2 de l'application canonique de E sur E/M_1 . Elle applique M_2 sur E/M_1 , puisque tout élément de E est congru (mod.M_1) à un élément de M_2 ; enfin elle est biunivoque puisque $M_1 \cap M_2 = \{0\}$.

L'isomorphisme défini dans la prop.8 et l'isomorphisme réciproque sont dits canoniques.

COROLLAIRE. Si M_2 et M_3 sont deux sous-modules supplémentaires d'un même sous-module M_1, l'application qui, à tout $x \in M_2$, fait correspondre son composant dans M_3 (relatif à la décomposition de E en somme directe de M_1 et M_3) est un isomorphisme de M_2 sur M_3.

Cet isomorphisme et son réciproque sont encore dits canoniques.

Si un module E est somme directe d'une famille $(M_\iota)_{\iota \in I}$ de sous-modules et si (J_1, J_2) est une partition de I, les sous-modules $N_1 = \sum_{\iota \in J_1} M_\iota$ et $N_2 = \sum_{\iota \in J_2} M_\iota$ (où les sommes sont directes, d'après la prop.5) sont supplémentaires.

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 somme directe 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 sous-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 aussi somme directe de la famille $(M_\iota)_{\iota \in I}$.

8. Familles libres. Bases.

DEFINITION 10. Dans un A-module unitaire E, on dit qu'une famille $(a_\iota)_{\iota \in I}$ d'éléments de E est libre si la relation $\sum_{\iota \in I} \lambda_\iota a_\iota = 0$ (où $\lambda_\iota = 0$ sauf pour un nombre fini d'indices) entraîne $\lambda_\iota = 0$ pour tout ι.

Deux éléments d'indices distincts d'une famille libre (a_ι) sont distincts ; car si $a_\alpha = a_\beta$ pour $\alpha \neq \beta$, on a la relation $\sum_\iota \lambda_\iota a_\iota = 0$ avec $\lambda_\alpha = \varepsilon$, $\lambda_\beta = -\varepsilon$ (ε élément unité de A) et $\lambda_\iota = 0$ pour les autres indices. Il nous sera commode, dans ce qui suit, de considérer une partie quelconque S d'un module E comme ensemble d'éléments d'une famille définie par une application biunivoque d'un ensemble d'indices sur S (par exemple l'application identique de S sur lui-même) ; on dira que S est une partie libre (ou un système libre) dans E si une

une quelconque des familles correspondantes est libre (auquel cas toutes le sont). Les éléments d'une partie libre de E sont encore dits linéairement indépendants. Si une partie de E n'est pas libre, on dit encore qu'elle est liée (ou est un système lié) et que ses éléments sont linéairement dépendants.

PROPOSITION 9. Pour qu'une partie S d'un module E soit libre, il faut et il suffit que toute partie finie de S soit libre.

La démonstration est immédiate à partir de la déf.10 et de la définition de la somme d'une famille infinie dans E .

En particulier la partie vide de E est libre ; toute partie réduite à un élément x d'une partie libre est libre : on dit que x est un élément libre de E si $\{x\}$ est une partie libre, c'est-à-dire si la relation $ax=0$ entraîne $a=0$. Il revient au même de poser la définition suivante :

DEFINITION 11. On dit qu'un élément x d'un A-module E est libre si son annulateur est nul.

Si x est un élément libre d'un A-module unitaire E , le sous-module A.x engendré par x est donc isomorphe à A_s .

Dans le A-module à gauche A_s , les éléments libres sont les éléments $\xi \in A$ qui ne sont pas diviseurs de zéro à droite. En particulier, l'élément unité de A (quand il existe) est libre.

La notion d'élément libre permet de caractériser les familles libres d'éléments d'un A-module unitaire E de la façon suivante : pour qu'une famille $(a_\iota)_{\iota \in I}$ soit libre, il faut et il suffit que chacun des éléments a_ι soit libre, et que la somme des sous-modules monogènes Aa_ι (respectivement engendrés par les a_ι) soit directe.

D'après la déf.10, si (a_ι) est une famille libre, aucun élément $a_\varkappa$ ne peut être combinaison linéaire des a_ι d'indice $\neq \varkappa$. Mais inversement, une famille (a_ι) qui remplit cette condition n'est pas nécessairement une famille libre (cf. § 3, n°1).

Par exemple, soit A un anneau d'intégrité ayant un élément unité ; soient a et b deux éléments distincts et $\neq 0$ de A , considéré comme A-module ; on a $(-b)a+ab=0$, 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 $a=xb$.

DEFINITION 12. On appelle base d'un module unitaire E toute partie libre de E qui engendre E .

Toute partie libre d'un module unitaire E est donc une base du sous-module de E qu'elle engendre.

En particulier, la partie vide de E est une base du sous-module $\{0\}$.

Soit $(a_\lambda)_{\lambda \in L}$ une base d'un A-module unitaire E . D'après la prop2 , tout $x \in E$ est combinaison linéaire des a_λ , donc $x = \sum_{\lambda \in L} \xi_\lambda a_\lambda$; en outre, les ξ_λ sont déterminés de façon unique, car la relation $\sum_\lambda \xi_\lambda a_\lambda = \sum_\lambda \xi'_\lambda a_\lambda$ s'écrit $\sum_\lambda (\xi_\lambda - \xi'_\lambda) a_\lambda = 0$, d'où $\xi_\lambda = \xi'_\lambda$ pour tout λ puisque (a_λ) est une famille libre ; l'élément ξ_λ s'appelle la composante d'indice λ (ou, par abus de langage, la coordonnée d'indice λ) de x par rapport à la base (a_λ).

En particulier, si E est un A-module unitaire monogène, dont l'élément a forme une base, tout $x \in E$ s'écrit d'une seule manière sous la forme $x = \xi a$; par abus de langage, on écrit parfois cette relation sous la forme $\xi = \frac{x}{a}$ lorsque l'anneau A est commutatif.

PROPOSITION 10. Pour qu'un A-module unitaire E possède une base, il faut et il suffit qu'il soit isomorphe à un module de la forme $A_g^{(L)}$ (L ensemble quelconque).

En effet, si $(a_\lambda)_{\lambda \in L}$ est une base de E , l'application qui, à tout $x \in E$ fait correspondre la famille $(\xi_\lambda)_{\lambda \in L}$ de ses composantes par rapport à (a_λ), est un isomorphisme de E sur $A_s^{(L)}$.

Inversement, si, pour tout $\lambda \in L$, on désigne par e_λ l'élément de $A_s^{(L)}$ dont tous les composants sont nuls, à l'exception de celui d'indice λ , qui est égal à l'élément unité ε de A , les e_λ forment une base du module $A_s^{(L)}$, appelée <u>base canonique</u> de ce module.

<u>Remarque</u>. Un module unitaire n'admet pas nécessairement de base. Par exemple, dans un anneau d'intégrité ayant un élément unité, et considéré comme A-module, nous avons vu ci-dessus qu'il n'existe aucune partie libre ayant plus d'un élément ; un idéal <u>non principal</u> de A ne peut donc avoir de base ; or, nous rencontrerons plus tard des anneaux d'intégrité dans lesquels il existe des idéaux non principaux.

Si un module unitaire E est somme directe d'une famille $(M_\iota)_{\iota \in I}$ de sous-modules, et si chacun des M_ι admet une base B_ι , la réunion des B_ι est une base de E .

PROPOSITION 11. <u>Soit M_1 un sous-module d'un module unitaire E , tel que le module quotient E/M_1 admette une base $(\dot{a}_\iota)_{\iota \in I}$. Si a_ι est un élément quelconque de la classe $\dot{a}_\iota$ (mod.M_1) , la famille $(a_\iota)_{\iota \in I}$ est libre et engendre un sous-module M_2 supplémentaire de M_1</u> .

En effet, la relation $\sum_\iota \lambda_\iota \dot{a}_\iota = 0$ entraîne $\lambda_\iota = 0$ pour tout ι par hypothèse ; comme elle équivaut à $\sum_\iota \lambda_\iota a_\iota \in M_1$, on voit d'une part que (a_ι) est une famille libre, et d'autre part que le sous-module M_2 engendré par cette famille est tel que $M_1 \cap M_2 = \{0\}$. Enfin, comme tout élément de E/M_1 est combinaison linéaire des $\dot{a}_\iota$, tout $x \in E$ est congru (mod.M_1) à une combinaison linéaire des a_ι , ce qui prouve que $E = M_1 + M_2$.

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 considérée 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 A admet un élément unité ε, 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 de 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 $\mathfrak{n}$ leur 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) Si un A-module unitaire E admet une base, l'annulateur de tout élément de E ne contient que des diviseurs à gauche de 0 dans A .

7) Si un A-module unitaire E admet une suite de Jordan-Hölder de longueur n (chap.I, § 6, n°14), 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) Soit E un A-module, somme directe d'une famille infinie

$(M_\iota)_{\iota \in I}$ de sous-modules (non réduits à 0). Montrer que tout système de générateurs de E a une puissance au moins égale à celle de I (soit S un système de générateurs de E ; remarquer que l'ensemble des indices ι tels que le composant d'indice ι d'un élément au moins de S soit $\neq 0$, a une puissance au plus égale à celle de S ; en déduire que, si S avait une puissance strictement inférieure à celle de I il existerait un $M_\varkappa$ qui serait contenu dans la somme des M_ι d'indice $\neq \varkappa$). En déduire que si E est somme directe d'une famille $(M_\iota)_{\iota \in I}$ de sous-modules monogènes et somme directe d'une autre famille $(N_\varkappa)_{\varkappa \in K}$ de sous-modules monogènes, I et K sont équipotents.

9) Montrer que tout A-module unitaire admettant une base dont I est l'ensemble d'indices, est équipotent à $A \times I$ si l'un au moins des ensembles A,I est infini.

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

11) Soit A un anneau sans diviseur de 0 et admettant 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 (utiliser l'exerc. 10 ci-dessus, et l'exerc.9 du chap.I, § 9).

12) Soit M un module <u>simple</u> (chap.I, § 6,déf.14) 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, <u>ou bien</u> pour tout $a \neq 0$ appartenant à M, on a $M = A.a$ (remarquer que, pour tout $x \in M$, on a $A.x \subset M$, et considérer le sous-module de M formé des $x \in M$ tels que $A.x = \{0\}$). 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 $A/\mathfrak{a}$.

§ 2. Applications linéaires.

1. Fonctions linéaires.

DEFINITION 1. Soient E et F deux modules par rapport au même anneau A . On appelle application linéaire de E dans F toute représentation (chap.I, § 4,n°4) de E dans F (*)

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 Z (§ 1,n°1), toute représentation u du groupe E (sans opérateur) dans le groupe F (sans opérateur) est aussi une application linéaire de E dans F , la relation $u(n.x)=n.u(x)$ 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 A-module, a un élément de E ; l'application $\lambda \to \lambda a$ du A-module A_s dans E est une application linéaire θ_a ; si E est un module unitaire, on a $\theta_a(\varepsilon)=a$ (ε élément unité de A) .

Toutes les propriétés des représentations des groupes à opérateurs (chap.I, § 6,n°s 12 et 13) sont valables pour les applications linéaires ; nous les rappellerons brièvement :

(*) Au chap.IX, les termes "application linéaire" recevront une acception plus large, une représentation de E dans F s'appelant application linéaire-homogène ; aucune confusion n'étant à craindre jusque là, nous omettrons le qualificatif "homogène" dans les chapitres antérieurs au chap.IX .

Pour qu'une application d'un module E dans un module F soit un <u>isomorphisme</u> de E dans F , il faut et il suffit que ce soit une application linéaire <u>biunivoque</u> 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'une 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 <u>restriction</u> de u à M est un <u>isomorphisme</u> de M sur u(M) .

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

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 A-modules, u une application linéaire de E dans F , v une application linéaire de F dans G , la <u>composée</u> v u est une application linéaire de E dans G .

Nous désignerons par $\mathcal{L}(E,F)$ 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 sous-groupe additif du module produit F^E (ensemble des applications de E dans F) ; par contre, si A n'est pas commutatif, $w=au$ n'est pas en général une application linéaire 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 $x \in E$ et tout $\lambda \in A$ que si a appartient au centre C de A . En d'autres termes, on ne peut munir $\mathscr{L}(E,F)$ que d'une structure de module par rapport à C (et non par rapport à A).

2. Applications linéaires d'un module quotient.

Soient E un A-module, H un sous-module de E , φ l'homomorphisme 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 qui s'annule pour tout $x \in H$, 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,n°7) 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 1. Soient E et F deux A-modules, H un sous-module de E , φ l'homomorphisme canonique de E sur E/H . Si, à toute application linéaire f de E/H dans F , on fait correspondre l'application linéaire $f \circ \varphi$ de E dans F , on définit un isomorphisme du module $\mathscr{L}(E/H,F)$ (par rapport au centre C de A) sur le sous-module de $\mathscr{L}(E,F)$ formé des applications linéaires de E dans F qui s'annulent dans H .

Cet isomorphisme et son isomorphisme réciproque sont dits canoniques.

3. Applications linéaires dans une somme directe.

Soient E un A-module, F un A-module somme directe d'une famille finie $(N_j)_{1 \leqslant j \leqslant m}$ de sous-modules ; pour tout $y \in F$, désignons par $k_j(y)$ le composant de y dans N_j $(1 \leqslant j \leqslant m)$. Soit u une application linéaire de E dans F ; pour tout $x \in E$, on a $u(x) = \sum_{j=1}^{m} k_j(u(x))$, c'est-à-dire $u = \sum_{j=1}^{m} k_j \circ u$; autrement dit, l'application linéaire u est bien déterminée par la connaissance des applications linéaires $u_j = k_j \circ u$ de E dans N_j $(1 \leqslant j \leqslant m)$. Réciproquement si, pour chaque indice j, u_j est une application linéaire quelconque de E dans N_j, $u = \sum_{j=1}^{m} u_j$ est une application linéaire de E dans F, telle que $u_j = k_j \circ u$. En résumé :

PROPOSITION 2. Si F est somme directe d'une famille finie (N_j) de sous-modules, le module $\mathscr{L}(E,F)$ est somme directe des sous-modules $\mathscr{L}(E, N_j)$.

4. Applications linéaires d'une somme directe.

Soient maintenant E un A-module, somme directe d'une famille quelconque (M_λ) de sous-modules, et F un A-module quelconque. Pour tout $x \in E$, désignons pas $h_\lambda(x)$ le composant de x dans M_λ ; on a donc $x = \sum_\lambda h_\lambda(x)$. Si u est une application linéaire de E dans F, on a $u(x) = u(\sum_\lambda h_\lambda(x)) = \sum_\lambda u(h_\lambda(x)) = \sum_\lambda u_\lambda(h_\lambda(x))$, 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 chaque 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 A-modules, 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 1. Le module $\mathscr{L}(E,F)$ est isomorphe au module produit $\prod_\lambda \mathscr{L}(M_\lambda, F)$.

COROLLAIRE 2. Si E admet une base (a_λ), pour toute famille (b_λ) d'éléments 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.

Cette application est définie par $u(\sum_\lambda \xi_\lambda a_\lambda) = \sum_\lambda \xi_\lambda b_\lambda$.

Pour que u soit un isomorphisme de E dans F, il faut et il suffit que la famille (b_λ) soit libre.

Supposons maintenant que E soit somme directe d'une famille finie $(M_i)_{1 \leqslant i \leqslant n}$ de sous-modules, et F somme directe d'une famille finie $(N_j)_{1 \leqslant j \leqslant m}$ de sous-modules. Alors les prop.2 et 3 montrent que le module $\mathscr{L}(E,F)$ est isomorphe au produit des mn modules $\mathscr{L}(M_i,N_j)$. De façon précise, toute application linéaire u de E dans F est déterminée par ses n restrictions u_i aux M_i, et chacune des u_i est déterminée par les m applications $k_j \circ u_i = u_{ji}$, en vertu de la formule $u_i(x) = \sum_{j=1}^{m} u_{ji}(x)$; u_{ji} est une application linéaire de M_i dans N_j, et ces mn applications peuvent être prises arbitrairement.

Soit G un troisième A-module, somme directe d'une famille $(P_k)_{1 \leqslant k \leqslant p}$ de sous-modules, et soit v une application linéaire de F dans G, (v_{kj}) la famille de mp applications linéaires qui lui correspond (v_{kj} étant une application de N_j dans P_k). Pour tout $x \in M_i$, on a

$$v(u_i(x)) = \sum_{j=1}^{m} v(u_{ji}(x)) = \sum_{k=1}^{p} \sum_{j=1}^{m} v_{kj}(u_{ji}(x))$$

Si on pose

$$w_{ki} = \sum_{j=1}^{m} v_{kj} \circ u_{ji} \qquad (1)$$

on voit que la famille des np applications linéaires w_{ki} correspond à l'application linéaire composée $w = v \circ u$ de E dans G .

5. Endomorphismes d'un module.

Soit E un A-module ; conformément aux définitions générales (chap.I, § 4, n°4), un endomorphisme de E est une application linéaire de E dans E ; l'ensemble de ces endomorphismes est donc l'ensemble que nous avons noté $\mathcal{L}(E,E)$; nous l'écrirons désormais $\mathcal{L}(E)$ 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 $(\gamma, u) \longrightarrow \gamma u$ entre opérateurs γ appartenant au centre C de A , et endomorphismes u de E , définit sur $\mathcal{L}(E)$ une structure d'anneau à opérateurs (chap.I, § 8, n°2), 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 $\mathcal{L}(E)$ (sans opérateur) est un sous-anneau de l'anneau $\mathfrak{E}$ des endomorphismes du groupe additif (sans opérateur); ~~qui peut être défini comme forme~~ il le compose des éléments de $\mathfrak{E}$ permutables avec les homothéties du module E (chap.I, § 8, cor.2 de la prop.2). On a déjà remarqué qu'en général une homothétie de E n'est pas un endomorphisme de la structure de module de E , lorsque l'anneau A n'est pas commutatif. (chap. I. § 6. n° 12).

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

6. Applications semi-linéaires.

Soient A et B deux anneaux isomorphes, $\lambda \to \lambda^\sigma$ un isomorphisme de A sur B . Soit E un A-module, F un B-module ; on dit qu'une application u de E dans F est une application semi-linéaire relative à l'isomorphisme σ si elle vérifie les identités $u(x+y)=u(x)+u(y)$, $u(\lambda x) = \lambda^\sigma u(x)$.

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 est l'anneau opposé A^0 de A.

Exemples.- 1) Si $\lambda \to \lambda^\sigma$ est un automorphisme d'un corps K , l'application qui, à tout élément (ξ_i) de l'espace vectoriel K_s^n , fait correspondre l'élément (ξ_i^σ) , est une application semi-linéaire relative à σ , de K_s^n sur lui-même.

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

Une application semi-linéaire biunivoque u de E sur F constitue, avec l'isomorphisme σ , un di-isomorphisme de E sur F (chap.I, § 4, n°1) ; par abus de langage, on dit que u est lui-même un di-isomorphisme relatif à σ .

On peut définir sur F une structure de A-module, en posant, pour tout $\lambda \in A$ et tout $y \in F$, $\lambda y = \lambda^\sigma y$, la loi de groupe additif sur F restant inchangée (la vérification des axiomes des modules est immédiate) ; désignons par F_σ le A-module ainsi défini. L'application identique φ de F_σ sur F est un di-isomorphisme de F_σ sur F (relatif à σ) ; il est immédiat que l'image par φ de tout sous-module

de F_σ est un sous-module de F et réciproquement ; en outre, on déduit de φ par passage aux quotients, un id-isomorphisme de tout module quotient F_σ/M sur le module quotient $F/\varphi(M)$.

Cela étant, toute application semi-linéaire u de E dans F peut s'écrire d'une seule manière $u = \varphi \circ v$, où v est une application linéaire de E dans le A-module F_σ . A toute propriété des applications linéaires correspond donc une propriété des applications semi-linéaires ; nous laisserons au lecteur le soin d'énoncer ces dernières.

Notons enfin que si E,F,G sont trois modules par rapport à trois anneaux isomorphes A,B,C respectivement, u une application semi-linéaire de E dans F , relative à un isomorphisme σ de A sur B , v une application semi-linéaire de F dans G , relative à un isomorphisme τ de B sur C , l'application composée v u est une application semi-linéaire de E dans G , relative à l'isomorphisme $\tau \circ \sigma$ de A sur C .

Exercices.- 1) Soit E un A-module, $F = \prod_{\iota \in I} F_\iota$ un produit de A-modules F_ι ; montrer que $\mathcal{L}(E,F)$ est isomorphe au produit $\prod_{\iota \in I} \mathcal{L}(E,F_\iota)$.

2) Soient E et F deux A-modules monogènes unitaires, a et b deux éléments engendrant respectivement E et F , $\mathfrak{a}$ et $\mathfrak{b}$ les annulateurs de a et b respectivement. Si Γ 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 $\mathcal{L}(E,F)$ des applications linéaires de E dans F est isomorphe au groupe quotient $\Gamma/\mathfrak{b}$.

3) Soient E et F deux A-modules, 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 automorphisme de $E \times F$. En déduire que, s'il existe une application linéaire v de F dans E , et un élément $a \in E$ tels que $v(u(a))=a$, il existe un automorphisme

w de $E \times F$ tel que $w(a,0)=(0,u(a))$.

4) Soit E un A-module unitaire admettant une base (a_λ). Montrer que le centre Z(E) du groupe des automorphismes GL(E) de E est formé des homothéties $x \longrightarrow \gamma x$, où γ parcourt le groupe des éléments inversibles du centre de A (écrire qu'un automorphisme $f \in Z(E)$ est permutable avec tout automorphisme u laissant invariant a_λ , et en déduire que $f(a_\lambda)=a_\lambda a_\lambda$). Montrer de même que le centre de l'anneau $\mathcal{L}(E)$ des endomorphismes de E est formé des homothéties $x \longrightarrow \gamma x$, où γ parcourt le centre de A .

5) a) Si u est un isomorphisme d'un A-module E dans E , u n'est pas diviseur à gauche de 0 dans l'anneau $\mathcal{L}(E)$.

b) Si E est un A-module unitaire admettant une base, et si u n'est pas diviseur à gauche de 0 dans $\mathcal{L}(E)$, u est un isomorphisme de E dans E .

c) Soit G le sous-groupe du groupe additif $\mathbb{Q}$, formé des nombres rationnels de la forme k/p^n , où p est un nombre premier fixe, n un entier $\geqslant 0$ quelconque, k un entier rationnel quelconque. Soit E le groupe quotient G/Z ; montrer que l'endomorphisme $x \longrightarrow px$ du Z-module E n'est pas diviseur à gauche de 0 dans $\mathcal{L}(E)$, mais n'est pas non plus un isomorphisme de E dans E .

6) a) Si u est un endomorphisme d'un A-module E tel que $u(E)=E$, u n'est pas diviseur à droite de 0 dans l'anneau $\mathcal{L}(E)$.

b) Montrer que, si E est un Z-module ayant une base, il existe des endomorphismes u de E tels que $u(E) \neq E$, mais que u ne soit pas diviseur à droite de 0 dans $\mathcal{L}(E)$.

§ 3. Structure des espaces vectoriels.

1. Bases d'un espace vectoriel.

Les familles libres dans un espace vectoriel peuvent être caractérisées par la propriété suivante (inexacte dans un module quelconque, cf. § 1, n° 8) :

PROPOSITION 1. *Pour qu'une famille (a_ι) d'éléments d'un espace vectoriel E soit libre, il faut et il suffit que, quel que soit l'indice $\varkappa$, $a_\varkappa$ ne soit pas combinaison linéaire des a_ι d'indice $\neq \varkappa$.*

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 $a_\varkappa = \sum_{\iota \neq \varkappa} (-\lambda_\varkappa^{-1} \lambda_\iota) a_\iota$.

On peut exprimer autrement l'énoncé en disant que pour tout $\varkappa$, $a_\varkappa$ ne doit pas appartenir au sous-espace vectoriel engendré par les a_ι d'indice $\neq \varkappa$.

En particulier, tout élément $x \neq 0$ d'un espace vectoriel est libre.

COROLLAIRE. *Si (a_ι) est une famille libre d'éléments d'un espace vectoriel E, et si $b \in E$ n'appartient pas au sous-espace engendré par (a_ι), l'ensemble formé des a_ι et de b est libre.*

En effet, le raisonnement de la prop. 1 montre qu'on ne peut avoir de relation de la forme $\mu b + \sum_\iota \lambda_\iota a_\iota = 0$ avec $\mu \neq 0$; d'autre part, l'hypothèse entraîne que si $\mu = 0$, on a aussi $\lambda_\iota = 0$ pour tout ι.

PROPOSITION 2. *Pour une partie B d'un espace vectoriel E, les trois propriétés suivantes sont équivalentes :*

a) *B est une base de E ;*

b) *B est une partie libre maximale de E ;*

c) *B est un système de générateurs minimal de E.*

En effet, si B est une base de E, tout élément de E est combinaison linéaire d'éléments de B, donc aucune partie de E contenant B et distincte de B n'est libre : a) entraîne b). D'autre part, si S est une partie de B distincte de B, et si $a \in B$ n'appartient pas à S,

a n'appartient pas au sous-espace engendré par S , donc S n'est pas un système de générateurs de E : a) entraîne c) .

Supposons maintenant que B soit une partie libre maximale de E ; si B n'engendrait pas E , il existerait un x n'appartenant pas au sous-espace engendré par B , donc (cor. de la prop.1) $B \cup \{x\}$ serait libre contrairement à l'hypothèse : b) entraîne a) .

Enfin, si B est un système de générateurs minimal de E , B est libre; sans quoi, il existerait $x \in B$ qui appartiendrait au sous-espace engendré par l'ensemble $S = B \cap \complement\{x\}$, d'après la prop.1 ; S serait donc un système de générateurs de E , contrairement à l'hypothèse : c) entraîne donc a) .

On remarquera que la première partie du raisonnement s'applique encore à un module quelconque E : la propriété a) entraîne donc toujours b) et c) .

Nous allons montrer que <u>tout espace vectoriel admet une base</u> ; plus précisément :

THEOREME 1.- <u>Tout système de générateurs</u> S <u>d'un espace vectoriel</u> E <u>contient une base de</u> E .

En effet, l'ensemble $\mathcal{F}$ des <u>parties libres</u> de S , ordonné par inclusion, est un ensemble <u>de caractère fini</u> (Ens.R , § 7,n°11) , d'après la prop.9 du § 1,n°8 . En vertu du th. de Zorn, $\mathcal{F}$ a donc un élément <u>maximal</u> B ; montrons que B engendre E , ce qui établira que B est une base de E . Dans le cas contraire, il existerait un $x \in S$ n'appartenant pas au sous-espace engendré par B , donc $B \cup \{x\}$ serait une partie libre de S (cor. de la prop.1), contrairement à la définition de B ; ce qui achève la démonstration.

COROLLAIRE.- <u>Tout espace vectoriel sur un corps K est isomorphe à un espace vectoriel de la forme</u> $K_s^{(I)}$.

Remarque. Lorsque S est fini, la démonstration du th.1 ne fait pas appel à l'axiome de choix, puisque sans utiliser cet axiome (~~remarque~~ Ens. Chap.III) on établit, que tout ensemble de parties d'un ensemble fini admet un élément maximal.

Exemple. Tout anneau contenant un corps K, et dont l'élément unité est aussi élément unité de K, est un espace vectoriel sur K, et admet donc une base par rapport à K (voir §7) ; 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 $\mathbb{R}$ admet une base (infinie) par rapport au corps des nombres rationnels $\mathbb{Q}$; toute base de $\mathbb{R}$ par rapport à $\mathbb{Q}$ est appelée base de Hamel.*

THEOREME 2 (théorème d'échange). Soient $(a_\iota)_{\iota\in I}$ une famille d'éléments d'un espace vectoriel E, V le sous-espace de E engendré par (a_ι), $(b_\lambda)_{\lambda\in L}$ une famille d'éléments de E telle que la famille $(\dot{b}_\lambda)_{\lambda\in L}$ des classes mod.V des b_λ engendre E/V. Dans ces conditions, il existe une sous-famille $(a_\iota)_{\iota\in J}$ de $(a_\iota)_{\iota\in I}$ et une sous-famille $(b_\lambda)_{\lambda\in M}$ de $(b_\lambda)_{\lambda\in L}$ telles que la réunion des ensembles d'éléments de ces deux familles soit une base de E.

En effet, le th.1 montre qu'il existe une sous-famille $(a_\iota)_{\iota\in J}$ de $(a_\iota)_{\iota\in I}$ qui est une base de V, et une sous-famille $(\dot{b}_\lambda)_{\lambda\in M}$ de $(\dot{b}_\lambda)_{\lambda\in L}$ qui est une base de E/V ; la famille $(b_\lambda)_{\lambda\in M}$ est alors une base d'un sous-espace supplémentaire de V (§1, prop.11), d'où le théorème.

Nous avons en particulier démontré que :

PROPOSITION 3. Pour tout sous-espace vectoriel V de E et toute base B de E, il existe une partie B' de B qui est une base d'un sous-espace vectoriel supplémentaire de V.

On peut donc remplacer la partie $B \cap \complement B'$ de B par une base de V sans cesser d'avoir une base de E , d'où le nom de "théorème d'échange" donné au th.2 .

COROLLAIRE. Toute partie libre de E est contenue dans une base de E .

Remarque. La démonstration du th.2 montre que l'existence d'un sous-espace supplémentaire d'un sous-espace V de E s'établit sans utiliser l'axiome de choix lorsque E/V possède un système de générateurs fini (voir la remarque suivant le th.1) .

2. Espaces vectoriels de dimension finie.

THEOREME 3. Si un espace vectoriel E sur un corps K a une base finie de n éléments, toute autre base de E a n éléments.

Raisonnons par récurrence sur n . Le théorème est vrai pour n=1 : en effet, si E est engendré par un élément a , tout élément $x = \lambda a \neq 0$ de E engendre aussi E puisque $a = \lambda^{-1} x$, donc aucune base de E ne peut avoir plus d'un élément. Supposons maintenant le théorème démontré pour n=m-1 et démontrons-le pour n=m . Soit $(a_i)_{1 \leqslant i \leqslant m}$ une base de m éléments de E , $(b_\iota)_{\iota \in I}$ une autre base de E .

Soit $b_\alpha = \sum_{i=1}^{m} \lambda_i a_i$ un élément de cette base, k un indice tel que $\lambda_k \neq 0$; si V est le sous-espace engendré par les m-1 éléments a_i d'indice $\neq k$, b_α n'appartient pas à V , donc forme avec les a_i d'indice $\neq k$ un système libre (cor. de la prop.1) ; en outre, comme $a_k = \lambda_k^{-1} b_\alpha + \sum_{i \neq k} (-\lambda_k^{-1}) \lambda_i a_i$, ce système libre est une base de E . Pour tout $\iota \neq \alpha$ on peut écrire $b_\iota = \mu_\iota b_\alpha + c_\iota$, où $c_\iota \in V$; comme les b_ι d'indice $\neq \alpha$ forment une base d'un supplémentaire W de Kb_α et que V est aussi supplémentaire de Kb_α , les c_ι forment une base de V (§ 1, cor. de la prop.8). Comme V admet une base de m-1 éléments, le théorème est démontré.

DEFINITION 1.- On dit qu'un espace vectoriel E sur un corps K est de dimension linéaire finie, ou de rang fini (ou encore qu'il a un nombre fini de dimensions linéaires) par rapport à K s'il possède une base finie. Le nombre d'éléments d'une base quelconque de E est alors appelé la dimension linéaire ou le rang de E (ou encore le nombre de dimensions linéaires de E) par rapport à K et noté $[E : K]$.

Si un espace vectoriel E sur K n'a pas de base finie, on dit encore qu'il est de dimension linéaire infinie (ou de rang infini, ou qu'il a une infinité de dimensions linéaires) par rapport à K .

Si une partie quelconque M d'un espace vectoriel E sur K engendre un sous-espace vectoriel de dimension linéaire finie, on appelle rang de M par rapport à K la dimension linéaire de ce sous-espace.

Par abus de langage, toutes les fois qu'aucune confusion n'est possible, on dit "dimension" au lieu de "dimension linéaire" et on supprime la mention "par rapport à K" dans les expressions précédentes.

Lorsqu'on dit qu'un espace vectoriel sur un corps K est de dimension $\geqslant n$, on entend dire qu'il est de dimension finie $\geqslant n$ ou de dimension infinie par rapport à K .

Le th.3 entraîne les corollaires suivants :

COROLLAIRE 1.- Tout espace vectoriel de dimension n sur un corps K est isomorphe à K^n . Pour qu'un espace vectoriel sur K soit isomorphe à un espace de dimension n par rapport à K , il faut et il suffit qu'il soit de dimension n par rapport à K .

COROLLAIRE 2.- Dans un espace vectoriel E de dimension n , tout système de générateurs de E a au moins n éléments ; un système de générateurs de E qui a n éléments est une base de E .

C'est une conséquence immédiate des théorèmes 1 et 3 .

COROLLAIRE 3.- Dans un espace vectoriel E de dimension n , toute partie libre de E a au plus n éléments ; une partie libre de n éléments est une base de E .

En effet d'après le cor. de la prop.3, toute partie libre de E est contenue dans une base de E .

On peut encore exprimer ce corollaire en disant que tout sous-espace d'un espace de dimension n est de dimension $\leqslant n$; s'il est de dimension n , il est identique à l'espace tout entier.

COROLLAIRE 4. Soient M et N deux sous-espaces de dimensions finies $[M:K]=m$, $[N:K]=n$, d'un espace vectoriel E sur un corps K . Si le sous-espace $M \cap N$ est de dimension q $(0 \leqslant q \leqslant \mathrm{Min}(m,n))$, le sous-espace $M+N$ est de dimension p telle que

$$p+q = m+n \quad . \tag{1}$$

La proposition est immédiate lorsque $q=0$, c'est-à-dire lorsque la somme $M+N$ est directe. En général (prop.3), M est somme directe de $M \cap N$ et d'un sous-espace M_1 , qui est donc de dimension $m-q$; N est somme directe de $M \cap N$ et d'un sous-espace N_1 de dimension $n-q$; donc $M+N$ est somme des sous-espaces $M \cap N$, M_1 et N_1 , et il est immédiat que cette somme est directe, ce qui donne $p=q+(m-q)+(n-q)$ c'est-à-dire (1).

Remarques. 1) Tout espace vectoriel monogène sur un corps K est un K-module simple (chap.I, § 6, n° 14, déf. 14), puisqu'il est engendré par un quelconque de ses éléments $\neq 0$. Un espace vectoriel de dimension finie sur K est donc un K-module semi-simple (chap.I, § 6, n° 15, déf. 15) ; le fait que deux bases finies d'un tel espace aient même nombre d'éléments est donc la traduction de la prop.13 du chap.I § 6, n° 15 (elle-même conséquence immédiate du th. de Jordan-Hölder) ; de même, pour un espace vectoriel de dimension finie, la prop.3 n'est que la traduction de la prop.14 du chap.I, § 6, n° 15 (pour la

(pour la généralisation des th.1 et 2, voir chap.I, § 6, exerc.18). De ces deux propriétés, on déduit d'ailleurs sans peine qu'un espace vectoriel E de dimension n ne peut avoir de base infinie : car n+1 éléments de cette base engendreraient un sous-espace V de E, et d'après la prop.3, l'ensemble formé de ces éléments et d'un certain nombre d'éléments d'une base de n éléments de E, serait encore une base finie de E, qui aurait ainsi au moins n+1 éléments, ce qui est absurde.

2) La démonstration du th.3 ne fait pas appel aux th.1 et 2 ; elle peut servir à les établir lorsqu'on suppose que E admet une base finie de n éléments. Il suffit en effet d'appliquer le raisonnement de récurrence du th.3 au cas où $(b_\iota)_{\iota \in I}$ est une famille quelconque d'éléments $\neq 0$ de E : il prouve qu'il existe une partie finie J de I, ayant $p \leqslant n$ éléments, telle que $(b_\iota)_{\iota \in J}$ soit une base du sous-espace engendré par la famille $(b_\iota)_{\iota \in I}$, et en outre qu'il existe n-p éléments de la base donnée $(a_i)_{1 \leqslant i \leqslant n}$ de E, formant avec les b_ι d'indice $\iota \in J$ une base de E. D'autre part, quand l'entier n et la famille $(b_\iota)_{\iota \in I}$ sont explicités (c'est-à-dire que l'ensemble I est explicité et que les composantes de chacun des b_ι par rapport à (a_i) sont explicitées), le même raisonnement fournit un moyen d'obtenir explicitement la famille $(b_\iota)_{\iota \in J}$ et les n-p éléments a_i formant avec cette famille une base de E : il suffit de remarquer que, dans la démonstration du th.3, les μ_ι et les c_ι se déterminent explicitement en remplaçant dans les expressions (explicites par hypothèse) des b_ι d'indice $\iota \neq \alpha$ comme combinaisons linéaires des a_i, l'élément a_k par son expression (explicite) comme combinaison linéaire de b_α et des a_i d'indice $\neq k$.

On obtient en outre par ce procédé l'expression explicite des composantes des b d'indice $\iota \notin J$ par rapport à la base $(b_\iota)_{\iota \in J}$.

3) Le th.3 est valable, non seulement pour les espaces vectoriels, mais aussi pour certaines catégories de modules (cf. exerc.7 et 8, et aussi chap.III, § 3). Par contre, on peut donner des exemples de modules admettant deux bases finies qui n'ont pas le même nombre d'éléments (cf. exerc.16);

4) Le th.3 exprime que deux bases d'un même espace vectoriel sont <u>équipotentes</u> si l'une d'elles est finie ; en réalité, la propriété est vraie sans cette restriction (cf. exerc. 4)).

On donne souvent aux sous-espaces vectoriels de dimension 1 (resp. de dimension 2) d'un espace vectoriel E sur un corps quelconque K le nom de <u>droites</u> (resp. <u>plans</u>), * par analogie avec le cas (le plus fréquent en Analyse) où K est le corps $\mathbf{R}$ des nombres réels *; de même, on dit qu'un sous-espace H de E est un <u>hyperplan</u> si E/H est un espace vectoriel de dimension 1 (ou, ce qui revient au même d'après la prop.3, si H admet un supplémentaire de dimension 1)(*). On peut encore définir les hyperplans comme les éléments maximaux de l'ensemble $\mathfrak{G}$, ordonné par inclusion, des sous-espaces vectoriels de E, <u>distincts de</u> E. En effet il y a correspondance biunivoque entre les sous-espaces contenant un sous-espace H, et les sous-espaces de l'espace quotient E/H (§ 1, prop.1) ;

(*) Au chap.IX, les mots de "droite", "plan" et "hyperplan" recevront une acception plus large, et les notions que nous désignons ci-dessus par ces mots seront appelées respectivement <u>droites homogènes</u>, <u>plans homogènes</u> et <u>hyperplans homogènes</u>. Mais aucune confusion n'est à craindre dans les chapitres antérieurs au chap.IX, et nous omettrons donc le qualificatif "homogène" jusque là.

pour que H soit maximal, il faut et il suffit donc que E/H ne contienne aucun sous-espace distinct de $\{0\}$ et de lui-même, ce qui signifie que E/H est de dimension 1 .

On notera que, dans un espace vectoriel de dimension finie n , les hyperplans sont les sous-espaces de dimension n-1 .

3. Rang d'une application linéaire.

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 de E supplémentaire de H (prop.3), u(E) est isomorphe à G , et la restriction de u à G est un isomorphisme de G sur u(G)=u(E) . Si (a_ι) est une base de G , les éléments $u(a_\iota)$ forment donc une base de u(E) .

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

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

PROPOSITION 4. Soient E et F deux espaces vectoriels de dimensions respectives m et n ; pour toute application linéaire u de E dans F on a

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

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, car la dimension de $H = u^{-1}(0)$ est égale à $m-\rho(u)$.

COROLLAIRE. Soit E un espace vectoriel de dimension finie n ; pour un endomorphisme u de E , les quatre propriétés suivantes sont équivalentes:

a) u est un automorphisme de E ;

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

c) u est une application de E sur E ;

d) u est de rang n .

Au contraire, lorsque E est de dimension infinie, un endomorphisme de E peut être biunivoque ou appliquer E sur E sans être un automorphisme de E (exerc.16).

Remarque.- Si K et K' sont deux corps isomorphes, on définit de la même manière le rang d'une application semi-linéaire u d'un espace vectoriel E sur K , dans un espace vectoriel F sur K' (relatif à un isomorphisme σ de K sur K') : c'est la dimension du sous-espace u(E) lorsque cette dimension est finie. Il est immédiat que ce rang est égal à celui de l'application linéaire v de E dans l'espace vectoriel F_σ sur K , associée à u ($\S 2, n^o 6$) .

Exercices.- 1) Soient M et N deux sous-modules semi-simples d'un module E , de longueurs (chap.I, $\S 6, n^{os}$ 14 et 15) respectives m et n . Si l'intersection $M \cap N$ est de longueur q , la somme $M+N$ est un module semi-simple de longueur p telle que $p+q=m+n$.

2) Soit E un module complètement réductible (chap.I, § 6, exerc.18), M et N deux sous-modules de E tels que E/M et E/N soient semi-simples ; soient m et n les longueurs respectives de E/M et E/N . Montrer que $E/(M \cap N)$ et $E/(M+N)$ sont semi-simples ; si q et p sont leurs longueurs respectives, on a $p+q=m+n$.

3) On dit qu'un module complètement réductible (chap.I, §6, ex.18) est homogène s'il est somme directe de sous-modules simples isomorphes à un même module. Soit E un module complètement réductible, somme directe d'une famille $(M_\iota)_{\iota \in I}$ de sous-modules simples ; tout sous-module simple de E est isomorphe à un des M_ι

(chap.I, § 6, exerc.18b)) ; pour chaque $\iota \in I$, le sous-module G_ι, somme directe de tous les sous-modules simples de E isomorphes à M_ι, est appelé le composant homogène d'indice ι 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.

4) a) Soit E un A-module complètement réductible homogène (exerc.3), 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 (se borner au cas où I est infini ; distinguer deux cas, d'après l'exerc.12 du § 1, 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 du § 1). Cas particulier des espaces vectoriels.

b) Soit E un A-module complétement 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 $(N_\varkappa)_{\varkappa \in K}$ 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 (à l'aide de l'exerc.3, se ramener à a)).

5) 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 longueur infinie est inexact.

6) a) On dit qu'un A-module satisfait à la condition maximale (resp. minimale) si l'ensemble de tous ses sous-modules satisfait à la condition maximale (resp. minimale ; cf. chap.I § 6, exerc. 15).

Montrer que, si E_1, E_2 sont deux A-modules satisfaisant à la condition maximale (resp. minimale), $E_1 \times E_2$ satisfait à la condition maximale (resp. minimale) (si (M_k) est une suite croissante (resp. décroissante) de sous-modules de $E_1 \times E_2$, montrer, en considérant les composants des M_k dans E_1, qu'il existe un indice p tel que, pour $k \geqslant p$, on ait $M_k = M_p + M_k \cap E_2$ (resp. $M_p = M_k + M_p \cap E_2$, d'où résulte que M_p/M_k est isomorphe à $(M_p \cap E_2)/(M_k \cap E_2)$)).

b) En déduire que, pour que le A-module A^n satisfasse à la condition maximale (resp. minimale), il faut et il suffit que A satisfasse à la condition maximale (resp. minimale).

7) a) Soit A un anneau ayant un élément unité et tel que le A-module A satisfasse à la condition maximale (exerc.6). Montrer que tout système de générateurs du module A^n a au moins n éléments (dans le cas contraire, il existerait une application linéaire de A^p sur A^n pour $p < n$, et par suite un endomorphisme u de A^n tel que $u(A^n) = A^n$ et $u^{-1}(0) \neq \{0\}$; montrer que ce résultat est incompatible avec la condition maximale dans A^n).

b) Soit B un sous-anneau de A ayant même élément unité que A. Montrer de même que tout système de générateurs de B^n a au moins n éléments (remarquer que tout système de générateurs de $B^n \subset A^n$ est aussi un système de générateurs de A^n). En déduire que si un B-module unitaire E admet une base d'un nombre fini d'éléments, toute autre base de E a le même nombre d'éléments.

8) Soit A un anneau ayant un élément unité et tel que le A-module A satisfasse à la condition minimale (exerc.6). Montrer que toute partie libre du module A^n a au plus n éléments (dans le cas contraire, il existerait un sous-module de A^p, où $p > n$, isomorphe à A^p et distinct de A^p ; ce résultat est incompatible avec la condition minimale dans A^p (cf. chap.I, §6, exerc. 15)).

En déduire que si un A-module unitaire E admet une base d'un nombre fini d'éléments, toute autre base de E a le même nombre d'éléments.

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

a) Si A admet un corps des quotients à gauche K (chap.I, § 9, exerc.8) et si E est un espace vectoriel sur K , M un A-module contenu dans E , montrer que toute partie de M qui est libre par rapport à A est aussi libre par rapport à K (remarquer que, si α et β sont deux éléments $\neq 0$ de A , il existe deux éléments γ , δ de A tels que $\alpha\beta^{-1} = \gamma^{-1}\delta$) .

b) Pour que, dans le A-module A^n , il n'existe pas de partie 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), en remarquant que $A^n \subset K^n$).

10) Soit E un espace vectoriel de dimension n sur un corps K , $(a_i)_{1 \leqslant i \leqslant n}$ une base de E , V un sous-espace de dimension $p < n$ de E . Pour tout $x = \sum_{i=1}^{n} \xi_i a_i \neq 0$ appartenant à V , on désigne par i(x) le plus grand des indices i tels que $\xi_i \neq 0$.

Montrer qu'il existe une suite strictement croissante $(i_k)_{1 \leqslant k \leqslant p}$ de p indices appartenant à l'intervalle $[1,n]$ de $\mathcal{N}$, et une base $(b_k)_{1 \leqslant k \leqslant p}$ de V , ayant les propriétés suivantes : i_k est le plus petit des indices i(x) pour tout les $x = \sum_{i=1}^{n} \xi_i a_i \in V$ non nuls tels que, pour tous les indices $h < k$, $\xi_{i_h} = 0$; pour tout $x \in V$ ayant ces propriétés et tel en outre que $i(x) = i_k$, on a $x = \lambda b_k$, où λ est un scalaire $\neq 0$.

En déduire que, pour tout $x = \sum_{i=1}^{n} \xi_i a_i \in V$, on a identiquement $x = \sum_{k=1}^{p} \xi_{i_k} b_k$.

11) Soit u une application linéaire d'un espace vectoriel E de dimension m dans un espace vectoriel F de dimension n ; on pose $H = {}^{-1}u(0)$. 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 ${}^{-1}u(W)$ est de dimension $r+m-\rho(u)$.

12) Soient u et v deux applications linéaires d'un espace vectoriel E de dimension m dans un espace vectoriel F de dimension n . Montrer que

$$|\rho(u)-\rho(v)| \leqslant \rho(u+v) \leqslant \mathrm{Min}(m,n,\rho(u)+\rho(v))$$

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

13) Soient E,F,G trois espaces 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 $u(E) \cap {}^{-1}v(0)$ 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

$$\rho(v\circ u)+\rho(w\circ v) \leqslant \rho(v)+\rho(w\circ v\circ u) \quad .$$

14) Si u et v sont deux endomorphismes d'un espace vectoriel E de dimension <u>finie</u>, tels que $u\circ v$ soit l'application identique de E , u et v sont deux automorphismes réciproques de E (cf. exerc. 16).

15) Soit E un espace vectoriel quelconque. Montrer que si u est un endomorphisme de E qui n'est pas diviseur à droite de 0 dans l'anneau $\mathcal{L}(E)$, on a $u(E)=E$ (cf. § 2, exerc. 6) .

16) Soit E un espace vectoriel ayant une base infinie dénombrable (e_n) .

a) L'endomorphisme u_1 de E tel que $u_1(e_{2n-1})=0$, $u_1(e_{2n})=e_n$ pour tout n applique E sur lui-même, mais n'est pas un automorphisme de E ; il existe un endomorphisme biunivoque v_1 de E tel que $v_1(E)\neq E$ et que $u_1 \circ v_1$ soit l'application identique de E .

b) Soit de même u_2 l'endomorphisme de E tel que $u_2(e_{2n})=0$, $u_2(e_{2n-1})=e_n$ pour tout n . Si A est l'anneau des endomorphismes de E , montrer que u_1 et u_2 forment une <u>base</u> du A-module A . En déduire que le A-module A^p est isomorphe à A pour tout $p>0$.

17) a) Soit E un espace vectoriel sur un corps K . Toute application f de E dans E permutable avec tous les <u>automorphismes</u> u de E (c'est-à-dire telle que $f(u(x))=u(f(x))$ pour tout $x \in E$ et tout automorphisme u de E) est de la forme $x \longrightarrow ax$, où a appartient à K (écrire que f est permutable avec tout automorphisme u laissant invariant un point $x \in E$, et en déduire que $f(x)=\rho(x)x$, où $\rho(x) \in K$) .

b) Soit f une application de $E \times E$ dans E , telle que, pour tout <u>automorphisme</u> 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 $f(x,y)=ax+\beta y$, où a et β sont des scalaires constants, et qu'on a $f(\lambda x, \mu x)=\varphi(\lambda , \mu)x$, où φ est une application arbitraire de $K \times K$ dans K (même méthode). Si en outre on a $f(u(x),u(y))=u(f(x,y))$ pour tout <u>endomorphisme</u> u de E , on a $f(x,y)=ax+\beta y$ quels que soient x,y . Généraliser aux applications de E^n dans E .

§ 4. Dualité.

1. Formes linéaires. Dual d'un module.

DEFINITION 1. - Etant donné un A-module à gauche E , on appelle forme linéaire sur E toute application linéaire de E dans le A-module A_s (anneau A considéré comme module à gauche par rapport à A).

Pour toute forme linéaire u sur E et tout $a \in A$, l'application $x \to u(x)a$ est encore une forme linéaire sur E , car pour tout $\lambda \in A$ on a $u(\lambda x)a=(\lambda u(x))a=\lambda((u(x)a)$; on désignera cette forme linéaire par ua . On voit aussitôt que, sur l'ensemble $\mathcal{L}(E,A_s)$ des formes linéaires sur E , la loi de groupe additif et la loi externe $(a,u) \to ua$ définissent une structure de module à droite par rapport à A . Muni de cette structure, $\mathcal{L}(E,A_s)$ s'appellera le module dual (ou simplement le dual) de E ; nous le noterons désormais E^*.

PROPOSITION 1. Si A est un anneau ayant un élément unité, le dual du module à gauche A_s est isomorphe au module à droite A_d .

En effet, soit u une forme linéaire sur A_s , et ε l'élément unité de A ; pour tout $\xi \in A$, on a $u(\xi)=u(\xi\varepsilon)=\xi u(\varepsilon)=\xi a$ en posant $a=u(\varepsilon)$; réciproquement, pour tout $a \in A$, $\xi \to \xi a$ est une forme linéaire u sur A_s telle que $u(\varepsilon)=a$; l'application $u \to u(\varepsilon)$ est donc un isomorphisme du dual de A_s sur le module à droite A_d .

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

Soit E un A-module, 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 $(x,x') \to \langle x,x' \rangle$ est appelée la forme bilinéaire fondamentale définie sur $E \times E^*$ (cf. chap.III et VIII) ; on a identiquement

(1) $\langle x+y, x' \rangle = \langle x, x' \rangle + \langle y, x' \rangle$

(2) $\langle x, x'+y' \rangle = \langle x, x' \rangle + \langle x, y' \rangle$

(3) $\langle ax, x' \rangle = a \langle x, x' \rangle$

(4) $\langle x, x'a \rangle = \langle x, x' \rangle a$

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

De même, pour tout $x \in E$, l'application partielle $x' \rightarrow \langle x, x' \rangle$ est une forme linéaire sur le A-module à droite E^* ; si on la désigne par $\tilde{x}$, on voit aussitôt que l'application $x \longrightarrow \tilde{x}$ est une application linéaire (dite canonique) de E dans le dual E^{**} de son dual (qu'on appelle le bidual de E).

Lorsque A possède un élément unité ε, l'application canonique de A_s dans son bidual est l'application identique de A_s sur lui-même, en vertu de la prop.1 ; toute forme linéaire x' sur A_s étant identifiée à l'élément $\xi' = x'(\varepsilon)$, la forme bilinéaire fondamentale est l'application $(\xi, \xi') \longrightarrow \xi\xi'$.

2. Orthogonalité.

DEFINITION 2. Soit E un module, E^* son dual ; on dit qu'un élément $x \in E$ et un élément $x' \in E^*$ sont orthogonaux si $\langle x, x' \rangle = 0$.

On dit qu'une partie M de E et une partie M' de E^* sont des ensembles orthogonaux si, quels que soient $x \in M$, $x' \in M'$, x et x' sont orthogonaux. En particulier, $x' \in E^*$ (resp. $x \in E$) est dit orthogonal à M (resp. M') s'il est orthogonal à tout élément de M (resp. M') .
Si x' et y' sont orthogonaux à M, il en est de même de $x'+y'$ et de $x'a$ pour tout $a \in A$, ce qui justifie la définition suivante :

DEFINITION 3. Etant donnée une partie quelconque M de E (resp. une partie quelconque M' de E^*), on appelle sous-module totalement orthogonal à M (resp. M') (ou simplement sous-module orthogonal à M (resp. M'), par abus de langage, lorsqu'aucune confusion n'est à craindre) l'ensemble des $x' \in E^*$ (resp. l'ensemble des $x \in E$) qui sont orthogonaux à M (resp. M').

Par définition d'une forme linéaire, le sous-module de E^* orthogonal à E se réduit à 0, le sous-module de E^* orthogonal à $\{0\}$ est identique à E^*.

Si M et N sont deux parties de E telles que $M \subset N$, M' et N' les sous-modules de E^* orthogonaux respectivement à M et N, on a $N' \subset M'$. Si (M_ι) est une famille de parties de E, le sous-module orthogonal à la réunion des M_ι est l'intersection $\bigcap_\iota M'_\iota$ des sous-modules M'_ι respectivement orthogonaux aux M_ι ; ce sous-module est aussi le sous-module orthogonal au sous-module engendré par la réunion des M_ι. Nous laissons au lecteur le soin d'énoncer les propriétés analogues pour les sous-modules orthogonaux aux parties de E^*.

Si M est un sous-module de E, M' le sous-module de E^* orthogonal à M, M" le sous-module de E orthogonal à M', on a $M \subset M''$, mais on peut avoir $M \neq M''$ (exerc. 3 et 5).

3. Dual d'un module quotient. Dual d'une somme directe.

PROPOSITION 2. Soient E un A-module, M un sous-module de E, φ l'homomorphisme canonique de E sur E/M. Si, à toute forme linéaire u sur E/M, on fait correspondre la forme linéaire $u \circ \varphi$ sur E, on définit un isomorphisme du dual de E/M sur le sous-module M' de E^* orthogonal à M.

Cette proposition n'est qu'un cas particulier de la prop. 1 du § 2. L'isomorphisme défini dans l'énoncé et son isomorphisme réciproque sont dits canoniques.

PROPOSITION 3. 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 , respectivement orthogonaux aux N_i , et pour chaque indice i , N'_i 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 $x = \sum_{i=1}^{n} h_i(x)$, donc, 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 $x \in N_i$, $h_i(x)=0$, donc $x' \circ h_i$ appartient au sous-module N'_i , et on a bien $E^* = \sum_{i=1}^{n} N'_i$; d'autre part cette somme est directe, car si une forme linéaire x' appartient à la fois à N'_i et à $\sum_{j \neq i} N'_j$, 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 $x'=0$. Enfin, pour établir la dernière partie de l'énoncé, il suffit d'appliquer la prop.2, en remarquant que M_i , supplémentaire de N_i , est isomorphe à E/N_i .

En raison de la prop.3, on identifie souvent le dual M_i^* de M_i au sous-module N'_i , en identifiant à toute forme linéaire u sur M_i la forme linéaire x' (bien déterminée) qui prolonge u à E et s'annule dans N_i .

COROLLAIRE. Le sous-module M'_i orthogonal à M_i , est égal à $\sum_{j \neq i} N'_j$.

En effet, comme M_i est contenu dans chacun des N_j d'indice $\neq i$, M'_i contient $\sum_{j \neq i} N'_j$; d'autre part, la prop.3, appliquée à la décomposition de E en somme directe de M_i et N_i , montre que E^* est somme directe de M'_i et N'_i ; comme E^* est aussi somme directe de $\sum_{j \neq i} N'_j$ et de N'_i , on a $M'_i = \sum_{j \neq i} N'_j$.

4. Formes coordonnées. Bases duales.

Soit E un A-module unitaire admettant une base finie $(a_i)_{1 \leqslant i \leqslant n}$; E est somme directe de n sous-modules isomorphes à A_s , donc, en vertu des prop.1 et 3, son dual E^* est somme directe de n sous-modules isomorphes à A_d . De façon précise, pour tout $x = \sum_{i=1}^{n} \xi_i a_i \in E$,

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)). Les a_i' $(1 \leqslant i \leqslant n)$ forment une <u>base</u> du dual E^* : en effet, pour toute forme linéaire x' sur E, on a $x'(x) = \sum_{i=1}^{n} \xi_i x'(a_i) = \sum_{i=1}^{n} a_i'(x)x'(a_i)$, c'est-à-dire $x' = \sum_{i=1}^{n} a_i'.x'(a_i)$; inversement, pour toute forme linéaire $y' = \sum_{i=1}^{n} a_i'\beta_i$, on a $y'(a_i)=\beta_i$ puisque $a_i'(a_i)=\varepsilon$ (élément unité de A) et $a_j'(a_i)=0$ pour $j \neq i$. La base (a_i') est dite <u>base duale</u> de la base (a_i) ; d'après le cor.2 de la prop.3 du § 2, la base duale (a_i') est bien déterminée par les conditions

$$(5) \qquad \begin{cases} \langle a_i, a_j' \rangle = 0 & \text{pour } i \neq j \\ \langle a_i, a_i' \rangle = \varepsilon & \text{pour tout } i \end{cases}$$

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

$$(6) \qquad \langle x, x' \rangle = \sum_{i=1}^{n} \xi_i \xi_i'$$

En particulier, si le dual du module A_s^n est identifié au module A_d^n, la base canonique de ce module n'est autre que la base duale de la base canonique de A_s^n.

Les relations (5) prouvent que l'application canonique $x \longrightarrow \tilde{x}$ de E dans son bidual E^{**} est un <u>isomorphisme de E sur</u> E^{**} ; aussi <u>identifie-t-on</u> E et E^{**} au moyen de cet isomorphisme, ce qui permet de dire, d'après (5) que (a_i) est la <u>base duale</u> de (a_i').

Lorsque E admet une base <u>infinie</u> (a_ι), on peut encore définir, pour tout indice ι, la <u>forme coordonnée</u> a_ι', qui, à tout x, fait correspondre sa composante d'indice ι relative à la base (a_ι). Mais la famille (a_ι'), qui est encore libre dans E^*, ne forme plus une base de ce module.

5. Dualité dans les espaces vectoriels.

Les résultats du n°4 s'appliquent en particulier aux espaces vectoriels de dimension finie :

PROPOSITION 4.- Le dual d'un espace vectoriel à gauche E de dimension n sur un corps K est un espace vectoriel à droite de dimension n sur K ; l'application canonique $x \to \tilde{x}$ de E dans son bidual E^{**} est un isomorphisme de E sur E^{**}.

Si K est en outre commutatif, le dual E^* d'un espace vectoriel E de dimension finie est donc isomorphe à E .

Si V est un sous-espace d'un espace vectoriel E (de dimension quelconque), le dual de E/V est isomorphe au sous-espace V' de E^* orthogonal à V (prop.2) ; en particulier, d'après la prop.4 :

THEOREME 1.- Si un sous-espace V d'un espace vectoriel E admet un supplémentaire de dimension finie p , le sous-espace V' de E orthogonal à V est de dimension p .

COROLLAIRE 1.- Pour tout hyperplan H de E , il existe une forme linéaire x' sur E telle que $H = \overset{-1}{x'}(0)$.

En effet, le sous-espace H' de E^* orthogonal à H est une droite d'après le th.1 ; si $x'_0 \in H'$ et $x'_0 \neq 0$, $\overset{-1}{x'_0}(0)$ est un sous-espace de E contenant H et non identique à E , donc identique à H . On dit que $x'_0(x)=0$ est une équation de H ; comme H' est une droite, toute équation de H est de la forme $x'_0(x)\mu=0$ avec $\mu \neq 0$.

COROLLAIRE 2.- Soit E un espace vectoriel de dimension finie n ; si V est un sous-espace de E , de dimension p , le sous-espace V' de E^*, orthogonal à V , est de dimension n-p .

PROPOSITION 5.- Pour tout sous-espace V d'un espace vectoriel E , le sous-espace V'' de E , orthogonal au sous-espace V' de E^* orthogonal à V , est identique à V .

Il faut prouver que pour tout $x \in \complement V$, il existe une forme linéaire $x' \in V'$ telle que $\langle x,x' \rangle \neq 0$. Soit W un sous-espace supplémentaire de V , y le composant de x dans W ; par hypothèse $y \neq 0$. Soit (a_ι)

(a_ι) une base de W ; il existe un indice a tel que la composante d'indice a de y soit $\neq 0$; si U est le sous-espace de W engendré par les a_ι d'indice $\neq a$, U+V est un hyperplan ne contenant pas x ; si $x'_0(z)=0$ est une équation de U+V , on a $x'_0 \in V'$ et $x'_0(x)\neq 0$.

Nous avons démontré, en d'autres termes, que tout sous-espace vectoriel de E est intersection des hyperplans qui le contiennent.

COROLLAIRE.- Dans un espace vectoriel E , pour tout $x\neq 0$, il existe une forme linéaire x' telle que $\langle x,x'\rangle \neq 0$.

Si (x'_ι) est une famille de formes linéaires sur E telle que le sous-espace V de E soit intersection de la famille d'hyperplans $x'^{-1}_\iota(0)$, on dit que les relations $x'_\iota(x)=0$ forment un système d'équations de V . Si V admet un supplémentaire de dimension finie p , le th.1 montre qu'il existe un système d'équations de V formé de p équations, dont les premiers membres sont des formes linéairement indépendantes.

THEOREME 2.- Soit V' un sous-espace de dimension finie p du dual E^* d'un espace vectoriel E . Le sous-espace V de E , orthogonal à V' , a un supplémentaire de dimension p ; si $(a'_i)_{1\leqslant i\leqslant p}$ est une base de V', il existe une suite finie $(a_i)_{1\leqslant i\leqslant p}$ d'éléments de E formant une base d'un supplémentaire de V , et satisfaisant aux relations (5) ; en outre le sous-espace de E^* orthogonal à V , est identique à V' .

Considérons l'application $x \to (\langle x,a'_i\rangle)$ de E dans K^p ; c'est une application linéaire u de rang p . En effet, si u(E) était de dimension $< p$, il existerait une forme linéaire $(\xi_1,\xi_2,\dots,\xi_p) \to \xi_1 a_1+\xi_2 a_2+\dots+\xi_p a_p$ non identiquement nulle sur K^p , et nulle dans u(E) , d'après le th.1 ; autrement dit, on aurait $\sum_{i=1}^{p} \langle x,a'_i\rangle a_i=0$ pour tout $x\in E$, c'est-à-dire $\sum_{i=1}^{p} a'_i a_i=0$, les a_i n'étant pas tous nuls, ce qui contredit l'hypothèse. Le sous-espace $V=u^{-1}(0)$ est évidemment le sous-espace de E orthogonal à V' ; si W est un supplémentaire de V ,

W est de dimension p , et la restriction de u à W est un isomorphisme de W sur K^p . Si a_i est l'élément de W tel que $u(a_i)$ soit égal à l'élément e_i de la base canonique de K^p $(1 \leqslant i \leqslant p)$, les a_i satisfont donc aux relations (5) et forment une base de W. Enfin, le sous-espace de E^* orthogonal à V contient V' et est de dimension p , d'après le th? ; il est donc identique à V' .

COROLLAIRE.- Pour toute forme linéaire $x' \neq 0$ sur E , le sous-espace $x'^{-1}(0)$ est un hyperplan.

Tenant compte de ce corollaire, la dernière partie du th.2 peut encore s'exprimer de la façon suivante : si un sous-espace V de E est l'intersection d'un nombre fini d'hyperplans $x_i'^{-1}(0)$, toute forme linéaire qui s'annule dans V est combinaison linéaire des x_i' .

Remarques.- 1) Lorsque E est de dimension finie, le th.2 est une conséquence du th.1, appliqué au dual E^* de E , E étant identifié à son bidual E^{**}.

2) Lorsque V' est un sous-espace de E^* de dimension infinie, le sous-espace de E^* orthogonal au sous-espace V de E orthogonal à V' , peut être distinct de V' (exerc. 11).

6. Equations linéaires.

Soient E et F deux A-modules ; toute relation de la forme

$$u(x) = y_0 \tag{7}$$

où u est une application linéaire donnée de E dans F , y_0 un élément donné de F , x une variable parcourant E , est appelée une équation linéaire ; on dit que x est l'inconnue de l'équation, y_0 son second membre ; si $y_0 = 0$, l'équation est dite homogène . Tout élément $x_0 \in E$ pour lequel la relation (7) est vraie est une solution de l'équation.

On dit qu'un problème mathématique est un <u>problème linéaire</u> si sa résolution équivaut à la recherche des solutions d'une équation linéaire ; de tels problèmes se présentent très fréquemment dans toutes les parties de la mathématique.

<u>Exemples</u>.- 1) Une équation linéaire (7) est dite scalaire ~~si F=A~~, autrement dit, si u est une <u>forme linéaire</u> sur E . Etant donnée une famille $(x'_\iota)_{\iota\in I}$ de formes linéaires sur E , et une famille $(\eta_\iota)_{\iota\in I}$ d'éléments de A , ayant même ensemble d'indices, le <u>système d'équations linéaires</u> (scalaires)

$$\langle x, x'_\iota \rangle = \eta_\iota \qquad (\iota \in I) \tag{8}$$

est par définition la relation "quel que soit $\iota \in I$, $\langle x, x_\iota \rangle = \eta_\iota$" . On dit que les η_ι sont les <u>seconds membres</u> du système (8) ; s'ils sont tous nuls, le système est dit <u>homogène</u>.

La recherche des $x \in E$ qui satisfont à cette relation est un problème linéaire, car le système est équivalent à l'équation (7), en prenant $F = A^I$, $y_\iota = (\eta_\iota)$, et désignant par u l'application $x \to (\langle x, x'_\iota \rangle)$ de E dans F .

Si E est un A-module unitaire admettant une base $(a_\lambda)_{\lambda\in L}$, et si on pose $x = \sum_\lambda \xi_\lambda a_\lambda$, et $a_{\lambda\iota} = \langle a_\lambda, x'_\iota \rangle$, le système (8) s'écrit

$$\sum_{\lambda\in L} \xi_\lambda a_{\lambda\iota} = \eta_\iota \qquad (\iota \in I) \tag{9}$$

Réciproquement le problème consistant à trouver une famille $(\xi_\lambda)_{\lambda\in L}$ de scalaires telle que $\xi_\lambda = 0$ sauf pour un nombre fini d'indices, et que pour tout $\iota \in I$, la relation (9) soit vraie, est un problème linéaire ; il est équivalent à la recherche des solutions du système (8), en prenant $E = A^{(L)}$, $x = \sum_\lambda \xi_\lambda a_\lambda$, où (a_λ) est la base canonique de E, et en désignant par x'_ι la forme linéaire $x \to \sum_\lambda \xi_\lambda a_{\lambda\iota}$. Les ξ_λ sont appelés les <u>inconnues</u> du système (9), les $a_{\lambda\iota}$ ses <u>coefficients</u>.

Lorsqu'il y a lieu de préciser, on dit qu'un système (9) est un <u>système d'équations linéaires scalaires à gauche</u>. Un système

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

est de même dit <u>système d'équations linéaires scalaires à droite</u> par rapport aux <u>inconnues</u> ξ_λ (nulles sauf un nombre fini d'entre elles) ; les $a_{\lambda\iota}$ sont encore dits les <u>coefficients</u>, les η_ι les <u>seconds membres</u> d'un tel système, qui se ramène aussitôt à un système (9), en considérant les ξ_λ , η_ι et $a_{\lambda\iota}$ comme appartenant à l'anneau A^0 <u>opposé</u> de A .

En supposant toujours que (a_λ) est une base de E , la relation (7) équivaut, avec les notations précédentes, à

$$(10) \qquad \sum_{\lambda \in L} \xi_\lambda b_\lambda = y_0$$

où $b_\lambda = u(a_\lambda)$. Réciproquement la recherche des familles $(\xi_\lambda)_{\lambda \in L}$ (telles que $\xi_\lambda = 0$ sauf pour un nombre fini d'indices) satisfaisant à la relation (10) est un problème linéaire ; il équivaut à la recherche des solutions de (7), en désignant par u l'application de $E = A^{(L)}$ dans F définie par $u(a_\lambda) = b_\lambda$ pour tout λ , (a_λ) étant la base canonique de E (§ 2, cor. 2 de la prop. 3) .

* 2) Résoudre un <u>système d'équations différentielles linéaires</u>

$$(11) \qquad y_i'(x) - \sum_{j=1}^{n} a_{ij}(x) y_j(x) = b_i(x) \qquad (1 \leqslant i \leqslant n)$$

dans un intervalle ouvert $I =]\alpha, \beta[$ de la droite réelle $\mathbb{R}$, où les a_{ij} et les b_i sont des fonctions définies dans I , à valeurs réelles, c'est trouver toutes les suites finies $(y_i)_{1 \leqslant i \leqslant n}$ de n fonctions à valeurs réelles, définies, continues et dérivables dans I , et satisfaisant aux relations (11) pour tout $x \in I$. Un tel problème est un problème linéaire ; en effet, soit F l'ensemble des applications $x \to (z_i(x))$

de I dans $\mathbb{R}^n$, et soit E le sous-ensemble de F formé des applications telles que les n fonctions z_i soient dérivables dans I ; F est un espace vectoriel sur le corps $\mathbb{R}$, et E un sous-espace vectoriel de F ; la fonction $b(x)=(b_i(x))$ est un élément de F, et si, pour toute fonction $y=(y_i)\in E$ on pose

$$u(y) = (y_i' - \sum_{j=1}^{n} a_{ij}y_i)_{1\leqslant i\leqslant n}$$

$y \longrightarrow u(y)$ est une application linéaire de E dans F. On voit donc que la résolution du système différentiel (11) équivaut à la recherche des solutions de l'équation linéaire $u(y)=b$. *

La résolution d'une équation linéaire (7) peut se décomposer en deux problèmes : 1° déterminer s'il existe des solutions de (7) (c'est-à-dire si $y_0 \in u(E)$) ; 2° dans l'affirmative, déterminer l'ensemble (non vide) des solutions de (7) (c'est-à-dire l'ensemble $^{-1}u(y_0)$).

Le second de ces problèmes peut se ramener au même problème pour l'équation $u(x)=0$, qu'on appelle l'équation homogène associée à (7) :

PROPOSITION 6.- Si x_0 est une solution de (7), l'ensemble des solutions de (7) est identique à l'ensemble des points x_0+x_1, où x_1 parcourt l'ensemble des solutions de l'équation homogène associée à (7).

En effet, la relation $u(x)=y_0$ s'écrit $u(x)=u(x_0)$, c'est-à-dire $u(x-x_0)=0$.

Autrement dit, l'ensemble des solutions de (7) est $x_0+{}^{-1}u(0)$. On notera que $^{-1}u(0)$ est un sous-module de E donc, n'est jamais vide, puisqu'il contient 0 (qui est appelé la solution nulle, ou solution triviale, de l'équation homogène $u(x)=0$).

Il résulte de la prop.6 que, pour que l'équation (7) ait au plus une solution, il faut et il suffit que $^{-1}u(0)=\{0\}$ (autrement dit, que l'équation homogène associée à (7) n'ait pas de solution non triviale) ; dans ce cas, pour tout $y\in F$, l'équation $u(x)=y$ a au plus une solution, autrement dit, u est un isomorphisme de E dans F.

Nous allons nous borner, dans ce qui suit, à l'étude des systèmes scalaires (8), où E est un espace vectoriel sur un corps K (commutatif ou non), et où en outre 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 7.- Pour qu'un système scalaire (8) d'équations linéaires sur un espace vectoriel E^*, de rang fini r, ait au moins 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 (8), l'ensemble des solutions de (8) est de la forme x_0+V, où V est un sous-espace de E admettant un supplémentaire de dimension r.

La condition d'existence d'une solution du système (8), donnée dans l'énoncé, est évidemment nécessaire. Prouvons qu'elle est suffisante.

En effet, il existe r des formes x'_ι, soient x'_{ι_k} $(1 \leqslant k \leqslant r)$ formant une base du sous-espace V' de dimension r du dual E^*, engendré par les x'_ι (§ 3, th.1). 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 de (8) est identique à l'ensemble des solutions du système partiel

$$\langle x, x' \rangle_k = \eta_{\iota_k} \qquad (1 \leqslant k \leqslant r) \tag{12}$$

Soit V le sous-espace de E orthogonal à V' ; d'après le th.2, il existe une base $(a_k)_{1 \leqslant k \leqslant r}$ d'un supplémentaire W de V telle que $\langle a_k, x'_{\iota_k} \rangle = 1$ pour $1 \leqslant k \leqslant r$, $\langle a_h, x'_{\iota_k} \rangle = 0$ pour $h \neq k$. Tout $x \in E$ se mettant d'une seule manière sous la forme $x = \sum_{k=1}^{r} \xi_k a_k + z$, où $z \in V$, pour que x soit solution du système (12), il faut et il suffit que $\xi_k = \eta_{\iota_k}$ pour $1 \leqslant k \leqslant r$, z étant arbitraire dans V ; ce qui achève la démonstration.

Un système (8) 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 le système (γ), correspond au cas où il n'y a que n inconnues), son dual E^* est de dimension n, donc $r \leqslant n$.

En particulier :

COROLLAIRE 1.- Un système (8) 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.- Pour qu'un système homogène (γ) de m équations à n inconnues (à coefficients dans un corps K) admette des solutions non triviales, il faut et il suffit que son rang soit $< n$.

Il en sera toujours ainsi si $m < n$.

COROLLAIRE 3.- Un système (γ) (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) Le critère donné dans la prop.7 pour l'existence des solutions d'un système (8) n'est plus suffisant lorsque ce système est de rang infini ; si on suppose par exemple que les x'_ι sont les formes coordonnées dans l'espace $E=K^{(I)}$ de dimension infinie (n°4), le critère de la prop.7 est vérifié quels que soient les seconds membres, puisque les x'_ι sont linéairement indépendantes ; mais le système (8) n'admet alors de solution que si les η_ι sont nuls à l'exception d'un nombre fini d'entre eux.

2) Dans un système quelconque (9), remplaçons tous les coefficients $a_{\lambda\iota}$ dont l'indice λ appartient à une partie donnée H de l'ensemble d'indices L, par 0. Si le nouveau système admet des solutions, à toute solution $(\xi_\lambda)_{\lambda \in \complement H}$ de ce système correspond une solution

$(\xi_\lambda)_{\lambda \in L}$ du système initial, obtenue en prenant $\xi_\lambda = \xi_\lambda$ pour $\lambda \in \complement H$, $\xi_\lambda = 0$ pour $\lambda \in H$. Inversement, si (ξ_λ) est une solution quelconque de (8), comme il n'y a qu'un nombre fini d'indices λ tels que $\xi_\lambda \neq 0$, cette solution s'obtiendra par le procédé précédent à partir d'une solution du système formé en annulant tous les a_{λ_ν} correspondant aux indices λ tels que $\xi_\lambda = 0$. Toute solution d'un système (9) sur un corps, est donc solution d'un système de rang fini ; mais ce système dépend de la solution de (9) considérée.

7. Transposée d'une application linéaire.

Soient E et F deux A-modules, 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.

DEFINITION 4.- *On appelle transposée d'une application linéaire* u *d'un module* E *dans un module* F, *et on note* ${}^t u$, *l'application* $y' \longrightarrow y' \circ u$ *du dual* F^* *de* F *dans le dual* E^* *de* E.

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

$$\langle u(x), y' \rangle = \langle x, {}^t u(y') \rangle \tag{13}$$

La transposée ${}^t u$ est une application linéaire de F^* dans E^*, car pour tout $\lambda \in A$, on a $(y'\lambda)\, u = (y' \circ u)\lambda$.

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

$${}^t(u+v) = {}^t u + {}^t v \tag{14}$$

$${}^t(\lambda u) = \lambda\, {}^t u \tag{15}$$

pour tout λ appartenant au centre de A.

Soit G un troisième A-module, u une application linéaire de E dans F, v une application linéaire de F dans G ; d'après (13) on a identiquement en $x \in E$ et $z' \in G^*$

$$\langle v(u(x)), z' \rangle = \langle u(x), {}^t v(z') \rangle = \langle x, {}^t u({}^t v(z')) \rangle$$

d'où la relation

(16) $$ {}^t(v \circ u) = {}^t u \circ {}^t v $$

Lorsque E et F sont des A-modules unitaires ayant chacun une base finie, de sorte qu'ils puissent être identifiés avec leurs bidуals respectifs ($n^o 4$), l'identité (15) montre que la transposée ${}^t({}^t u)$ 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.

DEFINITION 5.- Soit u un isomorphisme d'un module E sur un module F ; on appelle contragrédiente de u et on note $\check{u}$ la transposée ${}^t v$ de l'isomorphisme v réciproque de u.

PROPOSITION 8.- 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 ${}^t u$ de u.

En effet, la relation $x' = y' \circ u$ entraîne $y' = x' \circ v$, donc ${}^t u$ est un isomorphisme de F^* sur E^*, et ${}^t v = \check{u}$ est l'isomorphisme réciproque.

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

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

PROPOSITION 9.- Soit u une application linéaire d'un A-module E dans un A-module F. Pour qu'un élément $y' \in F^*$ soit orthogonal au sous-module u(E) de F, il faut et il suffit que ${}^t u(y') = 0$.

En effet, l'identité (13) montre que la relation $\langle u(x), y' \rangle = 0$ pour tout $x \in E$ équivaut à $\langle x, {}^t u(y') \rangle = 0$ pour tout $x \in E$, c'est-à-dire à ${}^t u(y') = 0$.

Lorsque E et F sont des espaces vectoriels, on déduit de la prop.9 et de la prop.5 une caractérisation du sous-espace u(E) :

THEOREME 3.- 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 (c'est-à-dire que $y_0 \in u(E)$) il faut et il suffit que y_0 soit orthogonal au sous-espace V' de F^* formé des $y' \in F^*$ tels que ${}^t u(y')=0$.

En effet, d'après la prop.9 , V' est le sous-espace orthogonal à u(E) , donc (prop.5) u(E) est le sous-espace orthogonal à V' .

COROLLAIRE.- 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 ${}^t u$ soit un isomorphisme de F^* dans E^*.

Le th.3 entraîne la proposition 7 dans le cas particulier d'un système scalaire (8) ayant un nombre fini d'équations

$$\langle x, x'_i \rangle = \eta_i \qquad (1 \leqslant i \leqslant m)$$

En effet, si (e_i) est la base canonique du module A^m , on vérifie sans peine que la transposée de l'application $x \longrightarrow (\langle x, x'_i \rangle)$ est l'application $y' \longrightarrow \sum_{i=1}^{n} x'_i \langle e_i, y' \rangle$; en écrivant que $y_0=(\eta_i)$ est orthogonal à tout y' tel que $\sum_{i=1}^{n} x'_i \langle e_i, y' \rangle = 0$, on retrouve la condition de compatibilité du système (8) donnée dans la prop.7 .

Supposons toujours que E et F soient des espaces vectoriels, et gardons les notations du th.3 ; d'après la prop.3, le dual du sous-espace u(E) de F est isomorphe à F^*/V' (puisque u(E) admet un supplémentaire dans F) ; mais d'après la définition de V' , F^*/V' est isomorphe à ${}^t u(F^*)$; donc :

THEOREME 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 ${}^t u(F^*)$ de E^* . En particulier, si u est de rang fini, u et ${}^t u$ ont même rang .

Transposée d'une application semi-linéaire.- Soit σ un isomorphisme d'un anneau A sur un anneau B , u une application semi-linéaire, relative à σ , d'un A-module E dans un B-module F (§ 2,n°6). Si τ est l'isomorphisme de B sur A , réciproquement de σ , pour tout $y' \in F^*$, l'application $x \to \langle u(x),y' \rangle^{\tau}$ est une forme linéaire sur E ; si on la désigne par ${}^t u(y')$, on définit une application ${}^t u$ de F^* dans E^* , qu'on appelle encore la transposée de u ; elle est donc définie par l'identité en x et y'

(18) $$\langle u(x),y' \rangle = \langle x, {}^t u(y') \rangle^{\sigma}$$

On vérifie immédiatement que ${}^t u$ est une application semi-linéaire de F^* dans E^* , relative à l'isomorphisme τ . Si φ désigne l'application identique de F_σ sur F , v l'application linéaire de E dans F_σ , associée à u , de sorte que $u = \varphi \circ v$ (§ 2,n°6), on vérifie aisément qu'on a ${}^t u = {}^t v \circ {}^t \varphi$, et ${}^t \varphi$ est un di-isomorphisme de F^* sur $(F_\sigma)^*$, relatif à l'isomorphisme τ ; ce qui permet d'étendre aussitôt aux transposées des applications semi-linéaires toutes les propriétés des transposées des applications linéaires établies ci-dessus.

Exercices.- 1) Soit A un anneau n'ayant pas de diviseur de zéro. Si E est un A-module dont l'annulateur n'est pas nul, montrer que le dual de E se réduit à 0 .

2) Montrer que le dual du corps $\mathbb{Q}$ des nombres rationnels, considéré comme $\mathbb{Z}$-module, est réduit à 0 .

3) Montrer que, dans un A-module E , l'image réciproque de 0 par l'application canonique $x \to \tilde{x}$ de E dans son bidual E^{**} , est le sous-module E_0 de E orthogonal à E^* . Donner un exemple où E^* et E_0 ne sont pas réduits à 0 (considérer un module contenant un élément dont l'annulateur contient un élément non diviseur de 0) .

4) Soit M un sous-module d'un module E , M' le sous-module de E^* orthogonal à M . Pour toute forme linéaire x' sur E , soit x'_M la restriction de x' à M ; la relation $x'_M = y'_M$ équivaut à $x'-y' \in M'$; 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 à cette application est un isomorphisme de E^*/M' dans M^* . Donner un exemple où cet isomorphisme n'applique pas E^*/M' sur M^* (prendre $E=A_S$ où A est un anneau sans diviseur de 0 et ayant un élément unité, et $M=A.a$, où a est un élément $\neq 0$ de A tel que $A.a \neq A$).

5) Soit E un A-module, E_0 le sous-module de E orthogonal à E^* ; donner un exemple où $E_0 = \{0\}$, mais où il existe un sous-module M de E , tel que, si M' est le sous-module de E orthogonal à M , M" le sous-module de E orthogonal à M' , on ait $M \neq M"$ (prendre $E=A_S$, où A est un anneau sans diviseur de 0 , ayant un élément unité, et pour M un sous-module quelconque de A_S , distinct de $\{0\}$ et de A_S) .

6) Soit (M_ι) une famille de sous-modules d'un module E , et soit $M = \bigcap_\iota M_\iota$. On désigne par $M"_\iota$ (resp. M") le sous-module de E orthogonal au sous-module M'_ι (resp. M') de E^* orthogonal à M_ι (resp. M). Montrer que si $M"_\iota = M_\iota$ pour tout ι , on a M"=M .

7) Soit E un module somme directe de deux sous-modules M et N . On désigne par E_0 (resp. M_0,N_0) le sous-module de E (resp. M,N) orthogonal à E^* (resp. M^*, N^*) ; on désigne par M" (resp. N") le sous-module de E orthogonal au sous-module M' (resp. N') de E^* orthogonal à M (resp. N) . Montrer que $E_0 = M_0 + N_0$, $M_0 = M \cap N"$, $N_0 = N \cap M"$, $M" = M + N_0 = M + E_0$.

8) Si un module E est somme directe d'une famille (M_ι) de sous-modules, son dual E^* est isomorphe au module produit des duals M_ι^* des M_ι.

9) Soient V et W deux sous-espaces d'un espace vectoriel E, V' et W' les sous-espaces de E^* orthogonaux à V et W respectivement. Montrer que le sous-espace de E^* orthogonal à $V \cap W$ est identique à $V'+W'$.

10) Donner un exemple de module E tel qu'il existe deux sous-modules M,N de E tels que, si M' et N' sont les sous-modules de E^* orthogonaux à M et N respectivement, le sous-module de E^* orthogonal à $M \cap N$ soit distinct de $M'+N'$ (prendre $E=A_S$, où A est un anneau sans diviseur de 0, ayant un élément unité, et qui ne peut être plongé dans un corps ; utiliser l'exerc.9 du chap.I, § 9).

11) Soit E un espace vectoriel de dimension infinie. Montrer que :

a) L'application canonique $x \to \tilde{x}$ de E dans son bidual E^{**} n'applique pas E sur E^{**}.

b) Il existe des sous-espaces V' de E^*, de dimension infinie, tels que, si V est le sous-espace de E orthogonal à V', V' soit distinct du sous-espace de E^* orthogonal à V (prendre pour V' le sous-espace engendré par les formes coordonnées correspondant à une base de E). En déduire qu'il existe une famille infinie (V_ι) de sous-espaces de E telle que, si V'_ι est le sous-espace de E^* orthogonal à V_ι, le sous-espace de E^* orthogonal à $\bigcap_\iota V_\iota$ soit distinct de $\sum_\iota V'_\iota$.

c) Montrer que, si V' et W' sont deux sous-espaces de dimension finie de E^*, V et W les sous-espaces de E orthogonaux à V' et W' respectivement, le sous-espace de E orthogonal à $V' \cap W'$ est $V+W$.

montrer que cette proposition est inexacte si V' et W' sont de dimension infinie (utiliser b)).

12) Pour qu'un système (S) d'équations linéaires scalaires sur un espace vectoriel E (par rapport à un corps K) soit de rang r, il faut et il suffit que l'application $x \to (\langle x,x' \rangle)$ de E dans K^I soit de rang r.

13) Soit u une application linéaire d'un module E dans un module F, $v={}^t u$ sa transposée ; pour tout sous-module M de E montrer que, si M' est le sous-module de E^* orthogonal à M, le sous-module de F^* orthogonal à u(M) est $^{-1}v(M')$; pour tout sous-module N' de F^*, si N est le sous-module de F orthogonal à N', le sous-module de E orthogonal à v(N') est $^{-1}u(N)$.

14) Soient E et F deux espaces vectoriels, u une application linéaire de E dans F. Si V est un sous-espace vectoriel de E, V' le sous-espace de E^* orthogonal à V, montrer que le dual de u(V) est isomorphe à ${}^t u(F^*)$ $(V' \cap {}^t u(F^*))$. Si W' est un sous-espace de F^* tel que ${}^t u(W')$ soit de dimension finie, W le sous-espace de F orthogonal à W', ${}^t u(W')$ est isomorphe au dual de l'espace $u(E)/(W \cap u(E))$.

15) 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 ${}^t u$ 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_ι) une base de E, il existe une forme linéaire y' sur F telle que $\langle e_\iota, x' \rangle = \langle e_\iota, {}^t u(y') \rangle$ pour tout ι).

16) Soit M un A-module simple.
a) Si $aM=\{0\}$ pour tout $a \in A$, et si M a p éléments (p étant premier, cf. § 1, exerc. 12), 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 $a \in M$ (§ 1, exerc. 12), et si $\mathfrak{a}$ est l'annulateur de a, le dual de M est isomorphe à l'annulateur à droite de $\mathfrak{a}$ dans 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, le sous-module M_0 de M orthogonal au dual M^* de M est réduit à 0.

17) Etendre la prop. 5 et les th. 3 et 4 aux modules complètement réductibles (§ 3, exerc. 2) tels que le dual d'aucun de leurs sous-modules simples ne se réduise à 0.

§ 5. Restriction du corps des scalaires.

1. Restriction à un sous-corps.

Soit E un espace vectoriel sur un corps K. Si on restreint le domaine d'opérateurs de la loi externe de E à un sous-corps K_0 de K, E devient un ~~sous~~-espace vectoriel par rapport à K_0. On sait d'autre part que K est un espace vectoriel par rapport à K_0.

PROPOSITION 1.- *Si $(a_\lambda)_{\lambda \in L}$ est une base de E par rapport à K, $(\beta_\mu)_{\mu \in M}$ une base de K par rapport à K_0, la famille $(\beta_\mu a_\lambda)_{(\lambda, \mu) \in L \times M}$ est une base de E par rapport à K_0.*

En effet, il est immédiat que la famille $(\beta_\mu a_\lambda)$ engendre E, considéré comme espace vectoriel sur K_0. Elle est d'autre part une famille libre dans cet espace vectoriel ; en effet, une relation $\sum_{\lambda,\mu} \rho_{\lambda\mu} \beta_\mu a_\lambda = 0$, avec $\rho_{\lambda\mu} \in K_0$ et $\rho_{\lambda\mu} = 0$ sauf pour un nombre fini de couples (λ, μ), s'écrit $\sum_\lambda \left(\sum_\mu \rho_{\lambda\mu} \beta_\mu \right) a_\lambda = 0$, donc entraîne $\sum_\mu \rho_{\lambda\mu} \beta_\mu = 0$ pour tout λ, et pour chaque λ la relation $\sum_\mu \rho_{\lambda\mu} \beta_\mu = 0$ entraîne $\rho_{\lambda\mu} = 0$ pour tout μ.

COROLLAIRE.- *Si $[E:K]$ et $[K:K_0]$ sont finis, il en est de même de $[E:K_0]$ et on a*

$$[E:K_0] = [E:K][K:K_0] \tag{1}$$

réciproquement, si $[E:K_0]$ est fini, $[E:K]$ et $[K:K_0]$ sont finis, et on a la relation (1).

La première partie est une conséquence immédiate de la prop.1. Inversement, si E admet une base finie par rapport à K_0, toute autre base de E par rapport à K_0 est aussi finie, ce qui entraîne que les ensembles d'indices L et M sont finis.

Toute partie de E, qui est libre par rapport à K est aussi libre par rapport à K_0, mais la réciproque n'est pas vraie, comme le montre la prop.1. On a toutefois la proposition suivante :

PROPOSITION 2.- Soit (a_ι) une famille d'éléments de E, libre par rapport à K ; soit H_0 le sous-espace vectoriel par rapport à K_0 engendré par (a_ι) ; toute partie de H_0 qui est libre par rapport à K_0 est aussi libre par rapport à K.

D'après la prop.9 du § 1, on peut se borner à prouver la proposition pour une partie finie de H_0 ; chacun des éléments d'une telle partie étant combinaison linéaire d'un nombre fini de a_ι, on peut en outre se borner au cas où la famille (a_ι) est une famille finie $(a_i)_{1 \leqslant i \leqslant n}$ de n éléments ; H_0 est alors de dimension n par rapport à K_0. Soient alors $b_1, b_2, \ldots, b_m$ $(m \leqslant n)$ des éléments de H_0 formant un système libre par rapport à K_0 ; il existe n-m éléments $a_{i_1}, a_{i_2}, \ldots, a_{i_{n-m}}$ du système libre (a_i) formant avec les b_i une base de H_0 par rapport à K_0 (§ 3, prop.3) ; donc les n éléments a_i sont des combinaisons linéaires, à coefficients dans $K_0 \subset K$, de $a_{i_1}, \ldots, a_{i_{n-m}}$, $b_1, b_2, \ldots, b_m$; ces derniers engendrent donc le sous-espace vectoriel H par rapport à K qui a pour base la famille (a_i) ; comme H est de dimension n par rapport à K, les éléments $a_{i_1}, \ldots, a_{i_{n-m}}$, $b_1, \ldots, b_m$ forment une base de H par rapport à K, donc $(b_i)_{1 \leqslant i \leqslant m}$ est un système libre par rapport à K.

COROLLAIRE.- Soit V_0 un sous-espace vectoriel de H_0 (par rapport à K_0). Si V est le sous-espace vectoriel par rapport à K engendré par V_0, on a $V_0 = V \cap H_0$.

En effet, soit (b_λ) une base de V_0 par rapport à K_0 ; (b_λ) est aussi une base de V par rapport à K, d'après la prop.2. On a évidemment $V_0 \subset V \cap H_0$; d'autre part, si $x \in V \cap H_0$, on peut écrire $x = \sum_\lambda \rho_\lambda b_\lambda$, où les $\rho_\lambda \in K$; autrement dit, x et les b_λ forment un système lié par rapport à K ; comme ils appartiennent à H_0, ils forment aussi un système lié par rapport à K_0, d'après la prop.2 ; or, (b_λ) est libre par rapport à K_0, donc x appartient nécessairement au sous-espace V_0 engendré par (b_λ) (§ 3, cor. de la prop.1).

THEOREME 1.- Si les coefficients et les seconds membres d'un système d'équations linéaires scalaires

$$\sum_{\lambda \in L} \xi_\lambda a_{\lambda\iota} = \eta_\iota \qquad (\iota \in I) \tag{2}$$

appartiennent à un sous-corps K_0 d'un corps K, et si le système admet une solution (ξ_λ) formée d'éléments de K, il admet aussi une solution (ξ_λ) formée d'éléments de K_0.

D'après la remarque 2 du § 4, n°6, on peut se limiter au cas d'un système de m équations à n inconnues ; un tel système est alors équivalent à une relation de la forme

$$\sum_{i=1}^{n} \xi_i b_i = y_0 \tag{3}$$

où y_0 et les b_i appartiennent à l'espace $E = K^m$; d'après l'hypothèse, ils appartiennent en outre au sous-espace vectoriel $E_0 = K_0^m$ par rapport à K_0, engendré par la base canonique de E.

Le cor. de la prop.2 montre alors que si V_0 (resp. V) est le sous-espace vectoriel par rapport à K_0 (resp K) engendré par les b_i, on a $V_0 = V \cap E_0$. Or, la relation (3) signifie que $y_0 \in V$; comme par hypothèse $y_0 \in E_0$, on a $y_0 \in V_0$, ce qui démontre le théorème.

COROLLAIRE 1.- Si les coefficients et les seconds membres d'un système (2) appartiennent à K_0, et si le système admet une seule solution formée d'éléments de K, ces éléments appartiennent à K_0.

COROLLAIRE 2.- Si les coefficients d'un système homogène

$$(4) \qquad \sum_{\lambda \in L} \xi_\lambda \alpha_{\lambda\iota} = 0 \qquad (\iota \in I)$$

appartiennent à K_0 et si le système admet une solution non triviale formée d'éléments de K, il admet aussi une solution non triviale formée d'éléments de K_0.

En effet, soit (ξ_λ) une solution non triviale formée d'éléments de K, et supposons que $\xi_\mu \neq 0$; alors la famille $(\xi_\mu^{-1} \xi_\lambda)_{\lambda \neq \mu}$ sera solution du système

$$\sum_{\lambda \neq \mu} \xi_\lambda \alpha_{\lambda\iota} = - \alpha_{\mu\iota} \qquad (\iota \in I)$$

D'après le th.1, ce système admet donc une solution $(\xi_\lambda)_{\lambda \neq \mu}$ formée d'éléments appartenant à K_0 ; en posant $\xi_\mu = 1$, la famille $(\xi_\lambda)_{\lambda \in L}$ est donc une solution non triviale de (4) formée d'éléments de K_0.

2. Modules réguliers sur un anneau d'intégrité.

Soit E un espace vectoriel sur un corps K. Si on restreint le domaine d'opérateurs de E à un sous-anneau A de K, E devient un A-module. Il est clair que tout élément $\neq 0$ de E, étant libre par rapport à K, est aussi libre par rapport à A.

DEFINITION 1.- On dit qu'un A-module est régulier si tout élément $\neq 0$ de ce module est libre.

En d'autres termes, dans un module régulier, la relation $ax=0$ équivaut à "$a=0$ ou $x=0$".

Nous venons de montrer que E, considéré comme un A-module, est régulier, et il en est évidemment de même de tout sous-module de E.

Lorsque A est un anneau d'intégrité, nous allons voir que l'on obtient ainsi tous les A-modules réguliers. De façon précise :

THEOREME 2.- Soit M un module régulier sur un anneau d'intégrité A. Il existe un espace vectoriel $\widetilde{M}$ sur le corps des fractions K de A et un sous-module M' de $\widetilde{M}$ (considéré comme A-module) isomorphe à M.

Soit K^* l'ensemble des éléments $\neq 0$ de K.

Considérons l'ensemble produit $K^* \times M$, et définissons, entre deux éléments (α,x) et (β,y) de ce produit, la relation suivante, que nous désignerons par R : "il existe un élément $\lambda \neq 0$ de A tel que $\lambda\alpha$ et $\lambda\beta$ appartiennent à A, et que $(\lambda\alpha)x=(\lambda\beta)y$". Montrons d'abord que R est une relation d'équivalence : elle est visiblement réflexive et symétrique, il suffit de voir qu'elle est transitive ; or, supposons qu'il existe deux éléments non nuls λ, μ de A tels que $\lambda\alpha$, $\lambda\beta$, $\mu\beta$, $\mu\gamma$ appartiennent à A, et que $(\lambda\alpha)x = (\lambda\beta)y$, $(\mu\beta)y=(\mu\gamma)z$; on en conclut $(\lambda\mu\alpha)x=\mu((\lambda\alpha)x)=\mu((\lambda\beta)y)=\lambda((\mu\beta)y)=\lambda((\mu\gamma)z)=(\lambda\mu\gamma)z$; comme $\lambda\mu$ appartient à A et n'est pas nul (puisque A est un anneau d'intégrité), (α,x) et (γ,z) sont bien liés par la relation R. Nous écrirons désormais la relation d'équivalence R sous la forme $(\alpha,x)\equiv(\beta,y)$.

Considérons l'ensemble quotient $\widetilde{M}=(K^* \times M)/R$; nous allons y définir une structure d'espace vectoriel par rapport à K (cf. chap.I, § 2, n°4 et § 9, n°4).

En premier lieu, si (α,x) est un élément de la classe $\dot{x} \in \widetilde{M}$, et ρ un élément de K^*, la classe qui contient l'élément $(\rho\alpha,x)$ est indépendante de l'élément (α,x) considéré dans la classe $\dot{x}$. En effet, si $(\alpha,x)\equiv(\beta,y)$, il existe deux éléments non nuls λ, μ de A tels que $\lambda\alpha$, $\lambda\beta$ et $\mu\rho$ appartiennent à A, et que $(\lambda\alpha)x=(\lambda\beta)y$, d'où $(\lambda\mu\rho\alpha)x=(\mu\rho)((\lambda\alpha)x)=(\mu\rho)((\lambda\beta)y)=(\lambda\mu\rho\beta)y$, d'où $(\rho\alpha,x)\equiv(\rho\beta,y)$. Nous désignerons par $\dot{\rho x}$ la classe de $(\rho\alpha,x)$.

Pour définir la somme de deux éléments de $\widetilde{M}$, remarquons d'abord que, pour tout élément $\lambda \neq 0$ de A, on a $(\alpha,x) \equiv (\frac{\alpha}{\lambda}, \lambda x)$; en effet,

si $\mu \neq 0$ est un élément de A tel que $\mu\alpha$ appartienne à A , on a $(\lambda\mu\alpha)x=\lambda(\mu\alpha)x)=(\mu\alpha)(\lambda x)=(\lambda\mu\frac{\alpha}{\lambda})(\lambda x)$. Soient alors $\dot{x}$ et $\dot{y}$ deux éléments de $\widetilde{M}$; il existe un élément $\delta \in K$ et deux éléments x,y de M tels que $(\delta,x)\in\dot{x}$, $(\delta,y)\in\dot{y}$; en effet, soit (α,u) un élément de $\dot{x}$, (β,v) un élément de $\dot{y}$; il existe deux éléments non nuls λ , μ de A tels que $\frac{\alpha}{\beta}=\frac{\lambda}{\mu}$; on prendra $\delta=\frac{\alpha}{\lambda}=\frac{\beta}{\mu}$, $x=\lambda u$, $y=\mu v$. Cela étant, la classe de l'élément $(\delta,x+y)$ ne dépend pas des éléments de la forme (δ,x) , (δ,y) choisis dans les classes $\dot{x}$ et $\dot{y}$; en effet, si $(\delta,x)\equiv(\delta',x')$, $(\delta,y)\equiv(\delta',y')$, il existe des éléments non nuls λ , μ de A tels que $\lambda\delta$, $\lambda\delta'$, $\mu\delta$, $\mu\delta'$ appartiennent à A et que $(\lambda\delta)x=(\lambda\delta')x'$, $(\mu\delta)y=(\mu\delta')y'$, d'où $(\lambda\mu\delta)x=(\lambda\mu\delta')x'$, $(\lambda\mu\delta)y=(\lambda\mu\delta')y'$, et par suite $(\lambda\mu\delta)(x+y)=(\lambda\mu\delta')(x'+y')$, ce qui prouve que $(\delta,x+y)\equiv(\delta',x'+y')$. Nous désignerons par $\dot{x}+\dot{y}$ la classe de $(\delta,x+y)$.

Il est immédiat que l'addition ainsi définie est commutative et associative ; tous les éléments $(\lambda,0)$ de $\widetilde{M}$ appartiennent à une même classe, qui est élément neutre pour l'addition dans $\widetilde{M}$; en outre, si (α,x) est un élément de $\dot{x}$, et $\dot{y}$ la classe contenant $(\alpha,-x)$, $\dot{x}+\dot{y}$ contient $(\alpha,0)$ et est donc l'élément neutre de $\widetilde{M}$, ce qui achève de prouver que $\widetilde{M}$ est un <u>groupe additif</u> . On achève la définition de la loi externe $(\rho,\dot{x})\to\rho\dot{x}$ entre éléments de K et éléments de $\widetilde{M}$ en prenant pour $0\dot{x}$ l'élément neutre de $\widetilde{M}$ quel que soit $\dot{x}$; la vérification des axiomes (M_I), (M_{II}) et (M_{III}) des modules (§1, n°1) est immédiate, et il est clair que $\widetilde{M}$ est un K-module unitaire, donc un espace vectoriel sur K .

Faisons maintenant correspondre à tout élément $x\in M$ la classe $\dot{x}$ de l'élément $(1,x)$ de $K\times M$; l'application $x\to\dot{x}$ est une <u>application linéaire</u> de M sur un <u>sous-module</u> M' de $\widetilde{M}$ ($\widetilde{M}$ étant considéré comme A-module), car pour tout $\lambda\in A$, on a $(1,\lambda x)\equiv(\lambda,x)$ si $\lambda\neq 0$,

et $(1,0)$ appartient par définition à la classe $\dot{0}x$. Pour voir que cette représentation est un isomorphisme, il suffit de montrer que la relation $(1,x)\equiv(1,y)$ entraîne $x=y$; or, cette relation signifie qu'il existe un élément $\lambda\neq 0$ de A tel que $\lambda x=\lambda y$, ou $\lambda(x-y)=0$; comme M est régulier par hypothèse, on en tire $x=y$.

C.Q.F.D.

D'après la définition de la loi de composition externe dans $\widetilde{M}$, il est clair que l'on a $\widetilde{M}=KM'$, autrement dit que l'espace vectoriel $\widetilde{M}$ est engendré par M' . Nous dirons que l'espace vectoriel $\widetilde{M}$ défini dans la démonstration d u th.2 est l'espace vectoriel associé au module régulier M ; le plus souvent, on identifie M au sous-module M' de $\widetilde{M}$.

L'espace vectoriel $\widetilde{M}$ est déterminé à une isomorphie près par la condition de contenir un A-module M' isomorphe à M , et engendrant l'espace vectoriel $\widetilde{M}$; cela résulte de la proposition suivante :

PROPOSITION 3.- Soient E_1, E_2 deux espaces vectoriels sur le corps des fractions K de l'anneau d'intégrité A , M_1, M_2 deux A-modules contenus respectivement dans E_1, E_2 , et tels que $E_1=KM_1$, $E_2=KM_2$; toute application linéaire f de M_1 dans M_2 se prolonge d'une seule manière en une application linéaire $\overline{f}$ de E_1 dans E_2 ; si f est un isomorphisme de M_1 sur M_2 , $\overline{f}$ est un isomorphisme de E_1 sur E_2 .

En effet, tout élément $y\in E_1$ peut s'écrire $y=ax$, avec $a\in K^*$ et $x\in M_1$; si le prolongement de f est possible, on doit avoir $\overline{f}(y)=af(x)$; inversement, si on définit $\overline{f}(y)$ de cette façon, la définition est bien indépendante de l'expression de y considérée, car si on a $ax=a'x'$, il existe $\lambda\in A$ non nul, tel que λa et $\lambda a'$ appartiennent à A et $(\lambda a)x=(\lambda a')x'$, donc $(\lambda a)f(x)=(\lambda a')f(x')$ et par suite $af(x)=a'f(x')$. L'application $\overline{f}$ est linéaire : en effet, si y et y' sont deux éléments de E_1 , il existe x,x' dans M_1 et $\rho\in K^*$ tels que $y=\rho x$, $y'=\rho x'$, d'où $\overline{f}(y+y')=\rho f(x+x')=\overline{f}(y)+\overline{f}(y')$; et si $\lambda\in K$,

on a $\overline{f}(\lambda y)=\overline{f}(\lambda \rho x)=(\lambda\rho)f(x)=\lambda\overline{f}(y)$.

Si f applique M_1 sur M_2 , $\overline{f}$ applique E_1 sur E_2 , car tout élément de E_2 peut alors s'écrire par hypothèse $\alpha f(x)=\overline{f}(\alpha x)$, où $\alpha\in K$ et $x\in M_1$. Enfin, si f est une application biunivoque de M_1 dans M_2 , $\overline{f}$ est une application biunivoque de E_1 dans E_2 ; en effet, si on a $\alpha f(x)=\alpha' f(x')$ où α et α' appartiennent à K^* , x et x' à M_1 , il existe $\lambda\neq 0$ dans A tel que $\lambda\alpha$ et $\lambda\alpha'$ appartiennent à A ; on a $(\lambda\alpha)f(x)=(\lambda\alpha')f(x')$ donc $f((\lambda\alpha)x)=f((\lambda\alpha')x')$, ce qui entraîne par hypothèse $(\lambda\alpha)x=(\lambda\alpha')x'$, c'est-à-dire $\alpha x=\alpha' x'$.

Conformément aux définitions données au § 3 (n^o2), si $\widetilde{M}$ est de dimension finie, cette dimension est appelée le rang du A-module régulier M . Si M admet un système fini de générateurs, il est de rang fini, car ce système engendre aussi $\widetilde{M}$; mais la réciproque est inexacte.

Par exemple, le corps $\mathbb{Q}$ des nombres rationnels est un $\mathbb{Z}$-module régulier de rang 1 , mais n'admettant pas de système fini de générateurs.

Plus particulièrement, si M admet une base (a_ι), la famille (a_ι) est aussi une base de $\widetilde{M}$: en effet, si on a $\sum_\iota \lambda_\iota a_\iota = 0$ où $\lambda_\iota\in K$ et $\lambda_\iota=0$ sauf pour un nombre fini d'indices, il existe un élément $\rho\neq 0$ de A tel que $\rho\lambda_\iota\in A$ pour tout ι , donc on a $\sum_\iota (\rho\lambda_\iota)a_\iota=0$, ce qui entraîne par hypothèse $\rho\lambda_\iota=0$ pour tout ι donc $\lambda_\iota=0$ pour tout .

Exercices.- 1) Soit V un sous-espace de dimension $p<n$ d'un espace vectoriel K^n . Montrer que, parmi tous les sous-corps $K'\subset K$ tels que l'intersection $V\cap K'^n$ soit un sous-espace de dimension p par rapport à K' , il en existe un plus petit (utiliser l'exerc.10 du § 3, en prenant pour (a_i) la base canonique de K^n ; montrer, à l'aide du th.1, que pour tout sous-corps K' ayant la propriété voulue, les p éléments b_k définis dans l'exerc.10 du § 3 appartiennent à K'^n).

2) Sur l'ensemble produit $A = Z \times (Z/(2))$ on définit une structure d'anneau commutatif en prenant pour loi de groupe additif le produit des lois additives de Z et $Z/(2)$, et en définissant la multiplication par la formule $(n,\varepsilon)(n',\varepsilon') = (nn', n\varepsilon' + n'\varepsilon + \varepsilon\varepsilon')$. Soit A_0 le sous-anneau de A formé des éléments $(n,0)$, qui a même élément unité que A et est isomorphe à l'anneau Z. Montrer que, dans le A_0-module engendré par la base canonique du A-module A^n, il existe des systèmes libres par rapport à A_0 mais non par rapport à A.

3) Soit K_0 un sous-corps d'un corps K tel que $[K:K_0] = 2$. Soit E un espace vectoriel par rapport à K, E_0 une partie 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 $x_1, x_2, \ldots, x_n$ est une famille d'éléments 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 ; si μ est un élément de K n'appartenant pas à K_0, on écrira les λ_k sous la forme $\rho_k + \mu\sigma_k$, où ρ_k et σ_k appartiennent à K_0).

Lorsque E est de dimension finie par rapport à K, montrer que si E_0, E'_0 sont deux espaces vectoriels par rapport à K_0 contenus dans E, V,V' les plus grands sous-espaces vectoriels de E (par rapport à K) contenus dans E_0, E'_0 respectivement, pour qu'il existe un automorphisme de E transformant E_0 en E'_0, il faut et il suffit que E_0 et E'_0 aient même dimension par rapport à K_0, V et V' même dimension par rapport à K.

4) Soit L un ensemble d'indices infini, K un corps quelconque. Montrer que toute base de l'espace vectoriel produit K^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^L dont toutes les coordonnées sont égales à 0 ou 1, E le sous-espace de K^L engendré par cette famille, N une partie de M telle que $(a_\mu)_{\mu \in N}$ soit une base de E (§ 3, th.1) ; pour tout indice $\mu \in \complement N$, soit $a_\mu = \sum_{\nu \in N} \xi_{\mu\nu} a_\nu$; en projetant cette relation sur les espaces facteurs de K^L, montrer, par application du th.1, que les $\xi_{\mu\nu}$ appartiennent au sous-corps K_0 de K engendré par les éléments 0 et 1 ; en remarquant que K_0 est dénombrable, montrer que N et M sont équipotents ; conclure en utilisant le th.2 du § 3, et l'exerc.4 du § 3).

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

En déduire qu'un espace vectoriel de dimension infinie sur un corps commutatif n'est jamais isomorphe à son dual (cf. § 4, exerc.7).

5) Généraliser le th.2 aux modules réguliers sur un anneau A non commutatif, admettant un corps des quotients à gauche (chap.I, § 9, exerc.8).

§ 6. Matrices.

1. Définition des matrices.

DEFINITION 1.- *On appelle matrice sur un ensemble non vide* E *toute famille* $(a_{\lambda\mu})_{(\lambda,\mu) \in L \times M}$ *d'éléments de* E *dont l'ensemble d'indices est le produit de deux ensembles finis* 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 apelée la colonne d'indice* μ *de la matrice.*

Les dénominations de "ligne" et de "colonne" proviennent de ce que, dans le cas où L et M sont des intervalles $[1,m]$, $[1,n]$ de $\mathcal{N}$, on imagine les éléments de la matrice disposés dans les cases d'un tableau rectangulaires ayant m lignes (rangées horizontales) et n colonnes (rangées verticales) :

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

Lorsqu'on parle de matrice à m lignes et n colonnes sans spécifier les ensembles d'indices des lignes et des colonnes il est sous-entendu que ces ensembles sont respectivement les intervalles $[1,m]$ et $[1,n]$ de $\mathcal{N}$.

Toute matrice dont l'un des ensembles d'indices L,M est vide est identique à la famille vide d'éléments de E : on l'appelle encore la matrice vide. Lorsque $L = \{\lambda_0\}$ et $M = \{\mu_0\}$ sont des ensembles réduits à un seul élément, on identifie souvent une matrice ayant L et M comme ensembles d'indices à l'unique élément qui la compose. On désigne d'ordinaire les matrices par des majuscules italiques.

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 sous-matrice de la matrice considérée ; on dit qu'elle s'obtient en supprimant 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 bordant 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 $\mu \in \complement K$.

L'ensemble des matrices sur un ensemble E, correspondant à des ensembles d'indices (finis) donnés L, M, est identique au produit $E^{L \times M}$. Si φ (resp. ψ) est une application biunivoque de L (resp. M) sur un ensemble L' (resp. M'), l'application qui à toute matrice $(a_{\lambda'\mu'})_{(\lambda',\mu') \in L' \times M'}$ sur E fait correspondre la matrice $(\beta_{\lambda\mu})_{(\lambda,\mu) \in L \times M}$, où $\beta_{\lambda\mu} = a_{\varphi(\lambda),\psi(\mu)}$, est une application biunivoque de l'ensemble $E^{L' \times M'}$ des matrices sur E, correspondant aux ensembles d'indices L', M', sur l'ensemble $E^{L \times M}$ des matrices sur E, correspondant aux ensembles d'indices L, M.

2. Matrices sur un anneau.

Les matrices qui sont de loin les plus importantes en Mathématique sont les matrices sur un anneau A. L'ensemble $A^{L \times M}$ des matrices sur l'anneau A, correspondant à des ensembles donnés L, M d'indices, peut être muni de la structure de groupe additif, produit des structures de groupe additif des facteurs A ; la somme 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 mêmes pour ces deux matrices.

On peut de même munir $A^{L \times M}$ de la structure de A-module à gauche (resp. de la structure de A-module à droite) 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. $(\xi_{\lambda\mu}\,\rho)$).

xixMx

si φ (resp. ψ) est une application biunivoque de L (resp. M) sur L' (resp. M'), l'application biunivoque de l'ensemble de matrices $A^{L' \times M'}$ sur l'ensemble de matrices $A^{L \times M}$ correspondant aux applications φ et ψ (n^o1) est un isomorphisme de chacune des structures de A-module du premier de ces ensembles sur la structure de même espèce du second.

On peut donc se borner, si on veut, au cas où L est l'intervalle $[1,m]$ de $\mathcal{N}$, M l'intervalle $[1,n]$. Supposons qu'on soit dans ce cas, et que A possède un élément unité ε ; pour tout couple $(i,j) \in L \times M$, soit 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 de matrices $A^{L \times M}$ de l'une des structures de module précédentes, les mn matrices E_{ij} forment la <u>base canonique</u> de ces modules.

<u>2. Matrices et applications linéaires</u>.

Soient A un anneau ayant un élément unité, L et M deux ensembles d'indices <u>finis</u>. Soient E et F deux A-modules <u>à droite</u> unitaires, admettant respectivement des <u>bases</u> $(a_\lambda)_{\lambda \in L}$, $(b_\mu)_{\mu \in M}$ ayant pour ensembles d'indices L et M. On sait (2, cor.2 de la prop.3) qu'une application linéaire u de E dans F est déterminée par la donnée des éléments $y_\lambda = u(a_\lambda)$ 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 $u(a_\lambda)=y_\lambda$. On a $u(a_\lambda) = \sum_{\mu \in M} b_\mu a_{\mu\lambda}$; les $a_{\mu\lambda}$ sont bien déterminés par la donnée de u, et inversement déterminent les $u(a_\lambda)$, donc u. Désignons par $\underline{M}(u;(a_\lambda),(b_\mu))$ (ou simplement par $\underline{M}(u)$ lorsqu'aucune confusion n'est possible) la matrice $(a_{\mu\lambda})_{(\mu,\lambda) \in M \times L}$ qu'on fait ainsi correspondre à u ; nous dirons que c'est <u>la matrice de l'application u, rapportée aux bases</u> (a_λ) <u>et</u> (b_μ) : la <u>colonne</u> d'indice λ de cette matrice est donc formée des composantes $a_{\mu\lambda}$

de $u(a_\lambda)$ relativement à la base (b_μ) de F . Il est clair que l'on a , pour deux applications linéaires quelconques u,v de E dans F

(1) $$\underline{M}(u+v)=\underline{M}(u)+\underline{M}(v)$$

Autrement dit, l'application $u \to \underline{M}(u;(a_\lambda),(b_\mu))$ est un <u>isomorphisme</u> du groupe additif $\mathcal{L}(E,F)$ des applications linéaires de E dans F , <u>sur</u> le groupe additif des matrices sur A ayant M comme ensemble d'indices des lignes et L comme ensemble d'indices des colonnes.

Lorsqu'on se donne la matrice $\underline{M}(u)=(a_{\mu\lambda})$ de u , rapportée aux bases (a_λ) et (b_μ), les composantes η_μ de u(x) relatives à la base (b_μ) sont données en fonction des composantes ξ_λ de x relatives à la base (a_λ), par la formule

(2) $$\eta_\mu = \sum_{\lambda \in L} a_{\mu\lambda}\, \xi_\lambda$$

pour tout $\mu \in M$.

<u>Remarque</u>.- Lorsque l'anneau A n'a pas d'élément unité, les formules (2) font encore correspondre à tout élément (ξ_λ) du module à droite A^L un élément (η_μ) du module A^M , et il est immédiat que l'application ainsi définie est linéaire ; mais plusieurs matrices distinctes peuvent alors définir la <u>même</u> application linéaire, et d'autre part, il peut exister des applications linéaires de A^L dans A^M qu'on ne peut obtenir de cette façon.

<u>4. Produit de matrices</u>.

Soient A un anneau ayant un élément unité, L,M,N trois ensembles d'indices finis, E,F,G trois A-modules à droite unitaires, admettant respectivement des bases $(a_\lambda)_{\lambda \in L}$, $(b_\mu)_{\mu \in M}$, $(c_\nu)_{\nu \in N}$.

Soient u une application linéaire de E dans F , v une application linéaire de F dans G . Proposons nous de trouver la matrice de l'application composée $w=v\circ u$ de E dans G , rapportée aux bases (a_λ) et (c_γ), connaissant les matrices $\underline{M}(u;(a_\lambda),(b_\mu))=(\alpha_{\mu\lambda})_{(\mu,\lambda)\in M\times L}$ et $\underline{M}(v;(b_\mu),(c_\gamma))=(\beta_{\gamma\mu})_{(\gamma,\mu)\in N\times M}$.

On a

$$w(a_\lambda)=v(u(a_\lambda))=v\Big(\sum_{\mu\in M} b_\mu \alpha_{\mu\lambda}\Big)=\sum_{\mu\in M} v(b_\mu)\alpha_{\mu\lambda}=\sum_{\mu\in M}\Big(\Big(\sum_{\gamma\in N} c_\gamma \beta_{\gamma\mu}\Big)\alpha_{\mu\lambda}\Big)$$

$$=\sum_{\gamma\in N} c_\gamma\Big(\sum_{\mu\in M}\beta_{\gamma\mu}\alpha_{\mu\lambda}\Big)$$

donc, si on pose $\underline{M}(w;(a_\lambda),(c_\gamma))=(\gamma_{\gamma\lambda})_{(\gamma,\lambda)\in N\times L}$, on a pour tout couple d'indices (γ,λ)

$$\gamma_{\gamma\lambda}=\sum_{\mu\in M}\beta_{\gamma\mu}\alpha_{\mu\lambda} \qquad (3)$$

DEFINITION 2.- Soient L, M, N trois ensembles d'indices finis, A un anneau , $\underline{X}=(\alpha_{\mu\lambda})_{(\mu,\lambda)\in M\times L}$ une matrice de l'ensemble $A^{M\times L}$, $\underline{Y}=(\beta_{\gamma\mu})_{(\gamma,\mu)\in N\times M}$ une matrice de l'ensemble $A^{N\times M}$. On appelle matrice produit de Y par X et on note YX la matrice $\underline{Z}=(\gamma_{\gamma\lambda})_{(\gamma,\lambda)\in N\times L}$ de l'ensemble $A^{N\times L}$ dont les éléments sont donnés par la formule (3) .

Avec cette définition, on peut donc écrire la formule

$$\underline{M}(v\circ u;(a_\lambda),(c_\gamma))=\underline{M}(v;b_\mu),(c_\gamma))\underline{M}(u;(a_\lambda),(b_\mu)) , \qquad (4)$$

ou, plus simplement

$$\underline{M}(v\circ u)=\underline{M}(v)\underline{M}(u) \qquad (5)$$

quand aucune confusion n'est à craindre.

Remarque.- Le produit YX 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 (3) figurent les éléments d'une même

ligne de $\underline{Y}$, multipliés à droite par les éléments d'une même colonne de $\underline{X}$: on dit que le produit de $\underline{Y}$ par $\underline{X}$ se fait "lignes par colonnes" .

Toute propriété relative à la somme ou à la composée d'applications linéaires se traduit en propriétés relatives à la somme ou au produit de matrices, grâce aux formules (1) et (5) . En particulier, on a les règles de distributivité et d'associativité

$$\underline{X}(\underline{Y}+\underline{Z}) = \underline{X}\underline{Y}+\underline{X}\underline{Z} \tag{6}$$

$$(\underline{Y}+\underline{Z})\underline{X} = \underline{Y}\underline{X}+\underline{Z}\underline{X} \tag{7}$$

$$\underline{X}(\underline{Y}\underline{Z}) = (\underline{X}\underline{Y})\underline{Z} \tag{8}$$

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

En traduisant de même la formule (1) 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.

Soient $(L_i)_{1 \leqslant i \leqslant p}$, $(M_j)_{1 \leqslant i \leqslant q}$, $(N_k)_{1 \leqslant k \leqslant r}$ trois partitions des ensembles d'indices L,M,N respectivement. Soit E_i (resp. F_j, G_k) le sous-module de E (resp. F,G) ayant pour base $(a_\lambda)_{\lambda \in L_i}$ (resp. $(b_\mu)_{\mu \in M_j}$, $(c_\nu)_{\nu \in N_k}$) ($1 \leqslant i \leqslant p$, $1 \leqslant j \leqslant q$, $1 \leqslant k \leqslant r$) ; E (resp. F,G) est somme directe des E_i (resp. F_j, G_k). A toute application linéaire u de E dans F , il correspond donc (§ 2,n°4) une famille (u_{ji}) d'applications linéaires, u_{ji} étant une application de E_i dans F_j définie par la condition que pour tout $x \in E_i$, $u_{ji}(x)$ est le composant de $u(x)$ dans F_j . Cette définition montre aussitôt que, si on pose $\underline{X}=\underline{M}(u)$, $\underline{X}_{ji}=\underline{M}(u_{ji})$, la matrice $\underline{X}_{ji}$ n'est autre que la sous-matrice de $\underline{X}$ obtenue en supprimant les lignes d'indice $\lambda \in \complement M_j$ et les colonnes

d'indice $\mu \in \bigcup L_i$; la matrice $\underline{X}$ peut donc s'imaginer comme un "tableau de matrices" à q "lignes" et p "colonnes"

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

Si v est une application linéaire quelconque de F dans E , la matrice $\underline{Y}=\underline{M}(v)$ peut de même être considérée comme un tableau de matrices 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 considère la matrice $\underline{Z}=\underline{YX}$ de l'application composée $w=v\circ u$, elle apparaît de la même manière comme un tableau de r lignes et p colonnes formé des sous-matrices $\underline{Z}_{ki}$ correspondant à la famille (w_{ki}) d'applications linéaires déterminée par w et les partitions (L_i) et (N_k) . Mais, d'après la formule (1) du §2,n°4 , on a $w_{ki} = \sum_{j=1}^{q} v_{kj} \circ u_{ji}$; donc

$$\underline{Z}_{ki} = \sum_{j=1}^{q} \underline{Y}_{kj}\underline{X}_{ji} \tag{9}$$

En d'autres termes, <u>le tableau des $\underline{Z}_{ki}$ s'obtient en formant le "produit" du tableau des $\underline{Y}_{kj}$ par celui des $\underline{X}_{ji}$ comme si ces tableaux étaient des matrices dont les $\underline{Y}_{kj}$ et les $\underline{X}_{ji}$ seraient respectivement les éléments</u> ; c'est ce qu'on appelle effectuer le produit $\underline{YX}$ "<u>par blocs</u>" . Bien entendu, pour qu'une telle opération soit possible, il faut que la partition de l'ensemble des <u>colonnes</u> de $\underline{Y}$ soit <u>la même</u> que la partition de l'ensemble des <u>lignes</u> de $\underline{X}$.

Les formules (2) qui donnent les composantes de $u(x)$ relatives à la base (b_μ), peuvent s'interpréter à l'aide de la notion de produit de matrices,

de la manière suivante : tout élément $x = \sum_{\lambda \in L} a_\lambda \xi_\lambda$ de E détermine une application linéaire $\xi \longrightarrow x\xi$ (que nous avons désigné par θ_x au § 2, n°1) de A_d dans E ; à cette application correspond la <u>matrice à une colonne</u> $\underline{M}(\theta_x) = (\xi_\lambda)_{\lambda \in L}$ (quand on la rapporte à la base de A_d formée de l'élément unité ε, et à la base (a_λ) de E). De même, $y = u(x) = \sum_{\mu \in M} b_\mu \eta_\mu$ détermine l'application linéaire θ_y de A_d dans F, à laquelle correspond de la même manière la matrice à une colonne $\underline{M}(v_y) = (\eta_\mu)_{\mu \in M}$; or on a $u(x\xi) = u(x)\xi$, autrement dit, $\theta_y = u \circ \theta_x$; en traduisant cette relation d'après la formule (4), on obtient les formules (2). Le plus souvent, lorsqu'aucune confusion n'en peut résulter, on identifie l'élément $x \in E$ à la matrice à une colonne $\underline{M}(v_x)$ (formée des <u>composantes</u> de x relatives à la base (a_λ)) ; avec cette convention les formules (2) s'écrivent en une seule formule

$$u(x) = \underline{M}(u).x \qquad (10)$$

5. Matrices carrées.

DEFINITION 3.- <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 ayant n lignes et n colonnes est une matrice d'<u>ordre n</u> .

> Lorsqu'on parle de matrice carrée d'ordre n sans spécifier l'ensemble d'indices (commun) des lignes et des colonnes, il est sous-entendu que cet ensemble est l'intervalle $[1,n]$ de $\mathbb{N}$.

Soit L un ensemble d'indices fini, A un anneau ayant un élément unité ε, E un A-module à droite ayant une base $(a_\lambda)_{\lambda \in L}$ dont L est l'ensemble d'indices. Pour tout <u>endomorphisme</u> u de E, la matrice $\underline{M}(u;(a_\lambda),(a_\lambda))$ de u rapporté à <u>la même base</u> (a_λ) <u>dans les deux sens</u> est une matrice carrée ; on dit que c'est la matrice de u <u>rapporté à la base</u> (a_λ).

D'après la déf.2, l'addition et la multiplication des matrices carrées ayant L comme ensemble d'indices des lignes et des colonnes, définissent sur cet ensemble une structure d'anneau (en raison des formules (6), (7) et (8)), et l'application $u \to \underline{M}(u)$ est un isomorphisme de l'anneau $\mathscr{L}(E)$ des endomorphismes de E sur l'anneau de matrices ainsi défini.

On notera que cette structure est définie sur l'ensemble $A^{L \times L}$, mais est distincte de la structure d'anneau produit des structures d'anneau des facteurs A de cet ensemble. Pour éviter toute confusion, on aura soin de ne pas employer la notation $A^{L \times L}$ pour désigner l'anneau de matrices que l'on vient de définir.

L'élément unité de cet anneau de matrices (qu'on note $\underline{I}_n$ si L est un ensemble à n éléments) correspond à l'automorphisme identique de E, et est donc la matrice $(\delta_{\lambda\mu})$, où $\delta_{\lambda\mu} = 0$ pour $\lambda \neq \mu$, et $\delta_{\lambda\lambda} = \varepsilon$ pour tout $\lambda \in L$.

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 éléments diagonaux, et la famille $(\xi_{\lambda\lambda})_{\lambda \in L}$ est appelée la diagonale de $\underline{X}$. Une matrice dont les éléments autres que les éléments diagonaux sont tous nuls s'appelle matrice diagonale ; la matrice unité $\underline{I}_n$ est une matrice diagonale, ainsi que tout multiple $\rho\underline{I}_n = \underline{I}_n\rho$ de cette matrice par un scalaire ρ (matrice dont tous les éléments diagonaux sont égaux à ρ) ; on notera que pour toute matrice $\underline{X}$ de l'ensemble $A^{L \times M}$, on a $(\rho\underline{I}_n)\underline{X} = \rho\underline{X}$, et pour toute matrice $\underline{Y}$ de l'ensemble $A^{M \times L}$, $\underline{Y}(\rho\underline{I}_n) = \underline{Y}\rho$ (M ensemble d'indices fini quelconque).

Si $\underline{X}$ et $\underline{Y}$ sont deux matrices diagonales, dont (ξ_λ) et (η_λ) sont les diagonales respectives, la somme $\underline{X}+\underline{Y}$ est la matrice diagonale dont la diagonale est $(\xi_\lambda + \eta_\lambda)$, le produit $\underline{X}\underline{Y}$ la matrice diagonale dont la diagonale est $(\xi_\lambda \eta_\lambda)$; les matrices diagonales forment donc un sous-anneau, isomorphe à l'anneau produit A^L, de l'anneau de toutes

les matrices carrées sur A ayant L pour ensemble d'indices des lignes et des colonnes ; les matrices ρI_n forment un sous-anneau, isomorphe à A, de l'anneau des matrices diagonales.

Soit π une permutation quelconque de l'ensemble d'indices L ; il existe un endomorphisme u_π de E et un seul tel que, pour tout $\lambda \in L$, on ait $u_\pi(a_\lambda)=a_{\pi(\lambda)}$ (§ 2, cor.2 de la prop.3). La matrice carrée $M(u_\pi)$ correspondant à cet endomorphisme est telle que, pour tout $\lambda \in L$, dans la colonne d'indice λ, les éléments sont nuls, à l'exception de celui qui se trouve dans la ligne d'indice $\pi(\lambda)$ et qui est égal à ε ; par abus de langage, on dit que la matrice $M(u_\pi)$ est la matrice de la permutation π (relativement à la base (a_λ)). Il est immédiat que les n! matrices correspondant aux permutations de L sont inversibles ; en outre, comme on a $u_{\pi\pi'}=u_\pi \circ u_{\pi'}$ pour deux permutations quelconques π, π' de L, les matrices $M(u_\pi)$ forment un groupe, isomorphe au groupe $\mathfrak{S}_L$ des permutations de L.

Si maintenant $(\rho_\lambda)_{\lambda \in L}$ est une famille quelconque de scalaires, u l'endomorphisme de E déterminé par les relations $u(a_\lambda)=\rho_\lambda a_{\pi(\lambda)}$, on dit que la matrice $M(u)$ est une matrice monomiale ; pour tout λ, les éléments de la colonne d'indice λ sont nuls, à l'exception (éventuelle) de celui qui se trouve dans la ligne d'indice $\pi(\lambda)$, et qui est égal à ρ_λ ; chaque ligne et chaque colonne de $M(u)$ contient donc au plus un élément $\neq 0$, et réciproquement, toute matrice ayant cette propriété est monomiale. On peut encore dire que la matrice monomiale $M(u)$ est le produit de la matrice $M(u_\pi)$ correspondant à la permutation π et de la matrice diagonale ayant (ρ_λ) pour diagonale.

Une autre généralisation de la notion de matrice diagonale est celle de "tableau diagonal de matrices". Considérons une partition $(L_i)_{1 \leqslant i \leqslant p}$ de l'ensemble d'indices L, et mettons toute matrice carrée ayant L comme ensemble d'indices des lignes et

et des colonnes, 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

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

Chacune des matrices X_{1i} est une matrice carrée ayant L_i pour ensembles d'indices des lignes et des colonnes.

Cela étant, on dira que le tableau précédent est un tableau diagonal si toutes les matrices X_{ij} telles que $i \neq j$ sont nulles. Le produit "par blocs" ($n^o 4$) de deux matrices mises sous la forme précédente montre que celles pour lesquelles le tableau correspondant est un tableau diagonal forment un anneau ; si E_i est le sous-module de E ayant pour base $(e_\lambda)_{\lambda \in L_i}$, on voit aisément que cet anneau est isomorphe à l'anneau produit $\prod_{i=1}^{p} \mathcal{L}(E_i)$ des anneaux des endomorphismes des E_i.

Remarque.- On aura soin de noter qu'une matrice sur A dont les ensembles L,M des indices des lignes et des colonnes ont même nombre d'éléments, mais ne sont pas identiques, ne doit pas être considérée comme une matrice carrée ; en particulier, le produit de deux telles matrices n'est pas défini. Bien entendu, à chaque application biunivoque de M sur L correspond ($n^o 1$) une application biunivoque de l'ensemble $A^{L \times L}$ des matrices carrées ayant L pour ensemble d'indices des lignes et des colonnes, sur l'ensemble $A^{L \times M}$; et on peut, si on veut, transporter par cette application à l'ensemble $A^{L \times M}$ la structure d'anneau défini sur l'ensemble des matrices carrées ;

mais à deux applications biunivoques distinctes de M sur L correspondront ainsi deux structures d'anneau distinctes sur l'ensemble $A^{L \times M}$.

6. Transposée d'une matrice.

Soient E et F deux A-modules unitaires à droite admettant des bases finies $(a_\lambda)_{\lambda \in L}$, $(b_\mu)_{\mu \in M}$. Les duals respectifs E^*, F^* de E et F sont des A-modules à gauche ; ils peuvent être considérés comme des modules à droite sur l'anneau A^0, opposé de A (§ 1, n°1) ; les bases duales (§ 4, n°4) (a'_λ), (b'_μ) de (a_λ) et (b_μ) respectivement, sont encore des bases de E^* et F^* quand on considère ces derniers comme A^0-modules à droite. Soit alors u une application linéaire de E dans F, $M(u)=(\alpha_{\mu\lambda})_{(\mu,\lambda) \in M \times L}$ la matrice de u, rapportée aux bases (a_λ) et (b_μ) ; proposons-nous de chercher la matrice $M({}^t u)$ de la transposée ${}^t u$ (§ 4, n°7) rapportée aux bases duales (b'_μ) et (a'_λ).

DEFINITION 4.- Etant donnée une matrice $X=(\alpha_{\mu\lambda})_{(\mu,\lambda) \in M \times L}$ sur un anneau A, ayant M pour ensemble d'indices des lignes, L pour ensemble d'indices des colonnes, on appelle transposée de X et on note ${}^t X$ la matrice $(\beta_{\lambda\mu})_{(\lambda,\mu) \in L \times M}$ sur l'anneau A^0 opposé de A, ayant L pour ensemble d'indices de lignes, M pour ensemble d'indices des colonnes, et définie par les relations $\beta_{\lambda\mu} = \alpha_{\mu\lambda}$ pour tout couple (λ, μ).

On dit encore que ${}^t X$ se déduit de X par échange des lignes et des colonnes.

Cela étant :

PROPOSITION 1.- La matrice de la transposée ${}^t u$, rapportée aux bases (b'_μ) et (a'_λ), est égale à la transposée de la matrice de u, rapportée aux bases (a_λ) et (b_μ).

En effet, soit $\underline{M}({}^t u)=(\beta_{\lambda\mu})_{(\lambda,\mu)\in L\times M}$ la matrice de ${}^t u$, rapportée aux bases (b'_μ) et (a'_λ) ; par définition, $\beta_{\lambda\mu}$ est la composante d'indice de ${}^t u(b'_\mu)$ dans E, c'est-à-dire $\langle a_\lambda, {}^t u(b'_\mu)\rangle = \langle u(a_\lambda), b'_\mu\rangle$ (§ 4, formule (13)) ; mais $\langle u(a_\lambda), b'_\mu\rangle$ n'est autre que la composante d'indice μ de $u(a_\lambda)$ dans F, c'est-à-dire $\alpha_{\mu\lambda}$.

Il est immédiat que ${}^t({}^t\underline{X})=\underline{X}$. D'après les formules (14) et (16) du § 4, on a

$$(11) \qquad {}^t(\underline{X}+\underline{Y}) = {}^t\underline{X} + {}^t\underline{Y}$$

$$(12) \qquad {}^t(\underline{XZ}) = {}^t\underline{Z} \cdot {}^t\underline{X}$$

chaque fois que les matrices $\underline{X}+\underline{Y}$ et $\underline{XZ}$ sont définies. Il faut naturellement se souvenir qu'au second membre de (12), les produits d'éléments de ${}^t\underline{Z}$ par des éléments de ${}^t\underline{X}$ doivent être pris dans l'anneau A^o.

Appliquons en particulier la prop.1 à une forme linéaire x' sur E. Sa transposée n'est autre que l'application linéaire de A_d^o dans E^* (considéré comme A^o-module à droite), que nous avons désigné ci-dessus par $\theta_{x'}$ (n°4). La transposée de la matrice à une ligne $\underline{M}(x')$ (x' étant rapportée à la base (a_λ) et à la base de A_d formée du seul élément ε), est donc la matrice à une colonne dont les éléments sont les composantes ξ'_λ de x' relatives à la base (a'_λ) considérées comme éléments de A^o (cela résulte aussi directement de la définition de $\underline{M}(x')$ et de celle des bases duales) ; conformément à la convention posée au n°4, on identifie cette matrice à une colonne au vecteur x' de E^*, et par suite, la relation (10) donne, pour $u=x'$

$$(13) \qquad \langle x, x'\rangle = {}^t x' . x$$

Soit u une application linéaire de E dans F ; pour toute forme linéaire $y' \in F^*$, on a, d'après (10) et la prop.1, ${}^t u(y') = \underline{M}({}^t u).y' = {}^t\underline{M}(u).y'$; les relations (12) et (13) montrent donc que

$$(14) \qquad \langle x, {}^t u(y')\rangle = {}^t y' . \underline{M}(u) . x$$

et la formule fondamentale (13) du § 4 prend donc l'aspect de la règle d'associativité du produit de matrices

$$ {}^t y' . (\underline{M}(u).x) = ({}^t y' . \underline{M}(u)).x \quad . $$

Les matrices carrées <u>inversibles</u> sur A ayant L pour ensemble d'indices des lignes et des colonnes correspondent aux <u>automorphismes</u> de E . Pour tout automorphisme u de E , l'application <u>contragrédiente</u> $\overset{\vee}{u}$ (§ 4, n° 7) est un automorphisme du dual E^* (considéré comme A^0-module à droite), réciproque de la transposée ${}^t u$ de u , et identique à la transposée de l'automorphisme réciproque de u ; si $\underline{X}=\underline{M}(u)$, on a donc, d'après la prop. 1, $\underline{M}(\overset{\vee}{u})=({}^t\underline{X})^{-1}={}^t(\underline{X}^{-1})$, ce qui permet de noter cette matrice ${}^t\underline{X}^{-1}$ sans ambiguité ; on l'appelle la <u>contragrédiente</u> de la matrice inversible $\underline{X}$ (on la note aussi parfois $\overset{\vee}{\underline{X}}$) . D'après (12) , si $\underline{X}$ et $\underline{Y}$ sont deux matrices carrées inversibles sur l'anneau A ayant même ensemble d'indices des lignes et des colonnes, on a

$$ (15) \qquad {}^t(\underline{XY})^{-1}=({}^t\underline{X}^{-1})({}^t\underline{Y}^{-1}) $$

(les produits figurant dans la matrice du second membre étant pris <u>dans l'anneau</u> A^0) .

7. Matrices sur un corps.

Les matrices à m lignes et n colonnes sur un corps K correspondent biunivoquement aux applications linéaires de l'espace vectoriel à droite $E=K^n_d$ dans l'espace vectoriel à droite $F=K^m_d$, rapportées aux bases canoniques de ces deux espaces. Par définition, le <u>rang</u> d'une telle matrice $\underline{X}$ est le rang de l'application linéaire u qui lui correspond ; comme c'est la dimension du sous-espace u(E) de F , il revient au même (en identifiant les colonnes de $\underline{X}$ aux images par u de la base canonique de E) de donner la définition suivante :

DEFINITION 5.- Etant donnée une matrice X à m lignes et n colonnes sur un corps K , on appelle rang de X par rapport à K et on note $\rho(X)$, la dimension du sous-espace de K_d^m engendré par les n colonnes de X .

On peut dire aussi que le rang de X est le nombre maximum de colonnes de X linéairement indépendantes. D'après la déf.5 , on a $\rho(X) \leqslant \mathrm{Min}(m,n)$; pour toute sous-matrice Y de X , on a $\rho(Y) \leqslant \rho(X)$.

La notion de rang d'une matrice ne dépend qu'en apparence du corps auquel on considère qu'appartiennent les éléments de la matrice. En effet :

PROPOSITION 2.- Si les éléments d'une matrice X à m lignes et n colonnes appartiennent à un sous-corps K_o d'un corps K , le rang de X par rapport à K_o est égal au rang de X par rapport à K .

En effet, les colonnes de X appartiennent au sous-espace H_o par rapport à K_o , engendré par la base canonique de l'espace K_d^m (par rapport à K) ; la proposition résulte donc de la prop.2 du § 5 .

La prop.1 ci-dessus et le th.4 du § 4 prouvent que :

PROPOSITION 3.- Le rang d'une matrice X sur un corps K est égal au rang de sa transposée ${}^tX$.

Les matrices carrées d'ordre n sur le corps K correspondent aux endomorphismes de $E=K_d^n$ (en prenant $[1,n]$ comme ensemble d'indices des lignes et des colonnes) ; elles forment un anneau isomorphe à l'anneau $\mathcal{L}(E)$ des endomorphismes de E . Aux automorphismes de E correspondent les matrices carrées inversibles ; par suite (§ 3, cor. de la prop.4) :

PROPOSITION 4.- Pour qu'une matrice carrée d'ordre n sur un corps K soit inversible, il faut et il suffit qu'elle soit de rang n .

8. Application des matrices 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

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

Soit (e_i) la base canonique de $E=A_d^m$; si on pose $a_j = \sum_{i=1}^{m} e_i a_{ij}$, $b = \sum_{i=1}^{m} e_i \beta_i$, on sait (§ 4, n°6) que le système (16) équivaut à l'équation

(17) $$\sum_{j=1}^{n} a_j\,\xi_j = b$$

La matrice $A=(a_{ij})$ à m lignes et n colonnes est dite <u>la matrice du système</u> (16) ; dire que le système (16) a une solution revient à dire que la matrice à une colonne $b=(\beta_i)$ est une <u>combinaison linéaire</u> des n colonnes de la matrice A .

Lorsqu'il s'agit d'un système (16) sur un <u>corps</u> K , l'interprétation précédente, et la définition du rang d'une matrice, prouvent que :

PROPOSITION 5.- <u>Pour qu'un système</u> (16) <u>d'équations linéaires sur un corps</u> K <u>ait une solution, il faut et il suffit que la matrice</u> B <u>obtenue en bordant la matrice</u> $A=(a_{ij})$ <u>du système par une</u> $(n+1)^{\text{ème}}$ <u>colonne</u> (β_i) <u>formée des seconds membres de</u> (16), <u>ait même rang que la matrice</u> A .

Cette condition est toujours remplie lorsque $m=n$, et que A est une matrice <u>inversible</u>, c'est-à-dire de rang n . Si on remarque qu'en désignant par x la matrice à une colonne $(\xi_j)_{1 \leqslant j \leqslant n}$, l'équation (17) s'écrit aussi $A.x=b$, on voit que dans ce cas, <u>l'unique</u> solution est donnée par la formule $x=A^{-1}.b$.

<u>9. Changements de bases.</u>

PROPOSITION 6.- <u>Soit</u> E <u>un</u> A-<u>module à droite unitaire, ayant une base</u> $(a_i)_{1 \leqslant i \leqslant n}$ <u>de n éléments. Pour qu'une famille de n éléments</u> $\overline{a}_i = \sum_{j=1}^{n} a_j a_{ji}$ $(1 \leqslant i \leqslant n)$ <u>de</u> E <u>soit une base de</u> E , <u>il faut et il suffit que la matrice carrée</u> $P=(a_{ji})$ <u>d'ordre n soit inversible.</u>

En effet, P n'est autre que la matrice de l'endomorphisme u de E défini par $u(a_i)=\overline{a}_i$ $(1 \leqslant i \leqslant n)$, rapporté à la base (a_i) . Or, pour que $(\overline{a}_i)$ soit une base de E , il faut et il suffit que u soit un automorphisme de E , d'où la proposition.

On dit que la matrice inversible P est *la matrice de passage de la base* (a_i) *à la base* $(\overline{a}_i)$. On peut aussi l'interpréter comme la matrice de l'application *identique* φ de E sur lui-même, rapportée aux bases $(\overline{a}_i)$ et (a_i) (*dans cet ordre*) ; la formule (4) montre alors aussitôt que la matrice de passage *de la base* $(\overline{a}_i)$ *à la base* (a_i) n'est autre que l'*inverse* P^{-1} de P.

Soient (a'_i), $(\overline{a}'_i)$ les *bases duales* de (a_i) et $(\overline{a}_i)$ respectivement dans le dual E^* de E (considéré comme A^0-module à droite) ; comme la transposée de l'application identique de E est l'application identique de E^*, la prop.1 montre que la matrice de l'application identique de E^*, rapportée aux bases (a'_i) et $(\overline{a}'_i)$ (dans cet ordre) est la transposée de la matrice de l'application identique de E, rapportée aux bases $(\overline{a}_i)$ et (a_i) ; cela signifie donc que la matrice de passage de la base (a'_i) à la base $(\overline{a}'_i)$ est la *contragrédiente* ${}^tP^{-1}$ de la matrice de passage P de la base (a_i) à la base $(\overline{a}_i)$.

PROPOSITION 7.- *Soient* E *et* F *deux* A*-modules à droite unitaires ayant des bases respectives* $(a_i)_{1 \leqslant i \leqslant n}$ *et* $(b_j)_{1 \leqslant j \leqslant m}$ *de* n *et* m *éléments. Soit* u *une application linéaire de* E *dans* F, U *la matrice* (*à* m *lignes et* n *colonnes*) *de* u *rapportée aux bases* (a_i) *et* (b_j). *Si* $(\overline{a}_i)_{1 \leqslant i \leqslant n}$ *est une deuxième base de* E, $(\overline{b}_j)_{1 \leqslant j \leqslant m}$ *une* $m \times n$ *deuxième base de* F, P *la matrice de passage de* (a_i) *à* $(\overline{a}_i)$, Q *la matrice de passage de* (b_j) *à* $(\overline{b}_j)$, U' *la matrice de* u *rapportée aux bases* $(\overline{a}_i)$ *et* $(\overline{b}_j)$, *on a*

$$U' = Q^{-1}UP \qquad (18)$$

En effet, on peut écrire $u = \psi \circ u \circ \varphi$, où φ est l'application identique de E, ψ l'application identique de F. Si, dans le second membre de cette relation, on rapporte φ à $(\overline{a}_i)$ et (a_i), u à (a_i) et (b_j), ψ à (b_j) et $(\overline{b}_j)$, la formule (18) résulte aussitôt de (4).

COROLLAIRE 1.- Si u est un endomorphisme de E , U et U' les matrices de u rapporté respectivement aux bases (a_i) et $(\overline{a}_i)$, on a

(19) $$U' = P^{-1}UP \quad .$$

COROLLAIRE 2.- Si $X = (\xi_i)$ et $\overline{X} = (\overline{\xi}_i)$ sont les matrices à une colonne formées des composantes d'un élément $x \in E$ relativement aux bases (a_i) et $(\overline{a}_i)$ respectivement, on a

(20) $$X = P.\overline{X}$$

Il suffit d'appliquer la prop.7, à l'application θ_x ($n^o 4$) de A_d dans E , rapportée d'une part aux bases $\{\varepsilon\}$ et (a_i) , d'autre part aux bases $\{\varepsilon\}$ et $(\overline{a}_i)$.

La formule (20) équivaut à

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

qu'on appelle formules du changement de coordonnées ; on observera qu'elles expriment les composantes de x relativement à la base (a_i) en fonction des composantes de x relativement à la base $(\overline{a}_i)$, et des éléments de P , c'est-à-dire des composantes de la base $(\overline{a}_i)$ relativement à la base (a_i) : on dit que les composantes d'un élément de E se transforment de façon contravariante (ou contrarédiente)par un changement de base.

Soient maintenant $X' = (\xi'_i)$, $\overline{X}' = (\overline{\xi}'_i)$ les matrices à une colonne (à éléments dans A^o) formées des composantes d'une forme linéaire $x' \in E^*$ relatives respectivement aux bases (a'_i) et $(\overline{a}'_i)$, duales de (a_i) et $(\overline{a}_i)$; comme la matrice de passage de (a'_i) à $(\overline{a}'_i)$ est ${}^tP^{-1}$, on a, d'après (20) , $X' = {}^tP^{-1}\overline{X}'$, ce qui s'écrit encore

(22) $$ {}^t\overline{X}' = {}^tX'.P$$

ou

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

On dit que les composantes d'une forme linéaire sur E se transforment de façon covariante (ou cocontrarédiente) par changement de base.

10. matrices équivalentes.

DEFINITION 6.- On dit que deux matrices X, 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

(24) $$X' = PXQ \quad .$$

Avec cette définition, la prop.7 peut s'énoncer en disant que, lorsqu'on change de base dans deux A-modules unitaires E et F (ayant des bases finies), la matrice d'une application linéaire u de E dans F , rapportée aux nouvelles bases, est équivalente à la matrice de u , rapportée aux anciennes bases.

Une autre interprétation consiste à considérer les applications linéaires u, u' de E dans F telles que X et X' soient les matrices de ces applications, rapportées à deux bases fixes $(a_i)_{1 \leqslant i \leqslant n}$ et $(b_j)_{1 \leqslant j \leqslant m}$ de E et F ; si φ et ψ sont les automorphismes de E et F dont les matrices sont Q et P respectivement (quand on rapporte ces automorphismes aux bases (a_i) et (b_j) respectivement), la relation (24) équivaut à $u' = \psi \circ u \circ \varphi$.

Avec l'une ou l'autre interprétation, il est clair que la relation "X et 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 $X=(\xi_{ij})$ et $X'=(\xi'_{ij})$, 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 l'on ait pour tout couple d'indices (i,j), $\xi'_{ij} = \xi_{\sigma(i),j}$ (on dit encore que X' s'obtient en effectuant la permutation σ sur les lignes de X).

Les matrices X et X' sont alors équivalentes, car on a $X' = XK$, où P est la matrice correspondant à la permutation σ^{-1} des indices de la base (b_j) de F (cf. n°5).

On dit de même que X et X' ne diffèrent que par l'ordre des colonnes, s'il existe une permutation τ de $[1,n]$ telle que $\xi'_{ij} = \xi_{i,\tau(j)}$ pour tout couple d'indices. Comme les transposées de X et X' ne diffèrent alors que par l'ordre des lignes, elles sont équivalentes, donc il en est de même de X et X' (de façon plus précise, on a $X' = XQ$, où Q est la matrice correspondant à la permutation des indices de la base (a_i) de E).

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 que X' se déduit de X en ajoutant à la colonne d'indice j de X la colonne d'indice k multipliée à droite par μ. Dans ce cas, X et X' sont encore équivalentes : en effet, avec la seconde interpétation considérée ci-dessus, on a $u'(a_j) = u(a_j) + u(a_k)\mu = u(a_j + a_k\mu)$, donc $u' = u \circ \varphi$, où φ est l'automorphisme de E défini par $\varphi(a_j) = a_j + a_k\mu$, $\varphi(a_h) = a_h$ pour tout $h \neq j$ (il s'agit bien d'un automorphisme, car l'endomorphisme φ' défini par $\varphi'(a_j) = a_j - a_k\mu$, $\varphi'(a_h) = a_h$ pour $h \neq j$, est réciproque de φ).

On voit de même que X et X' sont équivalentes lorsque X' se déduit de X en ajoutant à une ligne d'indice i de X, une ligne d'indice $h \neq i$, multipliée à gauche par un élément quelconque $\lambda \in A$.

PROPOSITION 8.- *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, d'après la seconde interprétation donnée ci-dessus de la notion d'équivalence : si u et u' sont deux applications linéaires de l'espace vectoriel E dans l'espace vectoriel E dans l'espace vectoriel F , φ un automorphisme de E , ψ un automorphisme de F , tels que $u' = \psi \circ u \circ \varphi$, u(E) et u'(E)= ψ(u(E)) ont même dimension.

Pour voir que la condition est suffisante, nous allons voir que toute matrice $\underline{X}$ de rang $r \leqslant \mathrm{Min}(m,n)$ est équivalente à la matrice

$$\underline{U} = \begin{pmatrix} \underline{I}_r & 0 \\ 0 & 0 \end{pmatrix} \tag{25}$$

dite matrice canonique de rang r à m lignes et n colonnes sur K (le second membre de (25) étant un tableau de matrices correspondant à la partition de $[1,m]$ en $[1,r]$ et $[r+1,m]$, et à la partition de $[1,n]$ en $[1,r]$ et $[r+1,n]$) .

Pour cela, nous montrerons que si $\underline{X}$ est la matrice d'une application u de rang r de E dans F , rapportée à deux bases (a_i) et (b_j) , il existe deux bases $(\overline{a}_i)$ et $(\overline{b}_j)$ de E et F respectivement, telles que $\underline{U}$ soit la matrice de u rapportée à ces nouvelles bases. En effet, $H = {}^{-1}u(0)$ est un sous-espace de dimension n-r de E ; soit G un supplémentaire de H dans E , de dimension r ; prenons une base $(\overline{a}_i)$ de E telle que $(\overline{a}_i)_{1 \leqslant i \leqslant r}$ soit une base de G , $(\overline{a}_i)_{r+1 \leqslant i \leqslant n}$ une base de H (§ 3, prop.3) Alors les vecteurs $u(\overline{a}_j)$ forment une base de u(E) pour $1 \leqslant j \leqslant r$; il existe donc une base $(\overline{b}_j)$ de F telle que $\overline{b}_j = u(\overline{a}_j)$ pour $1 \leqslant j \leqslant r$ (§ 3, prop.3). Il est clair que les bases $(\overline{a}_i)$ et $(\overline{b}_j)$ répondent bien à la question.

11. Matrices carrées semblables.

DEFINITION 7.- On dit que deux matrices carrées X,X' d'ordre n sur un anneau A ayant un élément unité, sont semblables, s'il existe une matrice carrée inversible P d'ordre n , telle que

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

Avec cette définition, on peut énoncer le cor.1 de la prop.7 en disant que, lorsqu'on change de base dans un A-module unitaire E (ayant une base finie), la matrice d'un endomorphisme u de E rapporté à la nouvelle base, est semblable à la matrice de u , rapporté à l'ancienne base.

Une autre interprétation consiste à considérer les endomorphismes u et u' et l'automorphisme φ de E tels que $\underline{X}$, $\underline{X}'$ et P soient les matrices de ces endomorphismes rapportés à une base fixe $(a_i)_{1 \leqslant i \leqslant n}$; la relation (26) 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) Deux matrices carrées qui ne diffèrent que par l'ordre des lignes (ou l'ordre des colonnes) sont équivalentes, mais non semblables en général. On obtient une matrice semblable à une matrice carrée $\underline{X} = (\xi_{ij})$ en effectuant la même permutation σ sur les lignes et les colonnes, c'est-à-dire en considérant la matrice $\underline{X}' = (\xi'_{ij})$ où $\xi'_{ij} = \xi_{\sigma(i),\sigma(j)}$ pour tout couple d'indices: en effet, si $\underline{P}$ est la matrice correspondant à la permutation σ des indices de la base (a_i), on voit aisément que $\underline{X}' = \underline{P}^{-1}\underline{X}\underline{P}$.

2) Deux matrices semblables sur un même corps K ont évidemment même rang, puisqu'elles sont équivalentes (prop.8) . Mais ici cette condition nécessaire n'est plus suffisante pour que deux matrices carrées sur K soient semblables ; au chap.V , nous donnerons des conditions nécessaires et suffisantes lorsque K est un corps commutatif .

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

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

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 $\underline{X}'_i = \underline{P}_i \underline{X}_i \underline{P}_i^{-1}$ pour $1 \leqslant i \leqslant p$, 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" (n°4)

12. Matrice d'une application semi-linéaire.

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

Soit E un A-module à droite unitaire, ayant une base finie $(a_\lambda)_{\lambda \in L}$, F un B-module à droite unitaire ayant une base $(b_\mu)_{\mu \in M}$. Soit u une application semi-linéaire de E dans F , relative à l'isomorphisme σ (§ 2, n°6) ; si $u(a_\lambda) = \sum_{\mu \in M} b_\mu a_{\mu\lambda}$, les $a_{\mu\lambda}$ sont bien déterminés par la donnée de u , et inversement déterminent les $u(a_\lambda)$, donc u ; on dit que la matrice $(a_{\mu\lambda})_{(\mu,\lambda) \in M \times L}$ est la matrice de u , rapportée aux bases (a_λ) et (b_μ), et on la note encore $\underline{M}(u;(a_\lambda),(b_\mu))$ ou $\underline{M}(u)$.

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

(27) $$u(x) = \underline{u}(u).x^\sigma$$

Soit C un anneau isomorphe à A et $\beta \to \beta^\tau$ un isomorphisme de B sur C, G un C-module à droite unitaire, ayant une base finie $(c_\nu)_{\nu \in N}$. Soit v une application semi-linéaire de F dans G, relative à l'isomorphisme τ ; si $\underline{U}$ est la matrice de u, rapportée aux bases (a_λ) et (b_μ), $\underline{V}$ la matrice de v, rapportée aux bases (b_μ) et (c_ν), la matrice de $v \circ u$, rapportée aux bases (a_μ) et (c_ν), est égale à $\underline{V}.\underline{U}^\tau$.

Soient (a'_λ) et (b'_μ) les <u>bases duales</u> de (a_λ) et (b_μ) dans E^* et F^* respectivement ; on sait (§4, n°7) que la <u>transposée</u> ${}^t u$ de u est une application semi-linéaire de F^* dans E^*, relative à l'isomorphisme σ^{-1} ; si $\underline{U}$ est la matrice de u, rapportée aux bases (a_λ) et (b_μ), la matrice de ${}^t u$, rapportée aux bases (b'_μ) et (a'_λ) est égale à ${}^t(\underline{U}^{\sigma^{-1}})$.

Enfin, si $(\overline{a}_\lambda)_{\lambda \in L}$, $(\overline{b}_\mu)_{\mu \in M}$ sont deux bases de E et F respectivement, $\underline{P}$ la matrice de passage de (a_λ) à $(\overline{a}_\lambda)$, $\underline{Q}$ la matrice de passage de (b_μ) à $(\overline{b}_\mu)$, la matrice de u, rapportée aux bases $(\overline{a}_\lambda)$ et $(\overline{b}_\mu)$, est égale à $\underline{Q}^{-1}\underline{U}\underline{P}^\sigma$.

<u>Exercices</u>.- 1) Soient E un A-module à droite unitaire, A_r l'anneau des matrices carrées d'ordre r sur l'anneau A. Sur l'ensemble E^r, on définit une loi de composition externe, dont A_r est l'ensemble d'opérateurs, en désignant par x.P, pour tout élément $x=(x_i)_{1 \leqslant i \leqslant r}$ de E^r, et toute matrice $\underline{P}=(a_{ij})$ de A_r, l'élément $y=(y_i)$ de E^r tel que

$$y_i = \sum_{j=1}^{r} x_j a_{ji} \qquad (1 \leqslant i \leqslant r)$$

Cette loi externe et la loi de groupe additif de E^r définissent sur cet ensemble une structure de module à droite par rapport à l'anneau A_r . Montrer que, pour que le A-module E admette un système de r générateurs, il faut et il suffit que le A_r-module E^r soit monogène.

2) 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 $(\underline{X}_{ij})$ n'a que des zéros au-dessus de la diagonale (c'est-à-dire que $\underline{X}_{ij}=0$ pour $i > j$) forment un sous-anneau de l'anneau des matrices carrées d'ordre n sur A . Comment peut-on caractériser les endomorphismes auxquels correspondent ces matrices ?

b) Si chacune des sous-matrices carrées $\underline{X}_{ii}$ $(1 \leqslant i \leqslant p)$ 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.

3) Soit $\underline{X}$ une matrice à m lignes et n colonnes sur un corps des sous-matrices de $\underline{X}$ ayant un nombre égal de lignes et de colonnes (soit $\rho(\underline{X})=r$; si $a_1, a_2, \ldots, a_r$ sont r colonnes de $\underline{X}$ formant un système libre dans K_d^m , et si on forme une base de K_d^m avec ces r vecteurs et m-r vecteurs de la base canonique (e_i), montrer que les composantes de $a_1, \ldots, a_r$ sur les r autres vecteurs de la base canonique forment une matrice de rang r).

4) Soit $\underline{X}$ une matrice à m lignes et n colonnes sur un corps K ; si r est le rang de $\underline{X}$, montrer que le rang d'une sous-matrice à m lignes et s colonnes formée en supprimant n-s colonnes de $\underline{X}$, a un rang $\geqslant r + s - m$.

5) Soit $X=(\alpha_{ij})$ une matrice à m lignes et n colonnes sur un corps K. Pour que X soit de rang 1, il faut et il suffit qu'il existe dans K une famille $(\lambda_i)_{1\leqslant i\leqslant m}$ de m éléments non tous nuls et une famille $(\mu_j)_{1\leqslant j\leqslant n}$ de n éléments non tous nuls, telles que $\alpha_{ij}=\lambda_i\mu_j$ pour tout couple d'indices.

6) Soit E un espace vectoriel à droite sur un corps K, H un hyperplan de E. Tout endomorphisme u de E, laissant invariant chacun des éléments de H, donne, par passage au quotient, un endomorphisme de l'espace quotient E/H de dimension 1, endomorphisme qui est donc de la forme $\dot{x}\rightarrow\dot{x}\,\mu(\dot{x})$, où $\mu(\dot{x}\lambda)=\lambda^{-1}\mu(\dot{x})\lambda$. Un automorphisme u pour lequel l'automorphisme correspondant de E/H est l'application identique, est appelé une transvection. Dans le cas contraire, on dit que c'est une dilatation ; l'ensemble des éléments $\mu(\dot{x})$, qui est une classe d'éléments conjugués (chap.I, § 7, n°5) dans le groupe multiplicatif K^* des éléments $\neq 0$ de K, est dite la classe de la dilatation.

a) Montrer que pour toute dilatation, il existe une droite supplémentaire de H et une seule, invariante par la dilatation.

b) Soit φ une forme linéaire telle que $H=\varphi^{-1}(0)$; montrer que pour toute transvection u, il existe un vecteur $a\in H$ bien déterminé tel que $u(x)=x+a\varphi(x)$. Si $\Gamma(E,H)$ est le groupe de tous les automorphismes de E laissant invariant chaque élément de H, montrer que les transvections (relatives à H) forment un sous-groupe abélien distingué $\Theta(E,H)$ de $\Gamma(E,H)$, isomorphe au groupe additif H ; le groupe quotient $\Gamma(E,H)/\Theta(E,H)$ est isomorphe à K^*.

Si E est de dimension finie, pour toute transvection u, il existe une base de E telle que la matrice de u, rapportée à cette base, ait tous les éléments diagonaux égaux à 1, et au plus un autre élément $\neq 0$.

c) montrer que le centralisateur (chap.I, § 6, exerc.13) du groupe Ⓗ (E,H) dans le groupe GL(E) des automorphismes de E est le composé Z(E) Ⓗ(E,H) des groupes permutables Ⓗ (E,H) et Z(E) (Z(E) désignant le centre de GL(E), groupe des homothéties centrales (§ 2, exerc.4)). Les seuls automorphismes appartenant à ce centralisateur et laissant invariant au moins un élément $x \neq 0$ de E sont les transvections du groupe Ⓗ (E,H) .

Le normalisateur (chap.I, § 6, exerc.13) de Ⓗ (E,H) dans GL(E) est le sous-groupe des automorphismes laissant invariant H .

7) On désigne par F(E) le sous-groupe de GL(E) formé des automorphismes u tels que l'ensemble des éléments x invariants par u soit un sous-espace ayant un supplémentaire de dimension finie (F(E)=GL(E) si E est de dimension finie). On désigne par C(E) le sous-groupe distingué de F(E) engendré par toutes les transvections.

a) Si E est de dimension > 1 , pour tout couple de vecteurs x,y non nuls de E , il existe une transvection u telle que $u(x)=y$ (autrement dit, le groupe C(E) opère transitivement dans le complémentaire de $\{0\}$ dans E) .

b) Soient V et W deux hyperplans distincts, $\dot{x}_o = x_o + V$ une classe mod.V distincte de V , $\dot{y}_o = y_o + W$ une classe mod.W distincte de W . Montrer que si E est de dimension > 1 , il existe une transvection transformant V en W et $\dot{x}_o$ en $\dot{y}_o$.

c) Montrer que, si E est de dimension > 1 , deux transvections quelconques (distinctes de l'application identique) sont conjuguées (chap.I, § 7, n°5) dans le groupe F(E) . Si E est de dimension > 2, deux transvections quelconques distinctes de l'application identique sont conjuguées dans le groupe C(E) (se ramener au cas où les hyperplans correspondant aux deux transvections sont identiques).

Si E est de dimension 2 , pour que deux transvections quelconques soient conjuguées dans C(E), il faut et il suffit que le sous-groupe Q de K^* engendré par les carrés des éléments de K^* soit identique à K^* (si u est une transvection, a un élément de E non invariant par u, et b=u(a)-a , montrer que pour toute transvection u' conjuguée de u dans C(E) , on a $u'(a)-a = a\lambda + b\mu$, où $\mu \in Q$).

d) Pour que deux dilatations u,u' soient conjuguées par rapport au groupe C(E) (c'est-à-dire qu'il existe un automorphisme $v \in C(E)$ tel que $u'=vuv^{-1}$), il faut et il suffit que les classes (exerc.6) de ces dilatations soient identiques (utiliser b)). En déduire que si la classe d'une dilatation est contenue dans le groupe des commutateurs Γ du groupe K^*, cette dilatation appartient au groupe C(E) .

8) a) Montrer que tout automorphisme u appartenant à F(E) est produit d'un automorphisme appartenant à C(E) et d'une dilatation dont l'hyperplan d'éléments invariants est un hyperplan fixe H_0 (procéder par récurrence sur la dimension du supplémentaire du sous-espace des éléments invariants par u , et utiliser l'exerc. 7d)).

b) Montrer que C(E) contient le groupe des commutateurs de F(E), et est identique à ce groupe sauf lorsque $K=\mathbb{Z}/(2)$ et que E est de dimension 2 sur K (pour montrer que C(E) contient le groupe des commutateurs de F(E), utiliser a) et l'exerc. 7d) ; pour voir que C(E) est contenu dans le groupe des commutateurs, montrer que, dans toute représentation de F(E) sur un groupe abélien, l'image de toute transvection est l'élément neutre, en utilisant les exerc.6b) et 7 c)) .

9) si E est de dimension >2 , montrer que tout sous-groupe distingué de GL(E), non contenu dans le centre Z(E) , contient le

le groupe des commutateurs $C(E)$, et que tout sous-groupe distingué de $C(E)$, non contenu dans $Z(E)$, est identique à $C(E)$ (si G est un sous-groupe distingué de $GL(E)$ u un automorphisme contenu dans G et n'appartenant pas à $Z(E)$, montrer qu'il existe une transvection v telle que $w=v^{-1}u^{-1}vu$ laisse invariant un hyperplan H, et n'appartienne pas à $Z(E)$; en déduire que, ou bien w est une transvection, ou bien il existe une transvection t laissant invariants les éléments de H et telle que $twt^{-1}w^{-1}$ n'appartienne pas à $Z(E)$; conclure à l'aide de l'exerc. 7c) ; raisonnement analogue pour les sous-groupes distingués de $C(E)$).

10) Soient $\underline{X}$ et $\underline{Y}$ deux matrices à m lignes et n colonnes sur un corps K ; s'il existe deux matrices carrées $\underline{P},\underline{P}_1$ d'ordre m et deux matrices carrées $\underline{Q}$, $\underline{Q}_1$ d'ordre n telles que $\underline{Y}=\underline{PXQ}$ et $\underline{X}=\underline{P}_1\underline{YQ}_1$, $\underline{X}$ et Y sont équivalentes (utiliser la prop.8).

11) Soient $\underline{X},\underline{X}'$, $\underline{Y},\underline{Y}'$, quatre matrices carrées d'ordre n sur un anneau A ayant un élément unité ; on suppose en outre que $\underline{X}$ soit inversible. Pour qu'il existe deux matrices carrées inversibles d'ordre n, $\underline{P}$ et $\underline{Q}$, 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.

§ 7. Algèbres.

1. Définition d'une algèbre.

DEFINITION 1.- *Etant donné un anneau commutatif A, ayant un élément unité ε, on appelle algèbre (ou système hypercomplexe) par rapport à A (ou algèbre sur A), tout 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 un sous-anneau A de son centre (ayant même élément unité que E), le composé d'un opérateur $z\in A$ et d'un élément $x\in E$ étant le produit zx ($=xz$) pour la multiplication dans l'anneau E .

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

Sur une algèbre E , la structure d'anneau à opérateurs opposée à celle de E est encore une structure d'algèbre sur A ; on dit que E , munide cette structure d'algèbre, 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 anneau d'opérateurs.

Remarques.- 1) Nous aurons plus tard à considérer des structures algébriques 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 on peut montrer que, dans les cas les plus importants, cette généralisation n'est qu'apparente : l'annulateur $\mathfrak{a}$ du A-module E (§ 1,n°5) est en effet un idéal bilatère tel que l'anneau quotient $A/\mathfrak{a}$ soit commutatif, et en passant à la structure normale associée à la structure de A-module sur E (§ 1,n°5), on constate qu'on obtient sur E une structure d'algèbre par rapport à $A/\mathfrak{a}$ (cf. exerc. 11) .

Il arrivera souvent qu'on ait à considérer, sur une algèbre E , une structure de module à gauche (ou à droite) par rapport à un sous-anneau non-commutatif B de E ; on se gardera de croire que E soit une algèbre sur B (si $\alpha \in B$, la relation (5) ne sera pas vraie en général).

2. Bases d'une algèbre. Tables de multiplication.

Les algèbres les plus intéressantes sont celles qui, considérées comme modules par rapport à leur anneau d'opérateurs A , admettent une base 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 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 de E ; cela résulte de la formule (6). Si $(a_\lambda)_{\lambda \in L}$ est une base de E par rapport à A, tout élément de E s'écrit d'une seule manière sous la forme $\sum_\lambda a_\lambda a_\lambda$; on peut donc écrire

$$(7) \qquad a_\lambda a_\mu = \sum \gamma_{\lambda\mu\nu} a_\nu$$

et la connaissance des éléments $\gamma_{\lambda\mu\nu}$ 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 (a_i) considérée.

Ce nom vient de ce que, dans le cas où l'ensemble d'indices 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 dans la colonne de a_j est la valeur du produit $a_i a_j$.

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

$$(8) \qquad (a_\lambda a_\mu) a_\nu = a_\lambda (a_\mu a_\nu)$$

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

$$(\gamma) \qquad \sum_\rho \gamma_{\lambda\mu\rho}\,\gamma_{\rho\nu\sigma} = \sum_\rho \gamma_{\lambda\rho\sigma}\,\gamma_{\mu\nu\rho}$$

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

Réciproquement, supposons donnés un A-module unitaire E , une base $(a_\lambda)_{\lambda\in L}$ de E , et une famille $(\gamma_{\lambda\mu\nu})$ d'éléments de A satisfaisant aux relations (γ) ; on peut alors définir une multiplication dans 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 double distributivité de cette loi par rapport à l'addition dans E est immédiate ; les conditions (γ) 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 (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 opposée 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 l'algèbre E soit commutative, 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 "symétrique" de la table de multiplication de E par rapport à sa "diagonale" ; une algèbre commutative est caractérisée par le fait que sa table de multiplication est "symétrique par rapport à sa diagonale" .

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

Une algèbre E par rapport à un corps (commutatif) K est un espace vectoriel par rapport à K ; sa dimension par rapport à K s'appelle plus souvent le rang de E par rapport à K ; rappelons qu'on le note $[E:K]$ lorsqu'il est fini (§ 3, n°2).

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 ; 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.

$u(x+y)=u(x)+u(y)$, $u(xy)=u(x)u(y)$, $u(ax)=au(x)$

$(a\in A$, $x\in E$, $y\in E)$.

On peut 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 (a_λ), une représentation f de E dans F est entièrement déterminée par les éléments $f(a_\lambda)$ (§ 2,cor.2 de la 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 les formules (6) et (7), qu'on ait $f(a_\lambda)f(a_\mu)=\sum_\nu \gamma_{\lambda\mu\nu} f(a_\nu)$ pour tout couple d'indices (λ,μ).

Lorsque E possède un élément unité e , l'application $a\longrightarrow ae$ est une représentation φ de l'anneau A (considéré comme algèbre par rapport à lui-même) dans l'algèbre E ; si $ae=0$, on a, pour tout $x\in E$, $ax=a(ex)=(ae)x=0$, donc l'annulateur $\mathfrak{a}=\varphi^{-1}(0)$ de e est aussi l'annulateur de E (§ 1,n°5), et $\varphi(A)$ est une sous-algèbre de E , isomorphe à $A/\mathfrak{a}$. Lorsque e est un élément libre (§ 1,n°8) de E (ce qui est le cas, en particulier, quand e est un élément d'une base de E) , la structure de A-module de E est donc normale (§ 1,n°5) et

et $\varphi(A)$ est isomorphe à A ; comme $ax=(\alpha e)x$, il n'y a pas lieu de faire de distinction entre la structure d'algèbre de E par rapport à A et sa structure d'algèbre par rapport à $\varphi(A)$; aussi identifie-t-on d'ordinaire A et $\varphi(A)$, 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 (sans opérateur) 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 , considéré comme une algèbre sur A , on doit avoir $f(ax)=af(x)=f(a)f(x)$ quel que soit $x \in E$; au contraire, si g est une représentation de E , considéré 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 le A-module F soit somme directe (§ 1,n°7) des sous-modules F_ι ; par abus de langage, on dit encore que l'algèbre F est somme directe des sous-algèbres F_ι . Mais il faut distinguer soigneusement cette notion de celle de produit d'algèbres : même lorsque l'ensemble d'indices est fini, l'algèbre F n'est isomorphe au produit des sous-algèbres F_ι que lorsqu'elle est leur composée directe (chap.I, § 8,n°11), ce qui n'a lieu que lorsque les F_ι sont tous des idéaux bilatères de F , ou, ce qui revient au même lorsque $F_\lambda . F_\mu = \{0\}$ 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 n'est pas entièrement déterminée par les lois multiplicatives 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. Exemples d'algèbres ; I. Anneaux d'endomorphismes.

Soit E un module à droite sur un anneau A nous avons vu (§ 2,n°5) que l'ensemble $\mathcal{L}(E)$ des endomorphismes de E est muni d'une structure d'anneau à opérateurs ayant pour domaine d'opérateurs le centre C de l'anneau A ; comme l'addition et la loi externe de cette structure déterminent sur $\mathcal{L}(E)$ une structure de C-module unitaire, on voit que $\mathcal{L}(E)$ est une algèbre par rapport à C , ayant pour élément unité l'application identique de E .

Le cas le plus important est celui où E admet une base de n éléments par rapport à A ; alors $\mathcal{L}(E)$ est isomorphe à l'anneau des matrices carrées d'ordre n sur l'anneau A , que nous désignerons par $\mathcal{M}_n(A)$ (§ 6,n°5). Lorsque A est commutatif, $\mathcal{M}_n(A)$ est une algèbre par rapport à A ; la base canonique (E_{ij}) de cette algèbre (§ 6,n°2) a pour table de multiplication

(10) $\begin{cases} E_{ij}E_{hk} = 0 & \text{si } j \neq h \\ E_{ij}E_{jk} = E_{ik} & \text{quels que soient } i,j,k. \end{cases}$

L'élément unité I_n de $M_n(A)$ 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 formée de deux éléments, dont l'un est élément unité de E ; on identifie donc A à un sous-anneau de E , l'élément unité de E étant identifié à l'élément unité de A , que nous noterons 1 . Si u est le second élément de la base considérée, tout élément de E s'écrit 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 déterminée par la donnée de u^2 , c'est-à-dire la relation

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

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

Etudions la structure de E lorsque A est un corps de caractéristique $\neq 2$ (chap.I, § 8, n° 8) ; si on remarque que

$$(a+bu)^2 = (ab+2a)(a+bu) + \beta b^2 - uab - a^2$$

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 $(a+bv)(a-bv)=a^2-\gamma b^2 \neq 0$ par hypothèse, donc $\frac{a}{a^2-\gamma b^2} - \frac{b}{a^2-\gamma b^2} v$ 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 <u>nombres complexes</u> (cf. chap. VI et <u>Top. gén.</u>, chap. VIII). *

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

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

* Lorsque A est le corps des nombres réels $\mathbb{R}$, les éléments de l'algèbre E sur $\mathbb{R}$ ayant pour base (1,v) telle que $v^2=0$, sont appelés <u>nombres duaux</u> . *

<u>8. Exemples d'algèbres : III . Quaternions</u>.

Soit A un anneau commutatif ayant un élément unité, E une algèbre sur A ayant une base de <u>quatre</u> éléments, dont le premier est <u>élément unité</u> de E , qu'on identifie à l'élément unité 1 de A , et dont les trois autres j,k,ℓ se multiplient selon la table :

$$(12)\qquad \begin{cases} j^2=k^2=\ell^2=-1 \\ jk=-kj=\ell \\ k\ell=-\ell k=j \\ \ell j=-j\ell=k \end{cases}$$

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

L'algèbre des quaternions E est isomorphe à l'algèbre opposée E^0 sur A. En effet, pour tout quaternion $x=a+bj+ck+d\ell$, désignons 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 une application linéaire biunivoque de E sur E^0 ; on a $\overline{jk}=\ell=-\ell=kj=\bar{k}.\bar{j}$, 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 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 $N(x)$. On a

$$N(xy)=N(x)N(y) \tag{13}$$

car $N(xy)=xy.\overline{xy}=xy(\bar{y}.\bar{x})=x(y\bar{y})\bar{x}=(y\bar{y})(x\bar{x})$ puisque $y\bar{y} \in A$.

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 $x^{-1}=\dfrac{\bar{x}}{N(x)}$ dans E.

On notera que les éléments $a+bj$ (resp. $a+ck$, $a+d\ell$) forment alors un sous-corps commutatif de E, extension quadratique de A correspondant à $\alpha=0$, $\beta=-1$ dans (11).

9. Exemples d'algèbres : IV. Algèbre d'un monoïde. Algèbre d'un groupe.

Soient A un anneau commutatif ayant un élément unité, S un monoïde (chap.I, § 1, n° 3) 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

une structure d'algèbre par rapport à A en prenant comme table de multiplication de la base (e_u)

(14) $$e_u e_v = e_{uv} .$$

En effet, les conditions d'associativité (8) sont bien satisfaites, puisque $(e_u e_v)e_w = e_{uv}e_w = e_{uvw} = e_u e_{vw} = e_u(e_v e_w)$ 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 le plus souvent S avec la base canonique (e_u) par cette application ; on écrit donc les éléments de l'algèbre $A^{(S)}$ sous la forme $\sum_{u \in S} \alpha_u . u$ $(\alpha_u \in A)$. Si S est commutatif, il en est de même de l'algèbre $A^{(S)}$; si S admet un élément neutre e , e est aussi (avec la convention précédente) élément unité de l'algèbre $A^{(S)}$.

Si T est une partie stable du monoïde S , l'ensemble des éléments de la forme $\sum_{u \in T} \alpha_u . u$ est une sous-algèbre de $A^{(S)}$, isomorphe à l'algèbre $A^{(T)}$ du monoïde T , et qu'on identifie à cette dernière.

Si B est un sous-anneau de A ayant même élément unité que A , l'ensemble des éléments $\sum_{u \in S} \alpha_u . u$ de $A^{(S)}$ tels que $\alpha_u \in B$ est un sous-anneau de $A^{(S)}$ (mais non une sous-algèbre relativement à l'anneau A) ; sa structure d'algèbre relativement à l'anneau B peut être identifiée à celle de l'algèbre $B^{(S)}$ du monoïde S relative à l'anneau B .

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 de $A^{(S)}$ dans l'algèbre $A^{(S')}$ en posant $f(\sum_{u \in S} \alpha_u . u) = \sum_{u \in S} \alpha_u f(u)$.

Soit maintenant B un anneau commutatif ayant un élément unité, φ une représentation de l'anneau A dans l'anneau B ; considérons

les algèbres $A^{(S)}$ et $B^{(S)}$ du même monoïde S comme munies seulement de leur structure d'anneau (sans opérateur) sous-jacente à leur structure d'algèbre. On définit alors une représentation f de l'anneau $A^{(S)}$ dans l'anneau $B^{(S)}$ en posant $f(\sum_{u \in S} a_u.u) = \sum_{u \in S} \varphi(a_u).u$. Si S admet un élément unité, de sorte que A (resp. B) puisse être identifié à un sous-anneau de $A^{(S)}$ (resp. $B^{(S)}$), la représentation f est un prolongement de la représentation φ .

Les algèbres de monoïdes les plus importantes sont les algèbres de groupes relatives à un corps.

Modules et groupes abéliens à opérateurs. La notion d'algèbre d'un monoïde permet de ramener l'étude des groupes abéliens à opérateurs quelconques à celle des modules.

De façon précise, à toute structure de groupe abélien à opérateurs sur un ensemble E , nous allons voir qu'on peut associer une structure de module sur E ayant même loi de groupe additif, et telle que :

1° tout sous-groupe stable de E (pour les lois externes données) soit un sous-module de E (pour la structure de module associée) et réciproquement ;

2° toute représentation du groupe à opérateurs E dans un groupe homologue F (chap.I, § 4, n°1) soit une représentation du module associé à E dans le module associé à F , et réciproquement.

Nous supposerons notées multiplicativement toutes les lois externes sur E . Soit Ω un ensemble somme (Ens. R, § 4, n°5) des domaines d'opérateurs des diverses lois externes sur E , chacun de ces domaines étant identifié avec la partie de Ω qui lui correspond. Soit $L(\Omega)$ le monoïde libre (chap.I, § 1, n° 3), déduit de Ω ; nous définirons une loi de composition

externe $(\alpha,x) \to \alpha x$ sur E , ayant $L(\Omega)$ comme domaine d'opérateurs, par récurrence sur la longueur du mot α dans $L(\Omega)$; si α est de longueur 1 , il appartient à un (et un seul) des domaines d'opérateurs des lois externes données sur E , et αx est défini. Si maintenant λx est défini pour les λ de longueur n-1 , et si α est de longueur n , on a $\alpha=\beta\gamma$, où γ est de longueur n-1 et β de longueur 1 , et on pose $\alpha x=\beta(\gamma x)$. On voit aussitôt que, pour deux mots quelconques α, β de $L(\Omega)$, on a $\alpha(\beta x)=(\alpha\beta)x$ par récurrence sur la longueur de α . Soit maintenant A l'algèbre du monoïde $L(\Omega)$ relative à l'anneau $\mathbb{Z}$ des entiers rationnels ; on définit une loi de composition externe $(\alpha,x)\to\alpha x$ sur E , ayant A comme anneau d'opérateurs, en posant, pour tout $\alpha = \sum_{\lambda\in L(\Omega)} n_\lambda \cdot \lambda$ $(n_\lambda \in \mathbb{Z})$, $\alpha x = \sum_{\lambda\in L(\Omega)} n_\lambda (\lambda x)$. On vérifie sans peine que cette loi externe satisfait aux axiomes (M_I), (M_{II}) et (M_{III}), donc définit sur E une structure de A-module à gauche, et que cette structure satisfait aux conditions 1^0 et 2^0 ci-dessus.

10. Exemples d'algèbres : V. Algèbre large d'un monoïde.

L'algèbre d'un monoïde S relative à un anneau A (commutatif et ayant un élément unité) peut encore être considérée comme le sous-module du module produit A^S , formé des familles $(a_u)_{u\in S}$ telles que $a_u=0$ sauf pour un nombre fini d'indices, dans lequel la multiplication est définie par la relation $(a_u)(\beta_u)=(\gamma_u)$ avec, pour tout $u\in S$,

$$\gamma_u = \sum_{vw=u} a_v\beta_w \tag{15}$$

(somme étendue à tous les couples (v,w) tels que $vw=u$) .

La somme du second membre de (15) a un sens parce que les α_u et β_u sont nuls sauf un nombre fini d'entre eux, donc il en est de même des produits $\alpha_v\beta_w$. Mais le second membre de (15) a encore un sens lorsque les familles (α_u) et (β_u) sont quelconques, mais que par contre le monoïde S vérifie la condition suivante :

(D) *Pour tout* $u \in S$, *il n'existe qu'un nombre fini de couples* (v,w) *d'éléments de* S *tels que* $vw=u$.

Supposons donc que S vérifie la condition (D) ; sur le A-module produit A^S , nous définirons une loi de composition interne $((\alpha_u),(\beta_u)) \to (\gamma_u)$, où pour tout $u \in S$, γ_u est donné par la formule (15) . Il est immédiat que la multiplication ainsi définie sur A^S est doublement distributive par rapport à l'addition, et satisfait aux identités (5) ; enfin, elle est associative, en vertu des identités

$$\sum_{uvw=t} \alpha_u\beta_v\gamma_w = \sum_{rw=t} ((\sum_{uv=r} \alpha_u\beta_v)\gamma_w) = \sum_{us=t} (\alpha_u(\sum_{vw=s} \beta_v\gamma_w))$$

Cette multiplication et les deux lois de composition de la structure de A-module de A^S définissent donc sur A^S une structure d'algèbre relative à l'anneau A ; nous dirons que l'ensemble A^S , muni de cette structure, est l'algèbre large du monoïde S , relative à l'anneau A (on aura soin de ne pas confondre cette structure d'algèbre avec la structure produit des structures d'algèbre des facteurs A de l'ensemble A^S) .

Il est immédiat que l'algèbre $A^{(S)}$ du monoïde S relative à A appelée encore algèbre stricte de S lorsqu'on veut éviter toute confusion) est une sous-algèbre de l'algèbre large de S relative à A (identique à cette dernière lorsque S est fini). Par abus de langage, on note encore tout élément $(\alpha_u)_{u \in S}$ de l'algèbre large de S relative à A , par la même notation $\sum_{u \in S} \alpha_u.u$ que les éléments de l'algèbre stricte de S , bien que le signe de sommation qui figure dans cette

notation ne représente aucune opération algèbrique, puisqu'il porte sur une infinité de termes $\neq 0$. Avec cette notation, la multiplication dans l'algèbre large de S s'écrit $(\sum_{u\in S}\alpha_u.u)(\sum_{u\in S}\beta_u.u)=\sum_{u\in S}((\sum_{vw=u}\alpha_v\beta_w).u)$.

Toutes les propriétés des algèbres strictes de monoïdes énoncées au n°9 s'étendent sans modification aux algèbres larges. En particulier, si S est commutatif, il en est de même de l'algèbre large de S ; si S admet un élément neutre e , e est aussi élément unité de l'algèbre large de S .

Parmi les monoïdes satisfaisant à la condition (D), citons en particulier l'ensemble $\mathcal{N}$ des entiers naturels, muni de la structure définie par l'addition, et l'ensemble $\mathcal{N}^*$ des entiers >0 , muni de la structure définie par la multiplication. Au chap.IV, nous étudierons de façon détaillée les algèbres (stricte et large) du monoïde additif $\mathcal{N}$ (relatives à un anneau quelconque) ; l'algèbre large du monoïde multiplicatif $\mathcal{N}^*$ joue aussi un rôle important en Théorie des nombres (cf. chap.V) .

Exercices.- 1) a) Soit E une algèbre de rang fini sur un corps commutatif K ; montrer que si $a\in E$ n'est pas diviseur de 0 , E admet un élément unité, et a est inversible (cf. chap.I, §2, prop.4) .

b) En déduire que s'il n'existe pas de diviseur de 0 dans E , E est un corps .

2) Soit K un corps commutatif de caractéristique 2 , E une extension quadratique de K , ayant pour base les éléments 1 et u , avec $u^2=\alpha u+\beta$ $(\alpha\in K$, $\beta\in K)$. Montrer que, si l'équation $x^2-\alpha x-\beta=0$ n'a pas de racine 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 $v^2=0$.

3) 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 .

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

5) 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 $e_1^2=e_2^2=e_3^2=0$, $e_1e_2=e_3$, $e_1e_3=e_2e_3=0$.

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

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

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

7) 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 E et K), avec la table de multiplication

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

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 à -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 .

8) Le <u>groupe quaternionique</u> $\mathfrak{Q}$ (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 $\mathfrak{Q}$ relative à 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 $\mathfrak{Q}$ qui correspond au quaternion -1 dans l'isomorphie précédente, les éléments de $\mathfrak{Q}$ peuvent s'écrire $e, j, k, \ell, c, cj, ck, c\ell$; considérer la base de E formée des éléments $\frac{1}{2}(e+c)$, $\frac{1}{2}(e-c)$, $\frac{1}{2}(e+c)j$, $\frac{1}{2}(e-c)j$, $\frac{1}{2}(e+c)k$, $\frac{1}{2}(e-c)k$, $\frac{1}{2}(e+c)\ell$, $\frac{1}{2}(e-c)\ell$)

9) montrer que l'algèbre E du <u>groupe diédral</u> $\mathfrak{D}_8$ d'ordre 8 (chap.I, § 6, exerc.20) relative à un corps 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 générateurs de $\mathfrak{D}_8$ considéré dans l'exerc. 20 du chap.I, § 6, les éléments de $\mathfrak{D}_8$ 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 quatre 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. 6).

Montrer de même que l'algèbre F du groupe diédral $\mathfrak{D}_6$ d'ordre 6 , relative à un corps K de caractéristique $\neq 2$ et $\neq 3$, est composé direct de deux corps isomorphes à K et de l'algèbre des matrices

d'ordre 2 sur K (considérer ici la base de F formée des éléments $e+a+a^2$, $a+a^2-2e$, $a-a^2$, et de ces trois éléments multipliés à droite par b) .

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

11) Soit E un module à gauche sur un anneau non commutatif A ; on suppose définie dans E une multiplication qui, avec la loi de groupe additif et la loi externe de la structure de module de E , définisse sur E une structure d'anneau à opérateurs ayant A comme domaine d'opérateurs. Dans ces conditions, montrer que, quels que soient $\alpha \in A$, $\beta \in A$, $x \in E$, $y \in E$, on a $(\alpha\beta)(xy)=(\beta\alpha)(xy)$. En déduire que, si tout élément de E est produit de deux éléments de E (ce qui est toujours le cas si E admet un élément unité), l'annulateur $\mathfrak{a}$ de E est tel que l'anneau quotient $A/\mathfrak{a}$ soit <u>commutatif</u> .
