RÉDACTION N° 140

COTE : NBR 043

TITRE : LIVRE II ALGÈBRE
CHAPITRE VII
MODULES SUR LES ANNEAUX PRINCIPAUX

ASSOCIATION DES COLLABORATEURS DE NICOLAS BOURBAKI

NOMBRE DE PAGES : 64

NOMBRE DE FEUILLES : 64

LIVRE II
ALGÈBRE
CHAPITRE VII
MODULES SUR LES ANNEAUX PRINCIPAUX

Le but de ce chapitre est d'étudier les anneaux d'intégrité dont tous les idéaux sont principaux, et les modules sur ces anneaux. Les propriétés élémentaires de ces anneaux et modules étant applicables à des classes plus générales d'anneaux et de modules, nous ferons d'abord une étude élémentaire de ces derniers, leur étude plus approfondie étant réservée à une autre Partie de ce Traité.

§ 1 - Modules et anneaux noethériens.

Etant donné un anneau quelconque A nous conviendrons de dire qu'un A-module E (et en particulier un idéal à gauche de A) est de type fini s'il est engendré (chap.I, § 6, n°10) par des éléments en nombre fini.

1. - Définition des modules et anneaux noethériens.

Définition 1 - Etant donné un anneau A (non nécessairement commutatif) et possédant un élément unité, un A-module M sera dit noethérien s'il est unitaire (chap.II, § 1, n°2, déf.2) et s'il vérifie l'axiome suivant :

(N) Tout ensemble de sous-modules de M, ordonné par inclusion, contient un élément maximal.

Nous énoncerons deux axiomes équivalents à l'axiome (N) :

(N') Toute suite croissante $M_0 \subset M_1 \subset M_2 \subset \ldots$ de sous-modules de M n'a qu'un nombre fini de termes distincts (On dit alors (Livre I, chap.III) que cette suite est stationnaire à partir d'un certain rang).

L'équivalence de (N) et (N') se déduit aussitôt du lemme de la théorie des ensembles ordonnés suivant :

Lemme - Soit E un ensemble ordonné ; les propriétés suivantes sont équivalentes :

a) Toute partie de E contient un élément maximal.

b) Toute suite croissante $a_1 \leqslant a_2 \leqslant a_3 \leqslant \dots$ d'éléments de E est stationnaire à partir d'un certain rang.

a) entraîne b) car l'ensemble A des éléments de la suite admet un élément maximal, soit a_n, et on a, pour $p \geqslant n$, à la fois $a_p \geqslant a_n$ et $a_p \leqslant a_n$. Réciproquement supposons que b) soit vérifiée, mais qu'il existe une partie A de E sans élément maximal ; alors, pour tout $a \in A$ il existe $f(a) \in A$ tel que $f(a) > a$; et l'existence de la suite (x_n) définie par induction au moyen de $x_1 \in A$ et $x_{n+1} = f(x_n)$ contredit b).

(N") Tout sous-module de M est de type fini.

(N) entraîne (N") car, étant donné un sous-module E de M, l'ensemble des sous-modules de type fini de E admet un élément maximal F ; pour tout $x \in E$, le module $F+Ax$ est de type fini, donc est égal à F, ce qui entraîne $x \in F$ et $F=E$. Réciproquement (N") entraîne (N'), car le module $E = \bigcup_{n=1}^{\infty} M_n$ est engendré par un nombre fini d'éléments $(x_1, \dots, x_s)$; par hypothèse tout x_i est contenu dans un des modules (M_n), soit $M_{n(i)}$; si q est le plus grand des indices $n(i)$, on a $x_i \in M_q$ pour tout i car la suite (M_n) est croissante, donc $M_q = E$, ce qui prouve que la suite (M_n) est stationnaire à partir de l'indice q.

Exemples - 1) Tout A-module ayant un nombre fini d'éléments est noethérien.

2) Tout espace vectoriel de dimension finie sur un corps K est un K-module noethérien en vertu de (N").

Définition 2 - Un anneau A est dit noethérien à gauche s'il possède un élément unité et si le A-module A_s (chap.II, § 1, n°1) est noethérien.

On définit de façon analogue les anneaux noethériens à droite.

Un anneau commutatif A est donc dit noethérien s'il possède un élément unité, et s'il satisfait à l'une des conditions équivalentes suivantes :

(N_o) Tout ensemble d'idéaux de A, ordonné par inclusion, contient un élément maximal.

(N'_o) Toute suite croissante d'idéaux de A n'a qu'un nombre fini d'éléments distincts.

(N''_o) Tout idéal de A est de type fini.

Exemples - 1) Tout anneau fini A est noethérien (à gauche et à droite

2) Tout corps est un anneau noethérien.

3) Un anneau commutatif A dont tous les idéaux sont principaux est noethérien en vertu de (N''_o). Il en est ainsi, par exemple, de l'anneau Z des entiers rationnels (Chap.I, § 8, n°5) et de l'anneau $K[X]$ des polynomes à une indéterminée sur un corps commutatif quelconque K (chap.IV, §1, n°5,).

2 - Propriétés des modules noethériens.

Proposition 1 - Soit F un sous-module d'un A-module E ; pour que E soit noethérien, il faut et il suffit que le sous-module F et le module quotient E/F soient noethériens.

Si E est noethérien, F est noethérien car tout sous-module de F est de type fini, en tant que sous-module de E ; d'autre part tout sous-module de E/F est de la forme M/F où M est un sous-module de E contenant F (chap.I, § 6, th.6), et est donc engendré par les classes (mod.F) des éléments d'un système fini de générateurs de M .

Si réciproquement F et E/F sont noethériens, soit M un sous-module de E ; son image canonique (M+F)/F dans E/F est, par hypothèse, engendrée par un nombre fini d'éléments $(x'_1,\dots,x'_s)$; soit x_i un représentant dans M de la classe x'_i ; pour tout $x \in M$, il existe donc s éléments

$(a_1,..,a_s)$ de A tels que $y = x - \sum_{i=1}^{s} a_i x_i$ appartienne à F . Mais y appartient aussi à M , donc au sous-module $F \cap M$ de F ; si $(y_1,..,y_t)$ est un système fini de générateurs de celui-ci, M est engendré par les générateurs en nombre fini $(x_1,\ldots,x_s,y_1,\ldots,y_t)$, ce qui montre que E est noethérien en vertu de (N'').

Corollaire 1 - Si E et F sont des modules noethériens, le module produit $E \times F$ est noethérien.

Corollaire 2 - Tout A-module produit d'un nombre fini n de modules noethériens est noethérien.

Ceci se déduit aussitôt du cor.2 par récurrence sur n .

Corollaire 3 - Tout module (à gauche) E de type fini sur un anneau noethérien (à gauche) A est un module noethérien ; en particulier tout sous-module de E est de type fini.

En effet, si E est engendré par n éléments, il est isomorphe à un module quotient du module produit A_s^n .

3 - Procédés de formation d'anneaux noethériens.

Nous allons, dans ce qui suit, énumérer les principaux procédés de formation d'anneaux noethériens à partir d'anneaux noethériens déjà connus. Tous les anneaux considérés dans ce n° seront supposés commutatifs, l'extension (d'ailleurs facile) aux anneaux non commutatifs étant laissée au lecteur (cf. exer. ,).

Proposition 2 - Si I est un idéal d'un anneau noethérien A , l'anneau quotient A/I est noethérien.

Remarque - Il n'est pas vrai que tout sous-anneau d'un anneau noethérien soit noethérien (cf. exerc.).

En effet les idéaux de A/I ne sont autres que les sous A-modules du A-module A/I , d'où le résultat en vertu de la prop.1.

Proposition 3 - Soient A un anneau, R son anneau des fractions (chap.I, § 9, déf.2) et M un monoïde multiplicatif non vide de A ne contenant aucun diviseur de zéro. Alors les éléments de A qui sont de la forme x/y avec $x \in A$ et $y \in M$ constituent un anneau $A_M = B$; B est noethérien lorsque A est noethérien.

L'hypothèse sur M exprime d'une part que la notation x/y a un sens, et d'autre part que $y \in M$ et $y' \in M$ entraînent que $yy' \in M$; on en conclut aussitôt que B est un anneau, en vertu des règles d'addition et de multiplication des fractions. Comme tout $x \in A$ s'écrit xy/y avec $y \in M$, on a $A \subset B$. Pour tout idéal I' de B , considérons l'idéal $f(I') = A \cap I'$, et, pour tout idéal I de A , considérons l'idéal $g(I) = B.I$ engendré par I dans B . L'idéal $g(f(I'))$ est évidemment contenu dans I'. Mais, pour tout élément x/y de I' ($x \in A$, $y \in M$), on a $x = (x/y).y \in f(I')$, et $x/y = (y/y^2).x \in g(f(I'))$. On a donc $I' = g(f(I'))$. Ceci montre que l'application f est une application biunivoque de l'ensemble des idéaux de B dans l'ensemble des idéaux de A ; et elle est évidemment croissante pour les relations d'inclusion. Si donc les idéaux de A satisfont à la condition (N_0), il en est de même a fortiori de ceux de B .

Remarque - Le cas le plus intéressant d'application de la prop.3 est celui où A est un anneau d'intégrité et où M est le complément dans A d'un idéal premier P (chap.I, § 8, exerc.13). Dans ce cas l'anneau B est souvent appelé l'anneau des quotients de P , et se note A_P .

Théorème 1 (Hilbert) - Si A est un anneau noethérien, l'anneau $A[X]$ des polynomes à une indéterminée sur A est noethérien.

Soit $\mathfrak{a}$ un idéal de $A[X]$; pour tout polynome non nul F de $\mathfrak{a}$, nous noterons $c(F)$ le coefficient dominant de F, et nous poserons $c(0)=0$. Soit I l'ensemble des éléments de A de la forme $c(F)$ où $F \in \mathfrak{a}$; si $a \in A$ on a $c(aF)=ac(F)$; si $c(F)+c(F') \neq 0$, et si n et n' sont les degrés de F et F', on a $c(X^{n'}F + X^{n}F') = c(F)+c(F')$; donc I est un idéal de A.

Par hypothèse I est engendré par des éléments (a_i) en nombre fini. Soient $a_i=c(F_i)$, n_i le degré de F_i, $n=\max(n_i)$, et $\mathfrak{B}$ l'idéal de $A[X]$ engendré par les (F_i). Le sous $A[X]$-module $\mathfrak{B}$ de $\mathfrak{a}$ étant de type fini, il nous suffira de montrer (prop.1) que le quotient $\mathfrak{a}/\mathfrak{B}$ est un $A[X]$-module de type fini ; nous allons même montrer que c'est un A-module de type fini.

Soit F un polynome de degré $N \geqslant n$ de $\mathfrak{a}$; on a $F=c(F)X^N+F'$, F' étant nul ou de degré $< N$. Comme $c(F) \in I$, on a $c(F)=\sum_i b_i a_i$ $(b_i \in A)$. Donc le polynome $F''=F-\sum_i b_i X^{N-n_i}.F_i$ sera nul ou de degré $\leqslant N-1$, et on aura $F \equiv F''$ (mod. $\mathfrak{B}$). Procédant par récurrence sur N on voit donc que tout polynome $F \in \mathfrak{a}$ est congru (mod. $\mathfrak{B}$) à un polynome $G \in \mathfrak{a}$ nul ou de degré $\leqslant n$. Donc le A-module $\mathfrak{a}/\mathfrak{B}$ est isomorphe à un module quotient M d'un sous-module du A-module des polynomes de degré $\leqslant n$; ce dernier étant de type fini, on en conclut (A étant noethérien) que M est de type fini (cor.3 de la prop.1).

Corollaire 1 - Si A est un anneau noethérien, l'anneau $A[X_1,\ldots,X_n]$ des polynomes à n indéterminées sur A est noethérien pour tout entier n.

C'est immédiat par récurrence sur n.

Corollaire 2 - Si A est, soit l'anneau Z des entiers rationnels, soit un corps K , l'anneau $A[X_1,\dots,X_n]$ est noethérien.

Ceci est un cas particulier du cor.1, Z et K étant noethériens.

Corollaire 3 - Soient R un anneau, A un sous-anneau noethérien de R , et $(x_1,\dots,x_n)$ des éléments de R en nombre fini ; alors le sous-anneau $A[x_1,\dots,x_n]$ de R , engendré par A et les x_i , est noethérien.

C'est en effet un quotient de l'anneau de polynomes $A[X_1,\dots,X_n]$ (Chap.IV, § , n°).

Théorème 2 - Si l'anneau A est noethérien, l'anneau $A[[X_1,\dots,X_n]]$ des séries formelles à n indéterminées sur A est noethérien pour tout entier naturel n .

Soit $\mathfrak{a}$ un idéal de $A[[X_1,\dots,X_n]]$; pour toute série formelle non nulle F de $\mathfrak{a}$, nous noterons P(F) la forme de plus bas degré de F (P(F) étant une forme de degré s si s est l'ordre de F) ; soit $\mathfrak{f}$ l'idéal de l'anneau de polynomes $A[X_1,\dots,X_n]$ engendré par les P(F) où $F \in \mathfrak{a}$; d'après le cor.1 du th.1 il possède un système fini de générateurs, que, en vertu de la condition (N_0), on peut extraire de l'ensemble des P(F) ; soit $(P(F_1),\dots,P(F_s))$ ce système. Nous allons montrer que $\mathfrak{a}$ est engendré par $(F_1,\dots,F_s)$.

Soit donc $F \in \mathfrak{a}$; supposons que nous ayons trouvé s polynomes $(P_{i,k})(1 \leqslant i \leqslant s)$ tels que la série formelle $G = F - \sum_i P_{i,k}F_i$ soit d'ordre $g > k$. Par hypothèse on peut écrire $P(G) = \sum_i Q_i P(F_i)$; mais comme $P(F_i)$ est une forme, les seuls termes de degré g de $Q_iP(F_i)$ proviennent de $Q_i'P(F_i)$ où Q_i' est la forme de degré $g-d^\circ(F_i)$ de Q_i ; on peut donc supposer que Q_i est une forme de degré $g-d^\circ(F_i)$. Il est clair que la série formelle $F - \sum_i P_{i,k+1}F_i$ est au moins d'ordre $k+1$. (en posant $P_{i,k+1} = P_{i,k} + Q_i$,)

On définit donc, par récurrence sur k, s suites $(P_{i,k})$ de polynomes qui, d'après ce qui vient d'être dit des degrés des Q_i, convergent chacune vers une série formelle S_i (chap.IV, § , n°). Par conséquent, la série formelle $F - \sum_i S_i F_i = F - \sum_i P_{i,k} F_i + \sum_i (P_{i,k} - S_i) F_i$ est au moins d'ordre k, car $P_{i,k} - S_i$ est au moins d'ordre $k - d^\circ(F_i)$ par construction. Comme ceci a lieu pour tout entier k, nous en déduisons que l'on a $F = \sum_i S_i F_i$. C.Q.F.D.

Corollaire - Si l'anneau A est, soit l'anneau $\mathbb{Z}$ des entiers rationnels soit un corps K, l'anneau $A[[X_1, \ldots, X_n]]$ est noethérien.

Exercices sur le § 1.

1) (A dire éventuellement dans le texte). Montrer que si (x_α) est un système de générateurs d'un module noethérien E, on peut extraire de (x_α) un système fini de générateurs de E.

2) Montrer que, si tout ensemble de sous-modules de type fini d'un module E contient un élément maximal, le module E est noethérien.

3) Montrer que, si A est un anneau noethérien, tout idéal I de A est intersection d'un nombre fini d'idéaux irréductibles (chap.I, § 8, exer.12) (Considérer un idéal maximal de l'ensemble des idéaux n'ayant pas cette propriété).

4) Donner un exemple de sous-anneau non noethérien d'un anneau noethérien (considérer un anneau A de polynomes à une infinité d'indéterminées sur un corps, comme sous-anneau de son corps des fractions).

5) Montrer que le sous-anneau de $K[X,Y]$ engendré, sur K, par la suite de monomes $(X, YX^2, Y^2X^3, \ldots, Y^{n-1}X^n, \ldots)$ n'est pas noethérien. (Considérer l'idéal engendré par cette suite).

6) Montrer que tout sous-anneau A de $K[X]$ contenant le corps K est noethérien (si $P \in A$ et $P \notin K$, on montrera que $K[X]$ est un module de type fini sur $K[P]$).

7) Soient A un anneau noethérien et M un idéal de A ; on prend la suite d'idéaux (M^n) pour système fondamental de voisinages de 0 dans A ; montrer que l'anneau A, complété de A pour cette topologie, est noethérien (si $(x_1,..,x_s)$ est un système de générateurs de M , considérer A comme un anneau quotient de $A[[x_1,\ldots,x_s]]$).

8) Généraliser les résultats du n°3 à des anneaux non commutatifs.

---

§ 2 - Anneaux principaux

Définition 1 - Un anneau A est dit principal s'il est anneau d'intégrité, s'il a un élément unité, et si tout idéal de A est principal.

Exemples - Z est un anneau principal (chap.I, §8, n°5, ex.4). Si K est un corps commutatif, l'anneau $K[X]$ des polynomes à une indéterminée à coefficients dans K est principal (chap.IV, §1, n°5, prop.7) ; il en est de même de l'anneau $K[[X]]$ des séries formelles à une indéterminée à coefficients dans K , car il est immédiat (Chap.IV, § , n°6) que tout idéal de cet anneau est de la forme (X^n). * L'anneau des entiers d'un corps $\mathcal{P}$-adique, et, plus généralement tout anneau de valuation discrète (cf.chap.X) est principal.*

Par contre l'anneau $K[X,Y]$ des polynomes à deux indéterminées sur un corps commutatif K n'est pas principal ; en effet, si l'idéal engendré par X et Y était principal, il serait engendré par un polynome P divisant X et Y , et de la forme $sX+tY$, donc de degré 1 et homogène ; X et Y seraient alors des multiples scalaires de $P=aX+bY$ ($a \in K$, $b \in K$), ce qui est impossible.

1 - Divisibilité dans les anneaux principaux.

Soient A un anneau principal, K son corps des fractions, et $\mathcal{P}^*$ le groupe ordonné des idéaux principaux de K (Chap.VI, §1, n°5) est réticulé. De façon plus précise :

Proposition 1 - Soient x_i $(1 \leqslant i \leqslant n)$ des éléments non nuls en nombre fini du corps des fractions K d'un anneau principal A . Alors le A-module $\sum_{i=1}^{n} Ax_i$ est un idéal fractionnaire principal (d) de K ; d est un pgcd des x_i ; et tout multiple de d (donc en particulier tout pgcd des x_i) peut être mis sous la forme $\sum_i a_i x_i$, où $a_i \in A$ pour tout .

Posons $x_i = u_i/v$ (chap.VI, §1, n°4, prop.6) les u_i et v étant entiers. Le A-module $v(\sum_i Ax_i) = \sum_i Au_i$ est un idéal (entier) de A, donc, par hypothèse, de la forme $Az=(z)$. Donc le A-module $\sum_i Ax_i$ n'est autre que l'idéal fractionnaire $(d)=Ad$ où $d=z/v$. On a $Ax_i \subset Ad$, ou $(x_i) \subset (d)$ c'est-à-dire $d \mid x_i$. Comme $d \in \sum_i Ax_i$, d est de la forme $d = \sum_i a_i x_i$ où $a_i \in A$, et par suite tout diviseur commun des x_i divise d , et d est bien un pgcd des x_i .

De l'existence d'un pgcd pour toute famille finie d'éléments de K , on déduit, par renversement de l'ordre (formule (2), n°8, §1, chap. VI), l'existence d'un ppcm pour toute famille finie d'éléments de K . Le groupe $\mathcal{P}$ est donc réticulé, et nous pouvons appliquer à un anneau principal les réqultats (DIV) du chap.VI, §1, n°8, 9, 10 et 11 .

Mais la prop.1 nous fournit aussi le résultat suivant, qui est particulier aux anneaux principaux.

Théorème 1 ("identité de Bézout") - Pour que les éléments x_i en nombre fini d'un anneau principal A soient étrangers (dans leur ensemble), il faut et il suffit qu'il existe des éléments a_i de A tels que

$$\sum_i a_i x_i = 1 .$$

C'est nécessaire d'après la prop.1 ; réciproquement, si $\sum_i a_i x_i = 1$ tout diviseur commun des x_i dans K^* divise 1, donc 1 est un pgcd des x_i.

Nous allons maintenant appliquer aux anneaux principaux les résultats du chap.VI, §1, n°12. Les entiers irréductibles d'un anneau principal A sont ceux qui engendrent les idéaux maximaux de A (chap.I, §8, n°7). Par suite, pour qu'an entier p d'un anneau principal soit irréductible, il faut et il suffit que l'anneau $A/(p)$ soit un corps (Chap.I, § 9, n°3, th.2), ou, autrement dit, que la congruence $ax \equiv b\ (p)$ admette une solution quels que soient $b \in A$ et a non multiple de p dans A. Plus généralement on a le résultat suivant :

Proposition 2 - Soient a,b,c des éléments du corps des fractions d'un anneau principal A, d un pgcd de a et c ; pour que la congruence $ax \equiv b\ (c)$ admette une solution $x_0 \in A$, il faut et il suffit que d divise b ; en ce cas les entiers solutions de $ax \equiv b\ (c)$ sont les mêmes que ceux qui satisfont à $x \equiv x_0\ (cd^{-1})$.

Si $ax \equiv b\ (c)$, il existe $y \in A$ tel que $b = ax + cy$, donc d divise b. Si réciproquement d divise b, on a, d'après la prop.1, $b = ax_0 + cy_0$, avec x_0 et y_0 entiers, donc $ax_0 \equiv b\ (c)$. Cela étant la relation $ax \equiv b\ (c)$ est équivalente à $a(x-x_0) \equiv 0\ (c)$, ou, en posant $a = da'$ et $c = da'$, à $a'(x-x_0) \equiv 0\ (c')$; comme a' et c' sont des entiers étrangers (chap.VI, §1, n°11, prop.12 (DIV)) cette dernière relation est équivalente, si x est entier, à $x-x_0 \equiv 0\ (c')$ en vertu du lemme d'Euclide (ibid., cor.1 de la prop.11 (DIV)).

Théorème 2 - Soient A un anneau principal et (p_α) une famille d'entiers irréductibles de A telle que tout entier irréductible de A soit associé à un p_α et à un seul. Alors tout élément non nul x du corps de fractions de A s'écrit, d'une manière et d'une seule sous la forme

$$(1) \qquad x = u \prod_\alpha p_\alpha^{n_\alpha},$$

où u est un élément inversible de A, et les n_α des entiers rationnels nuls sauf un nombre fini d'entre eux ; pour que x soit entier, il faut et il suffit que tous les n_α soient positifs.

Ceci est une traduction de la prop.16 et du th.2, n°12, § 1, chap.VI . Comme $\mathcal{O}^*$ est un groupe réticulé, il nous suffira, pour constater que nous sommes bien dans les conditions d'application du th.2 (ibid.), de montrer que tout ensemble d'idéaux principaux de A (c'est-à-dire tout ensemble d'idéaux de A), ordonné par inclusion, contient un élément maximal, c'est-à-dire que A est un anneau noethérien (§ 1, n°1). Or il en est bien ainsi d'après la condition (N''_0) (§ 1, n°1).

Remarque - Le second membre de (1) est appelé la décomposition de x en facteurs irréductibles ; la connaissance de cette décomposition, pour des éléments de K^* en nombre quelconque, permet de déterminer immédiatement leurs relations de divisibilité, leur pgcd et ppcm, etc.

2 - Anneau des entiers rationnels.

Comme on l'a dit, cet anneau Z est un anneau principal ; son corps des fractions est Q ; le groupe multiplicatif U des éléments inversibles de Z a deux éléments, 1 et -1. Le groupe Q_+^* des nombres rationnels >0 (chap.I, § 9, n°5) constitue un ensemble de représentants, dans Q^*, du groupe multiplicatif $\mathcal{O}^* = Q^*/U$ des idéaux fractionnaires de Q , auquel on l'identifiera le plus souvent. En particulier, chaque fois qu'il sera question de pgcd ou de ppcm dans le corps Q (relativement à l'anneau Z), il sera sous entendu que ce seront des éléments de Q_+^* ; grâce à cette convention on pourra parler du pgcd et du ppcm d'une famille finie de nombres rationnels.

Les entiers irréductibles >0 de Z seront appelés nombres premiers rationnels, ou, plus brièvement, nombres premiers (cf. chap.I, § 8, n°7) ;

tout élément irréductible de Z est donc de la forme p ou -p, où p est un nombre premier. Le th.2 (n^o1) montre donc que tout nombre rationnel non nul s'écrit, d'une manière et d'une seule, sous la forme $\varepsilon \prod_i p_i^{n_i}$, où (p_i) est l'ensemble des nombres premiers où $\varepsilon = 1$ ou -1, et où les n_i sont des entiers rationnels, nuls sauf un nombre fini d'entre eux.

Proposition 3 - L'ensemble des nombres premiers est infini.

Soit (p_n) la suite croissante des nombres premiers. Nous poserons $P_n = \prod_{i=1}^{n} (1 - \frac{1}{p_i})^{-1}$; il est clair que la suite (P_n) de nombres rationnels est croissante. Nous allons démontrer que cette suite n'est pas bornée, ce qui impliquera qu'elle est infinie. Or on vérifie aussitôt l'inégalité $(1-1/p)^{-1} \leqslant 1+(1/p)+\ldots+(1/p)^s$ quel que soit l'entier positif s. Donnons-nous arbitrairement un entier $k > 0$, et soit p_n le plus grand nombre premier inférieur à 2^k ; par multiplication membre à membre des n inégalités ci-dessus (pour $p=p_1,\ldots,p_n$, et pour $s=k$), nous obtenons notamment au second membre, par développement des n facteurs, les inverses des 2^k premiers entiers naturels ; nous les obtenons tous, car tout entier $q \leqslant 2^k$ n'a d'autres facteurs premiers que les $(p_1,\ldots,p_n)$, et chacun ne figure dans la décomposition de q qu'avec un exposant $\leqslant k$ (puisque $p_i \geqslant 2$). On a donc l'inégalité : $P_n \geqslant \sum_{j=1}^{2^k} (1/j)$ (2).

Posons $U(t) = \sum_{j=1}^{2^t} (1/j)$; $U(t+1)-U(t)$ est la somme de 2^t termes, dont chacun est supérieur à $1/2^{t+1}$; on a donc $U(t+1)-U(t) \geqslant 1/2$, d'où, par addition, $U(t) \geqslant t/2$. On déduit alors de l'inégalité (2) que l'on a $P_n \geqslant k/2$; comme k est arbitraire, on en déduit que la suite (P_n) n'est pas bornée.

Remarques - 1) Nous venons de démontrer que le produit $\prod_{p \text{ premier}} (1-(1/p))^{-1}$ est divergent (Top.Géné., chap.IV, §7, n^o6). Par contre, pour tout nombre complexe s tel que $\mathcal{R}(s) > 1$, on montre que la série de terme général $(1/n^s)$ est absolument convergente,

et on en déduit, par un raisonnement analogue à celui qui vient d'être fait, que le produit infini $\prod_{p \text{ premier}} (1-(1/p^s))^{-1}$ est aussi convergent, et que sa valeur $\zeta(s)$ est égale à la somme de la série de terme général $(1/n^s)$. La fonction $\zeta(s)$ ainsi définie est d'une grande utilité dans l'étude de la répartition des nombres premiers.

2) Pour une démonstration plus courte de la prop.3, nous renvoyons le lecteur à l'Introduction de ce Traité.

3 - Anneaux de polynomes à une indéterminée sur un corps.

L'anneau $K[X]$ des polynomes à une indéterminée sur un corps K est également, comme on l'a dit déjà plusieurs fois (chap.IV, §1, n°5, prop.7), un anneau principal. Son corps des fractions est le corps $K(X)$ des fractions rationnelles en X à coefficients dans K. L'anneau $K[X]$ contient le sous-anneau des polynomes de degré 0, ou autrement dit des constantes, qu'on identifie à K (chap.IV, §1, n°1) ; les éléments de K^* sont inversibles dans K, donc dans $K[X]$; et réciproquement, la formule $\deg(uv) = \deg(u)+\deg(v)$ (chap.IV, §1, n°4, cor.1 du th.1) montre que tout polynome inversible de $K[X]$ est de degré 0 ; le groupe U des éléments inversibles de $K[X]$ est donc identique à K^*. Donc deux polynomes associés ne diffèrent que par un facteur constant non nul ; en particulier toute classe de polynomes associés contient un polynome unitaire (c'est à dire dont le coefficient dominant est 1 ; cf.chap.IV, §1, n°3) et un seul. Le sous-groupe du groupe multiplicatif $K(X)^*$ engendré par les polynomes unitaires est donc un ensemble de représentants, dans $K(X)$, du groupe $\mathcal{P}^* = K(X)^*/U$ des idéaux fractionnaires principaux de $K(X)$. En particulier, chaque fois qu'il sera question de pgcd ou de ppcm dans le corps $K(X)$ (relativement à l'anneau $K[X]$), il sera le plus souvent sous-entendu que ce seront des quotients de polynomes unitaires ; grâce à cette convention on pourra parler du pgcd

et du ppcm d'une famille finie de fractions rationnelles.

Les éléments irréductibles de $K[X]$ ne sont autres que les polynomes irréductibles (chap.IV, §1,n°4,déf.4). Tout élément non nul de $K(X)$ s'écrit donc, d'une manière et d'une seule, sous la forme $a\prod_i P_i^{n_i}$, où $a \in K^*$, et où (P_i) est la famille de tous les polynomes unitaires et irréductibles de $K[X]$, les exposants n_i étant nuls à l'exception d'un nombre fini (th.2).

Dans les anneaux $K[X]$ et Z on peut préciser quelque peu la prop.1 du n°1 :

Proposition 4 - Soient f,g deux polynomes étrangers dans $K[X]$ (resp. deux entiers rationnels étrangers) ; alors tout polynome h (resp. tout entier h), de degré $< \deg.f+\deg.g$ (resp. tel que $|h| < |fg|$) peut être mis, d'une manière et d'une seule (resp. éventuellement dense), sous la forme $h = uf+vg$ où u et v sont des polynomes nuls ou tels que $\deg.u \leqslant \deg.g$ et $\deg.v \leqslant \deg.f$ (resp. des entiers tels que $|u| < |g|$ et $|v| < |f|$).

Dans les deux cas les éléments u tels qu'il existe v tel que $h = uf+vg$ sont les solutions de $uf \equiv h\ (g)$; d'après la prop.2, il existe une telle solution u_0, et les solutions u de $uf \equiv h\ (g)$ sont celles de $u \equiv u_0\ (g)$. Le reste u_1 de la division euclidienne de u_0 par g (chap.IV, §1,n°5 pour les polynomes, Livre I, chap.III pour les nombres) satisfera bien à cette dernière congruence, et on aura $\deg.u_1 < \deg.g$ (resp. $|u_1| < |g|$, et $|u_1 - |g|| < |g|$) ; si on prend $u=u_1$ (resp. $u=u_1$ si h et f sont de même signe, $u=u_1-|g|$ s'ils sont de signes contraires), il existera v tel que $h-uf = vg$; et, comme $\deg(h-uf) < \deg.f+\deg.g$, on aura bien $\deg.v < \deg.f$ (resp. comme $|uf| \leqslant |gf|$, comme $|h| < |gf|$, et comme h et uf sont de signes contraires on a $|h-uf| < |gf|$, et donc $|v| < |f|$; notons que, dans le cas où on est

est amené à prendre $u=-|g|$, h est un multiple wg de g, et la solution $u=0$; $v=w$ répond à la question). Enfin toute autre solution (u',v') de $h=uf+vg$ est telle que $u'=u+mg$ (prop.2), ce qui implique $v'=v\mp mf$, avec $m\neq 0$; ceci implique $\deg.u'=\deg(mg) \geqslant \deg.g$ puisque $\deg.u<\deg.g$, d'où l'unicité (resp. $|u'|<\varepsilon$ et $|v'|<|f|$ impliquent $m=\operatorname{sgn}(-ug)$ et $m=\operatorname{sgn}(vf)$, d'où une ou deux solutions selon que ces signes sont distincts ou non).

Le cas des deux solutions peut se produire : prenons $f=7$, $g=5$; on a $11 = 3.7+(-2).5 = (-2).7+5.5$.

Proposition 5 - Soient K un corps et E un surcorps de K ; si les polynomes f et g de $K[X]$, admettent h pour pgcd dans $K[X]$, h est aussi pgcd de f et g dans $E[X]$.

Il est clair que f et g sont des multiples de h dans $E[X]$. Comme, d'autre part, on peut trouver $u\in K[X]$ et $v\in K[X]$ tels que $h=uf+vg$ (prop.1), le pgcd h' de f et g dans $E[X]$ divisera h, ce qui implique $h'=h$.

Exercices sur le § 2.

1) Montrer que si A est un anneau d'intégrité, l'anneau $A[X_\iota]$ ne peut être principal : a) si le nombre d'indéterminées X est $\geqslant 2$; b) si A n'est pas un corps. (Considérer les idéaux $(X_\alpha)+(X_\beta)$ dans le premier cas $(\alpha \neq \beta)$, $(a)+(X_\alpha)$ dans le second, a étant un élément non inversible de A).

2) Montrer que dans l'anneau de séries formelles $K[[X]]$ tout élément irréductible est associé à X .

3) Montrer que tout anneau d'intégrité, noethérien, et tel que tout idéal maximal soit principal, est un anneau principal. Montrer par contre que le monoïde S des éléments positifs de $Z \times Z$ ordonné lexicographiquement (chap.VI, § 1, n°6) satisfait à la condition (D) du n° 10, § 7, chap.II, et que l'algèbre large (ibid.) A de ce monoïde S sur un corps K est un anneau non noethérien dont l'unique idéal maximal est principal.

§ 3 - Modules sur les anneaux principaux.

N-B : Le rédacteur s'est placé dans l'hypothèse du rejet du noethérien à la "grande divisibilité", conformément à l'avis du Comité de mars 1950.

Avant d'aborder l'étude des modules sur les anneaux principaux, nous allons donner quelques propriétés générales des modules. Dans tout ce § , et sauf mention expresse du contraire, A désignera un anneau commutatif avec élément unité ; tous les modules seront supposés unitaires. Nous conviendrons de dire qu'un A-module E (et en particulier un idéal I de A) est de type fini s'il est engendré (chap.I, § 6, n° 10) par des éléments en nombre fini.

1 - Sommes directes finies de modules monogènes.

Rappelons que, dans les conditions où nous nous plaçons, tout A-module monogène E est isomorphe à un module quotient A/I où I est un idéal de A (chap.II, § 1, prop.11). Nous allons étudier dans ce n° les modules sommes directes de modules monogènes A/I_s , où les I_s forment une suite croissante finie d'idéaux de A . On verra en effet (n°6) que, sur un anneau principal tout module de type fini est isomorphe à une telle somme directe.

Lemme 1 - Soient M un sous-module d'un A-module E , f l'homomorphisme canonique de E sur E/M , et l'homomorphisme de l'algèbre extérieure $\bigwedge E$ sur l'algèbre extérieure $\bigwedge(E/M)$ déduit de f par prolongement canonique (chap.III, §5,n°9) ; alors le noyau de $\overline{f}$ est l'idéal bilatère I engendré par M dans $\bigwedge E$.

Comme $\overline{f}$ est un homomorphisme d'algèbre, et comme $\overline{f}(M) = (0)$, on a bien $f(I)=(0)$ et I est contenu dans le noyau de f ; il existe donc un homomorphisme canonique g de $(\bigwedge E)/I$ sur $\bigwedge(E/M)$, dont nous avons à montrer que c'est un isomorphisme. Pour ce faire nous allons définir un homomorphisme h de $\bigwedge(E/M)$ dans $(\bigwedge E)/I$ tel que $h \circ g$ soit l'automorphisme identique de $(\bigwedge E)/I$.

Considérons pour cela l'application multilinéaire m_n de E^n dans $(\bigwedge^n E)/I$ qui, à $(x_1,..,x_n)$ fait correspondre la classe de $x_1 \wedge \ldots \wedge x_n$ dans $(\bigwedge^n E)/I$; comme $m_n(x_1,\ldots,x_n)=0$ chaque fois que l'un des x_i appartient à M , m_n définit, par passage aux quotients, une application multilinéaire $\overline{m}_n$ de $(E/M)^n$ dans $(\bigwedge^n E)/I$. Puisque m_n est antisymétrique par définition, il en est de même de $\overline{m}_n$, qui définit donc (chap.III, §5,scholie à la déf.5) une application linéaire h_n de $\bigwedge^n(E/M)$ dans $(\bigwedge^n E)/I$. Comme I est somme directe de ses composantes homogènes $I_n=I\cap(\bigwedge^n E)$, h_n applique $\bigwedge^n(E/M)$ dans $(\bigwedge^n E)/I_n$; les (h_n) définissent donc un homomorphisme h de $\bigwedge(E/M)$ dans $(\bigwedge E)/I$: si $\sum_n y_n$ est la décomposition de $y \in \bigwedge(E/M)$ en composantes homogènes, $h(y)$ sera $\sum_n h_n(y_n)$. Comme g fait correspondre à la classe de $x_1 \wedge \ldots \wedge x_n$ dans $(\bigwedge^n E)/I$ l'élément $\overline{x}_1 \wedge \ldots \wedge \overline{x}_n$ de $\bigwedge(E/M)$ ($\overline{x}_i$ désignant la classe de x_i mod.M), il est clair que $h\,g$ est l'automorphisme identique de $(\bigwedge E)/I$.

Proposition 1 - Soit E un A-module somme directe de n modules monogènes A/I_s (les I_s étant des idéaux de A) ; alors le module $\bigwedge^n E$ est isomorphe à la somme directe des modules A/I_H , I_H désignant, pour toute partie

$H=(i_1,\dots,i_p)$ de $[1,n]$, l'idéal $I_{i_1}+\dots+I_{i_p}$ de A engendré par les I_{i_j}

Soit e_s un générateur de A/I_s (I_s étant donc l'annulateur de e_s). Si (a_s) $(1\leqslant s\leqslant n)$ est la base canonique du module A^n, soit f l'homomorphisme de A^n sur E défini par $f(a_s)=e_s$ $(1\leqslant s\leqslant n)$, et $\bar{f}$ son prolongement canonique, homomorphisme de $\bigwedge(A^n)$ sur $\bigwedge E$. Pour tout entier p, $\bigwedge^p(A^n)$ est le module libre ayant pour base la famille (a_H) (chap.III, § 5, n°9), H parcourant l'ensemble des parties de p éléments de $[1,n]$. Comme, en vertu du lemme 1, le noyau de $\bar{f}$ est engendré par $\sum_s I_s a_s$, tout élément de ce noyau est de la forme $\sum_H x_H a_H$ où x_H est une somme d'éléments de A appartenant chacun à l'un des idéaux I_{i_j} $(i_j\in H)$; ce noyau est donc somme directe des modules $I_H a_H$. C.Q.F.D.

Proposition 2 - Soit E un A-module somme directe de n modules monogènes A/I_s où les idéaux I_s forment une suite croissante telle que $I_1\subset I_2\subset\dots\subset I_n\neq A$. Alors, pour $1\leqslant p\leqslant n$, I_p est l'annulateur de $\bigwedge^p E$, qui n'est donc pas réduit à (0) ; et $\bigwedge^m E=0$ pour $m>n$.

En effet, si $s(H)$ est le plus grand entier de la partie H de $[1,n]$, on a, avec les notations de la prop.1, $I_H=I_{s(H)}$; comme $s(H)$ est supérieur à p pour toute partie H de p éléments, et lui est égal pour la partie $(1,2,\dots,p)$, I_p est l'intersection des I_R ; c'est donc bien, en vertu de la prop.1, l'annulateur de $\bigwedge^p E$.

Corollaire - Si le module E de la prop.1 est aussi isomorphe à la somme directe de m modules A/I'_t, avec $I'_1\subset\dots\subset I'_m=A$, on a $m=n$ et $I'_s=I_s$ pour $1\leqslant s\leqslant n$. ("unicité des I_s").

2 - Facteurs directs et projecteurs.

Définition 1 - Soit M un module à gauche sur un anneau A (commutatif ou non, avec ou sans élément unité). On dit qu'un sous-module E de M est facteur direct de M s'il admet un supplémentaire F, c'est à dire s'il existe un sous-module F de M tel que M soit somme directe de E et F.

Lemme 2 - Pour qu'un sous-module E d'un module M soit facteur direct, il faut et il suffit qu'il existe une application linéaire p de M sur E telle que $p \circ p = p$.

Réciproquement, si q est un endomorphisme de M tel que $q \circ q = q$, M est somme directe de $E = q(M)$ et de $F = {}^{-1}q(0)$.

Si E est facteur direct, soit F un supplémentaire de E ; alors tout $x \in M$ se met, et d'une seule manière, sous la forme $x=p(x)+p'(x)$ où $p(x) \in E$ et $p'(x) \in F$ (chap.II, § 1, n°7) ; si $z \in E$, on a $p(z)=z$, d'où $p(p(x))=p(x)$, c'est-à-dire $p \circ p = p$. Si, réciproquement, q est un endomorphisme de M tel que $q \circ q = q$, tout $x \in E$ s'écrit $x = q(x) + (x-q(x))$; on a $q(x) \in E$, et $x-q(x) \in F$ car $q(x-q(x)) = q(x)-q(q(x))=0$; ainsi M est somme de E et F ; or, si $x \in E \cap F$, on a $q(x)=x$ et $q(x)=0$, donc $x=0$ et M est somme directe de E et F . Si, enfin, E est un sous-module de M tel qu'il existe une application linéaire p de M sur E telle que $p \circ p = p$, on prendra pour q l'endomorphisme $i \circ p$ de M , i désignant l'application canonique de E dans M ; on a en effet $q(M)=E$ et $q \circ q = q$; M est alors somme directe de E et de $F = {}^{-1}q(0) = {}^{-1}p(0)$.

Corollaire - Pour que le noyau ${}^{-1}f(0)$ d'une application linéaire f d'un module M sur un module N soit facteur direct de M , il faut et il suffit qu'il existe une application linéaire g de N dans M telle que $f \circ g$ soit l'automorphisme identique de N ; g est alors un isomorphisme de N dans M , et M est somme directe de ${}^{-1}f(0)$ et de $g(N)$.

S'il existe une telle g , $p=g \circ f$ est un endomorphisme de M tel que $p \circ p = g \circ f \circ g \circ f = g \circ f = p$, et que $p(M) = g(M)$ et ${}^{-1}p(0) = {}^{-1}f(0)$, d'où les conclusions. Si réciproquement ${}^{-1}f(0)$ est facteur direct, f induit sur un supplémentaire de ${}^{-1}f(0)$ (prop.1, chap.II, § 1, n°4) un isomorphisme h de celui-ci sur N, et il suffit de prendre pour g

Définition 2 - Un endomorphisme p d'un module M tel que $p \circ p = p$ est appelé un projecteur. Si M est somme directe de E et F, et si, pour $x \in M$, $p(x)$ et $q(x)$ sont les composants de x dans E et F, p et q sont dits les projecteurs associés à E et F dans la décomposition, en somme, directe.

3 - Modules de torsion sur un anneau principal.

Rappelons (chap.II, § 1, n°6) qu'un élément x d'un A-module E est dit libre si la relation $ax=0$ $(a \in A)$ entraîne $a=0$.

Définition 3 - On dit qu'un élément x d'un module E sur un anneau A (commutatif ou non, avec ou sans élément unité) est un élément de torsion s'il n'est pas libre, c'est-à-dire s'il existe $a \neq 0$, $a \in A$ tel que $ax=0$. Un module E est dit de torsion si tous ses éléments sont de torsion.

Remarques - 1) A l'origine des mots "module de torsion", est l'interprétation de ces modules en Topologie Algébrique.

2) Si $x \in E$ est élément de torsion, il en est de même de tout élément du sous-module Ax. Par contre, il est inexact que toute combinaison linéaire d'éléments de torsion soit de torsion, comme le montre l'exemple de l'élément $1=3+2.2$ dans $\mathbb{Z}/(6)$ considéré comme module sur lui-même. On a cependant le résultat suivant dans le cas où A est un anneau d'intégrité :

Proposition 3 - Dans un module E sur un anneau d'intégrité 1A toute combinaison linéaire $y = \sum_i a_i x_i$ $(a_i \in A)$ d'éléments de torsion (x_i) est élément de torsion. Les éléments de torsion forment donc un sous-module M de E appelé sous-module de torsion.

En effet, pour tout i, il existe un élément non nul $b_i \in A$ tel que $b_i x_i = 0$; alors le produit $b = \prod_i b_i$ n'est pas nul, et on a évidemment $by=0$ en vertu de la commutativité de A.

Définition 4 - Soit p un entier irréductible d'un anneau principal A ; un A-module M sera dit local pour p (ou p-local), si pour tout $x \in M$, il existe un entier $n \geqslant 0$ tel que $p^n x = 0$.

Exemple - Le module monogène $A/(p^s)$ est local pour p .

Théorème 1 - Pour tout entier irréductible p d'un anneau principal A , soit M_p l'ensemble des éléments x d'un A-module de torsion M tels qu'il existe un entier s tel que $p^s x = 0$. Alors M est somme directe des modules locaux M_p .

Il est clair que M_p est un sous-module de M local pour p . Tout élément $x \neq 0$ de M a un annulateur non nul dans A, donc de la forme (a). Soit $a = u \prod_i p_i^{n(i)}$ la décomposition de a en facteurs irréductibles (§ 2, th.2). Les entiers $b_i = a/p_i^{n(i)}$ sont étrangers dans leur ensemble, car aucun p_i ne peut les diviser tous ; nous pouvons donc écrire l'identité de Bezout $\sum_i c_i b_i = 1$ où $c_i \in A$ (§ 2, th.1). On a alors $x = \sum_i c_i b_i x$; or, comme $p_i^{n(i)} c_i b_i x = c_i a x = 0$, on a $c_i b_i x \in M_{p_i}$ et M est bien somme des M_p . Reste à montrer que cette somme est directe : de $0 = \sum_i x_i$, avec $p_i^{n(i)} x_i = 0$, on déduit, au moyen de l'identité de Bézout $c_j p_j^{n(j)} + d_j \prod_{i \neq j} p_i^{n(i)} = 1$ ($c_j \in A$, $d_j \in A$) et du fait que $\prod_{i \neq j} p_i^{n(i)} x_j = 0$, que l'on a $x_j = (c_j p_j^{n(j)} + d_j \prod_{i \neq j} p_i^{n(i)}) . x_j = 0$; comme ceci a lieu pour tout indice j , le théorème est démontré.

Définition 5 - Avec les hypothèses et les notations du th.1, les sous-modules M_p s'appellent les facteurs locaux du module de torsion M .

4 - Décomposition canonique des nombres rationnels et des fractions rationnelles à une indéterminée.

Soit K le corps des fractions d'un anneau principal A ; K est un A-module que, pour éviter les confusions, nous noterons K_A ; A est alors le sous-module de K_A engendré par l'élément unité 1 ; et le module quotient K_A/A est le quotient de K_A par la relation d'équivalence $x - x' \in A$,

qui, avec les notations de chap.VI, §1,n°5 s'écrit aussi $x \equiv x' \pmod{1}$; le module $M = K_A/A$ se note souvent aussi $K \bmod 1$. Soit f l'application canonique de K_A sur M.

M est un <u>module de torsion</u>, car tout élément de M est de la forme $f(a/b)$ $(a \in A, b \in A)$ $b \neq 0$), d'où $bf(a/b)=f(a)=0$. On peut donc lui appliquer le th.1, n°3. Déterminons d'abord les facteurs locaux de M : $f^{-1}(M_p)$ est l'ensemble K_p des éléments de K de la forme ap^{-n} où $a \in A$ et où n est un entier naturel. On en conclut donc que tout x de K s'écrit sous la forme

$$x = a_0 + \sum_i a_i p_i^{-s_i}$$

où $a_0 \in A$, où les p_i sont des entiers irréductibles non associés deux à deux, où les s_i sont des entiers > 0, et où, pour $1 \leqslant i \leqslant n$, a_i est un élément de A non multiple de p_i. De plus, x étant donné, les p_i et les s_i sont déterminés de manière unique (à une permutation des indices près), et chaque a_i $(1 \leqslant i \leqslant n)$ est bien déterminé $\bmod p_i^{s_i}$.

Pour pousser plus loin cette décomposition, supposons que, pour chaque p, on se soit donné dans A un système complet R_p de représentants des classes de A mod.p ; on voit alors aussitôt, par récurrence sur s, que les éléments de A de la forme $\sum_{h=0}^{s-1} r_h p^h$, avec $r_h \in R_p$ pour $0 \leqslant h \leqslant s-1$, forment un système complet de représentants des classes de A $\bmod p^s$. Il s'ensuit que tout $x \in K$ peut être mis, <u>d'une manière et d'une seule</u> sous la forme

$$x = a + \sum_i \sum_{h=0}^{s_i-1} r_{ih} p_i^{-h}$$

où $a \in A$, où les p_i sont des entiers irréductibles de A, et où $r_{ih} \in R_{p_i}$ quels que soient i et h. Les cas les plus importants sont les suivants :

I - A est l'anneau Z des entiers rationnels et K=Q . Les entiers irréductibles sont les nombres premiers p ; pour tout p on prend pour R_p l'intervalle $[0,p-1]$ de Z ; d'où la décomposition canonique :

$$x = a + \sum_i \sum_h e_{ih} p_i^{-h}$$

où $a \in Z$, $e_{ih} \in Z$, $0 \leqslant e_{ih} \leqslant p_i - 1$.

II - A est l'anneau $E[X]$ des polynomes à une indéterminée sur un corps E, et K=E(X). Les entiers irréductibles de A sont les polynomes irréductibles $p(X) \in E[X]$, que l'on peut prendre unitaires (§ 2,n°3). Pour chaque polynome irréductible p , un système complet R_p de représentants des classes de A mod.p se compose, en vertu de la division euclidienne des polynomes (Chap.IV, § 1,n°5), des polynomes de degré strictement inférieur à celui de p . D'où la décomposition (dite canonique) d'une fraction rationnelle $r(X) \in E(X)$:

$$r(X) = a(X) + \sum_i \sum_h v_{ih}(X).p_i(X)^{-h} ,$$

où a(X) et les $v_{ih}(X)$ sont des polynomes, les $p_i(X)$ des polynomes unitaires irréductibles distincts, et où $v_{ih}(X)$ est un polynome de degré strictement inférieur à celui de $p_i(X)$ quels que soient i et h . Si, en particulier, E est un corps algèbriquement clos, les $p_i(X)$ sont de la forme $X-a$, avec $a \in E$ (chap.V, § 4,prop.1),-et les v_{ih} sont donc des constantes.

5 - Modules libres sur un anneau principal.

Définition 6 - E étant un module sur un anneau A (commutatif ou non, avec ou sans élément unité), on dit que E est sans torsion si tout élément non nul de E est libre.

Autrement dit 0 est le seul élément de torsion d'un module sans torsion

Remarque - Si on se borne aux modules unitaires, un anneau A n'admet de A-modules sans torsion $\neq (0)$ que s'il est sans diviseur de zéro : si, en effet, on a ab=0 (a,b: éléments non nuls de A)

et si x est un élément non nul d'un A-module, on a, soit $ax=0$ et x est de torsion, soit $bx\neq 0$ et $a(bx)=0$ et bx est de torsion.

Dans le cas où A est un anneau d'intégrité, soit K son corps des fractions ; rappelons (chap.III, § 2, n°3, th.2) qu'on définit un homomorphisme canonique $x \to f(x) = 1 \otimes x$ de E dans l'espace vectoriel $E_{(K)}$ obtenu par extension à K de l'anneau d'opérateurs A de E , et que le noyau $f^{-1}(0)$ de f est le sous-module de torsion de E (n°3, prop.3), ensemble des éléments non libres de E . Si E est sans torsion f est donc un isomorphisme de E dans $E_{(K)}$, et E peut être identifié à son image $f(E)$; lorsqu'il en est ainsi on aura donc, conformément aux définitions du chap.II, le droit de dire qu'une partie X de E est de rang fini n dans E (resp. de rang infini) si elle est de rang fini n (resp. de rang infini) dans $E_{(K)}$; d'autre part pour qu'une famille d'éléments de E soit libre sur A, il faut et il suffit qu'elle soit libre sur K dans $E_{(K)}$ ((chap.III, § 2, n°3, prop.5).

Lorsque A est un anneau d'intégrité le module quotient E/M d'un A-module E par son sous-module de torsion M est un module sans torsion. D'autre part tout module libre sur un anneau d'intégrité est évidemment sans torsion ; par contre il existe des modules sans torsion sur un anneau d'intégrité (et même principal) qui ne sont pas libres.

Ainsi le groupe additif de Q , considéré comme module sur Z , est sans torsion ; cependant ce n'est pas un groupe monogène, et toute famille d'au moins 2 éléments de Q n'est pas libre.

Théorème 2 - Tout sous-module M d'un module libre L sur un anneau principal A est un A-module libre ; si L est de rang fini n, M est de rang fini inférieur à n .

La dernière assertion est claire si on considère L et M comme des parties de l'espace vectoriel $L_{(K)}$. Pour montrer que M est libre soit

$(e_\iota)_{\iota \in I}$ une base de L ; pour $x \in L$ et $\iota \in I$ nous noterons $p_\iota(x)$ la composante d'indice ι de x par rapport à la base (e_ι). Pour $J \subset I$ nous noterons L_J le sous-module (libre) de L engendré par la famille $(e_\iota)_{\iota \in J}$: c'est l'ensemble des $x \in L$ tels que $p_\iota(x)=0$ pour tout $\iota \notin J$; on a $L_\emptyset = 0$.

Soit Φ l'ensemble des éléments (J,B) de $\mathcal{P}(I) \times \mathcal{P}(M)$ tels que B soit une base de $M \cap L_J$ (ce qui implique que $M \cap L_J$ est un module libre). Φ n'est pas vide car il contient $(\emptyset,0)$. Nous ordonnerons Φ en posant $(J,B) \leqslant (J',B')$ chaque fois que $J \subset J'$ et $B \subset B'$. Muni de cet ordre Φ est un ensemble ordonné inductif : soit donc (J_α,B_α) une famille totalement ordonnée d'éléments de Φ, et posons $J = \bigcup_\alpha J_\alpha$ et $B = \bigcup_\alpha B_\alpha$; il nous suffira de montrer que $(J,B) \in \Phi$; d'abord B est libre puisque toute partie finie de B, qui est contenue dans un B_α est libre ; d'autre part B engendre $M \cap L_J$, car, pour tout $x \in M \cap L_J$, l'ensemble des ι tels que $p_\iota(x) \neq 0$ est une partie finie de J, donc est contenue dans un J_α ; alors $x \in M \cap L_{J_\alpha}$, c'est-à-dire dans le module engendré par B_α, donc dans celui engendré par B ; ainsi B est bien une base de $M \cap L_J$.

En vertu du th. de Zorn (Ens.R, § 6, n°10) Φ admet donc un élément maximal (J,B) ; notre théorème sera démontré si nous faisons voir que J=I. Soit, en effet, $\iota \notin J$, et posons $J' = J \cup \{\iota\}$ et $M' = M \cap L_{J'}$. $p_\iota(M')$ est un idéal de A, donc de la forme Aa $(a \in A)$ puisque A est un anneau principal ; il existe donc $x \in M'$ tel que $a = p_\iota(x)$. Pour tout $z \in M'$ on a donc $p_\iota(z) = ba = bp_\iota(x)$ $(b \in A)$, et par conséquent z-bx est élément de $M' \cap L_J = M \cap L_J$, c'est-à-dire du module engendré par B. Ainsi M' est engendré par $B \cup \{x\}$; nous poserons $B' = B \cup \{x\}$, si $a \neq 0$; dans le cas où a=0, nous pouvons prendre x=0, et nous poserons B'=B ; en tous cas $M' = M \cap L_{J'}$ est engendré par B'.

Mais B' est une partie libre de M : c'est clair si a=0 car B'=B ; d'autre part toute relation $y+bx=0$ ($b \in A$, $y \in M \cap L_J$) entraîne $p_i(y+bx)=ba=0$, donc $b=0$ dans le cas $a \neq 0$, ce qui montre que B' est libre puisque B est libre. On a par conséquent $(J',B') \in \Phi$ en contradiction avec le fait que (J,B) est maximal dans Φ .

Remarque - Le théorème, et sa démonstration, subsistent si L est un module à gauche, unitaire et libre sur un anneau non commutatif A, sans diviseur de zéro, et tel que tout idéal à gauche de A soit principal.

Corollaire - Tout sous-module F d'un module E engendré par n éléments sur un anneau principal A , peut être engendré par n éléments au plus.

Il existe en effet un homomorphisme f de A^n sur E , et $f^{-1}(F)$, qui est un module libre de rang $m \leqslant n$, est engendré par m éléments, dont les images par f engendreront F .

6 - Modules de type fini sur un anneau principal.

Tout module de type fini sur un anneau principal A pouvant être considéré comme un module quotient d'un module libre par un sous-module, nous allons d'abord étudier les "positions respectives" d'un A-module libre et d'un de ses sous-modules. Plus précisément :

Théorème 3 - Soit L un module libre sur un anneau principal A , et M un sous-module de rang fini n de L . Il existe alors n éléments e_i de L et n éléments $a_i \neq 0$ de A ($1 \leqslant i \leqslant n$) tels que

a) les e_i forment une base d'un facteur direct M_0 de L .

b) les $a_i e_i$ forment une base de M ,

c) a_i divise a_{i+1} pour $1 \leqslant i \leqslant n-1$.

De plus M_0 et les idéaux principaux (a_i) sont déterminés d'une manière unique par ces conditions ; M_0/M est le module de torsion de L/M , et est isomorphe à la somme directe des A-modules $A/(a_i)$; enfin L/M est somme directe de M_0/M et d'un module libre isomorphe à L/M_0 .

1) Existence des e_i et des a_i .

Nous démontrerons celle-ci par récurrence sur n . Le cas n=0 est trivial. Pour ramener le cas du rang n à celui du rang n-1, nous allons montrer l'existence de $e_1 \in L$ et de $a_1 e_1 \in M$ $(a_1 \in A)$ tels que les sous-modules Ae_1 et $Aa_1 e_1$ soient facteurs directs de L et de M respectivement.

Etant donné un élément $x \in L$, les éléments $f(x) \in A$ où f parcourt l'ensemble des formes linéaires sur L, constituent un idéal de A , appelé le contenu de x dans L ; le contenu de x est ici un idéal principal Ac_x de A . Il est clair que l'on a $c_{bx}=bc_x$ pour tout $b \in A$. Toute forme linéaire f sur A étant combinaison linéaire des formes coordonnées p_i par rapport à une base (z_i) de L (chap.II, §4,n°4), le contenu c_x de x est un pgcd des composantes de x par rapport à cette base (§ 2, prop.1). Par conséquent l'élément $y=c_x^{-1}.x$ appartient à L et est de contenu 1 . On peut donc caractériser le contenu c_x de x dans L, comme étant un ppcm des $b \in A$ tels qu'il existe $z \in L$ tel que $bz=x$.

Nous allons maintenant montrer que, si x est de contenu 1 dans L, le sous-module Ax est facteur direct de L et réciproquement. La réciproque est immédiate car il existe alors un projecteur p de L sur Ax (n°2, lemme 2), et on considère la forme linéaire f définie par $p(z)=f(z).x$. Si x est de contenu 1, il existe une forme linéaire f telle que $f(x)=1$, et l'endomorphisme p défini par $p(z)=f(z).x$ est un projecteur de L sur Ax .

Ceci étant, considérons l'ensemble des contenus (c_x) dans L des éléments $x \in M$. Dans la famille d'idéaux (c_x) de A il existe un élément maximal (a_1) contenu de $x_1 \in M$ (§ 2, lemme au th.2) ; soit f_1 une forme linéaire sur L telle que $f_1(x_1)=a_1$. Alors $e_1=a_1^{-1}.x_1$ est élément de contenu 1 de L . D'autre part x_1 est de contenu 1 dans M :

s'il était de contenu c dans M , l'élément $c^{-1}x_1$ serait élément de M et de contenu $c^{-1}a_1$ dans L , ce qui, en vertu du caractère maximal de (a_1) implique que c est inversible dans A .Ainsi les sous-modules Ae_1 et Aa_1e_1 sont bien facteurs directs de L et M respectivement.

Soit p le projecteur de L sur Ae_1 défini par $p(z)=f_1(z).e_1$; on a $p(M)=Aa_1e_1$: en effet, si $p(y)=be_1$ et si l'on prend pour d un pgcd de a_1 et de b, on a $d=ua_1+vb$ avec $u\in A$ et $v\in A$ (prop.1, § 2) d'où en posant $z=ux_1+vy$, $p(z)=d.e_1$; or il existe $z'\in L$ tel que $z=c_z.z'$; donc dc_z^{-1} est entier, c_z divise d et donc a_1 ; en vertu du caractère maximal de (a_1) ceci implique $(c_z)=(d)=(a_1)$; donc b est multiple de a_1.

Ainsi L est somme directe de Ae_1 et de $L'=p^{-1}(0)$, et M somme directe de Aa_1e_1 et de $M'=M\cap p^{-1}(0)$. Comme L' est un module libre (th.1 du n°5), et comme M' est de rang n-1, nous pouvons leur appliquer l'hypothèse de récurrence : il existe donc un facteur direct M'_o de L' , une base $(e_2,..,e_n)$ de M'_o et des éléments non nuls $(a_2,...,a_n)$ de A tels que $(a_2e_2,...,a_ne_n)$ soit une base de M' ; et que a_i divise a_{i+1} pour $2\leqslant i\leqslant n-1$; si L'' est un supplémentaire de L'_o dans L' , L est somme directe de L'' et $M_o=M'_o+Ae_1$; alors $(e_1,..,e_n)$ est une base de M_o et $(a_1e_1,...,a_ne_n)$. Il ne nous reste donc plus à montrer que le fait que a_2 est multiple de a_1 .

Or, si on pose $z=a_1e_1+a_2e_2$, on a $z\in M$; de $z=c.z'$ $(c\in A,\ z'\in L)$ on déduit que c divise a_1 et a_2 ; en particulier le contenu (c_z) de z divise (a_1) d'où $(c_z)=(a_1)$ en vertu du caractère maximal de (a_1) ; mais comme c_z divise a_2 , on en déduit que a_2 est multiple de a_1 .

MERDE POUR LES CONTENUS !!! L'ETAT 3 ETAIT MEILLEUR !

Remarque - On en déduit aussitôt que le contenu de tout élément $x \in M$ est multiple du "contenu maximal" (a_1). Dans le cas où M est le sous-module engendré par deux éléments (y,z), nous voyons donc qu'un pgcd de c_y et c_z est le contenu d'une combinaison linéaire de y et z . En particulier si (b_ι) et (b'_ι) sont deux familles d'éléments de A ayant le même ensemble d'indices, il existe u et u' dans A tels que la famille $(ub_\iota + u'b'_\iota)$ ait même pgcd que la famille $(\text{pgcd}(b_\iota , b'_\iota))$.

2) Unicité de M_0 et des idéaux (a_i).

Comme les a_i sont différents de 0, il est clair que M_0 est l'ensemble des $x \in L$ tels qu'il existe $m \neq 0$ dans A tel que $mx \in M$; autrement dit M_0/M est le sous-module de torsion de L/M . Ceci détermine M_0 de façon unique.

Comme L est somme directe de M_0 et d'un supplémentaire L", L/M est somme de M_0/M et de $L''+M$ M , somme qui est directe puisque $M_0 \cap (L''+M)=M$; d'autre part $L''+M/M$ est isomorphe à $L''/(M \cap L'') = L''$, ce qui montre que c'est un module libre isomorphe à L/M_0.

Enfin, au moyen de la base (e_1), on voit que M_0/M est isomorphe à la somme directe des n modules monogènes $A/(a_i)$. Parmi les idéaux (a_i) soit r le nombre de ceux qui sont égaux à A : les r premiers idéaux (a_i) sont ainsi égaux à A , les n-r derniers en étant distincts. Alors L/M_0 est aussi isomorphe à la somme directe des modules $A/(a_n),..,A/(a_{r+1})$ où $(a_n) \subset (a_{n-1}) \subset \ldots \subset (a_{r+1}) \neq A$. Nous sommes donc dans les conditions d'application du cor. de la prop.2 (n^o1) : l'entier n-r et les idéaux (a_i) sont donc déterminés de façon unique.

Corollaire 1 - Pour qu'un sous-module M de rang fini d'un module libre L sur un anneau principal A soit facteur direct de L , il faut et il suffit que L/M soit sans torsion.

Avec les notations du th.3, si L/M est sans torsion, on a $M=M_0$, et M_0 est facteur direct de L ; si, réciproquement M est facteur de L , L/M est isomorphe à un sous-module de L (supplémentaire de M), et est donc un module libre (th.2) et, a fortiori, sans torsion.

Corollaire 2 - Tout module de type fini E sur un anneau principal A est isomorphe à une somme directe de modules monogènes A/I_s en nombre fini m, où les I_s sont des idéaux de A tels que $I_1 \subset I_2 \subset \dots \subset I_m \neq A$, et sont déterminés de façon unique par ces conditions.

En effet, si E peut être engendré par N générateurs, il est isomorphe à un module quotient L/M où $L = A^N$; comme M est de rang fini $n \leqslant N$, nous sommes dans les conditions d'application du th.3, E est donc isomorphe à la somme directe du module de torsion M_0/M et du module libre L/M_0 ; ce dernier est de la forme A^p (où, d'ailleurs, p=N-n) et p, rang du module quotient de E par son module de torsion, est déterminé de façon unique par E . On aura donc $I_s=(0)$ pour $1 \leqslant s \leqslant p$. Quant aux idéaux suivants, ce sont les (a_t) du th.3, dont la suite est déterminée de façon unique.

Corollaire 3 - Tout module de type fini sur un anneau principal est somme directe de son module de torsion et d'un module libre.

Ceci a été démontré dans la démonstration du cor.2 . On notera que, si le sous-module de torsion est unique, il n'en est pas de même du module libre qui en est supplémentaire.

De ceci on déduit aussitôt :

Corollaire 4 - Sur un anneau principal, tout module sans torsion et de type fini est un module libre de rang fini.

Le th. 3 permet de poser la définition suivante :

Définition 7 - Les hypothèses et les notations étant celles du th.3, les éléments a_i de A sont appelés les facteurs invariants du sous-module M du module L .

Les facteurs invariants sont donc bien déterminés à des facteurs inversibles dans A près. Dans le cas, très fréquent en pratique, où l'anneau A est, soit Z, soit un anneau de polynomes $K[X]$, les conventions du § 2 ($n^o 2$ et $n^o 3$) permettent de déterminer entièrement les facteurs invariants : ce seront des entiers > 0 (resp. des polynomes unitaires).

Nous étudierons le cas où A est un anneau de polynomes dans le § suivant. Un groupe abélien sans opérateurs étant canoniquement muni d'une structure de module unitaire sur Z (chap.II, § 1, $n^o 1$), nous pouvons lui appliquer les résultats précédents ; étant donnée l'importance de ce cas, nous énoncerons à nouveau, pour A=Z, les cor.2 et 3 :

Théorème 4 - Soit G un groupe abélien engendré par des éléments en nombre fini. Alors G est somme directe d'un sous-groupe isomorphe à Z^p et du sous-groupe fini F formé des éléments d'ordre fini de G ; F est somme directe de groupes cycliques d'ordres $n_1, n_2, \ldots, n_q$, où les n_i sont des entiers > 1 dont chacun divise le précédent. Dans ces conditions F, p, q et les n_i sont déterminés de façon unique par G .

Exemple - Si K est un complexe simplicial fini, les groupes d'homologie à coefficients entiers $H_n(K)$ sont, pour toute dimension n, des groupes abéliens à un nombre fini de générateurs. $H_n(K)$ est donc somme directe d'un sous-groupe isomorphe à $Z^{p(n)}$ et de son sous-~~mm~~groupe de torsion, lui-même somme directe de groupes cycliques d'ordres $t_1(n), \ldots, t_{q_n}(n)$ tels que $t_i(n)$ divise $t_{i-1}(n)$; p(n) est appelé le n-ème nombre de Betti de K, et les $t_i(n)$ $(1 \leqslant i \leqslant q_n)$ sont appelés les coefficients de torsion

de X en dimension n . C'est cette application topologique qui est à l'origine des mots "sous module de torsion".

Remarque - Si les ordres $n_1,\dots,n_q$ des groupes cycliques dont F est la somme directe sont bien déterminés par la condition de divisibilité du th.4, il n'en est pas de même de ces sous-groupes eux-mêmes (même à une permutation près) : ainsi, dans le produit G de Z (p) par lui-même (p:premier), les sous-groupes sont identiques aux sous-espaces vectoriels sur le corps $Z/(p)$, et G est somme directe de sous-espaces de dimension 1 de $p(p+1)$ façons distinctes.

7 - Applications linéaires de modules libres et matrices sur un anneau principal.

A étant un anneau principal, considérons une application linéaire f d'un A-module libre L de rang m dans un A-module libre L' de rang n . Les résultats précédents permettent d'élucider la nature de f, et, par un choix convenable des bases dans L et L', de mettre la matrice de f sous une forme particulièrement simple, dite forme canonique de cette matrice.

Proposition 4 - Soit A un anneau principal, et f une application linéaire de rang r d'un A-module libre L de rang m , dans un A-module libre L' de rang n . Il existe alors des bases (e_i) $(1 \leqslant i \leqslant m)$ et (e'_j) de L et L' telles que $f(e_i)=a_i e'_i$ pour $1 \leqslant i \leqslant r$, et $f(e_i)=0$ pour $i > r$, les a_i étant des éléments non nuls de A dont chacun divise le suivant les a_i sont les facteurs z invariants de $f(L)$ dans L', et dans les conditions précédentes, sont déterminés de façon unique (à des facteurs inversibles dans A près) .

Corollaire - Soit X une matrice de rang r, à n lignes et m colonnes, sur un anneau principal A . Il existe alors une matrice X_0 équivalente à X (chap.II, § 6, n°10, déf.6) et de la forme

$$\begin{pmatrix} a_1 & 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & a_2 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & 0 & a_3 & \dots & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & a_r & 0 & \dots & & 0 \\ 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 \end{pmatrix}$$

les a_i étant des éléments non nuls de A dont chacun divise le suivant ; X_o est déterminée de façon unique par ces conditions, à des facteurs inversibles de A près pour les a_i . Les a_i sont appelés les facteurs invariants de la matrice X . Pour que deux matrices $\underset{r}{X}$ et X' à n lignes et m colonnes sur un anneau principal soient équivalentes, il faut et il suffit donc qu'elles aient même rang et mêmes facteurs invariants (à des facteurs inversibles dans A près).

Etant donné que les matrices X et X' sont dites équivalentes s'il existe des matrices carrées inversibles P et Q sur A , d'ordres n et m , telles que X' = PXQ, le corollaire n'est que la traduction matricielle de la prop.4 : en effet X et X' sont les matrices de la même application linéaire par rapport à deux couples de bases de L et L'. Reste donc à démontrer la prop.4 .

Soit $L_o = f^{-1}(0)$ le noyau de f ; L/L_o est isomorphe au module f(L) qui est libre en tant que sous-module de L' (th.2,n°5) ; L_o est donc facteur direct de L, et admet un supplémentaire L_1 sur lequel f induit un isomorphisme sur f(L) = M . Le rang r de M (et de L_1) est aussi le rang de l'application linéaire $\bar{f}$ de $L_{(K)}$ dans $L'_{(K)}$ (K : corps des fractions de A) qui prolonge canoniquement f ; on dira que r est le rang de f . [N-B : le rédacteur propose de vider cette explication ecurille qui interrompt le fil des idées ; le lecteur saura trop bien ce que doit

être le "rang de f" après les trop longues gammes bourbachiques du début du n°5]. Si (a_i) $(1 \leqslant i \leqslant r)$ sont les facteurs invariants de M dans L', le th.3 montre qu'il existe une base (e'_j) $(1 \leqslant j \leqslant n)$ de L' telle que $(a_i e'_i)$ $(1 \leqslant i \leqslant r)$ soit une base de M . Comme f induit un isomorphisme de L_1 sur M , il existe donc une base (e_i) $(1 \leqslant i \leqslant r)$ de L_1 telle que $f(e_i) = a_i e_i$. Et on complètera cette base de L_1 en une base (e_k) $(1 \leqslant k \leqslant n)$ de L au moyen d'une base (e_s) $(r+1 \leqslant s \leqslant n)$ du noyau L_0 .

On dit souvent que les a_i sont les <u>facteurs invariants</u> de l'application linéaire f . On notera qu'ils dépendent <u>essentiellement</u> du module L' contenant l'image $M = f(L)$; si, par exemple, on prend $L' = M$, les facteurs invariants sont tout égaux à 1 ; on peut cependant remplacer L' par un module L" contenant L' et tel que L/M et L'/M aient même sous-module de torsion, sans changer les facteurs invariants de f .

On remarquera que dans le cas où A est un corps, les résultats ci-dessus sont triviaux. Il n'en est pas de même du problème de la <u>similitude</u> (chap.II, §6, n°11) de deux matrices carrées sur un corps, problème que nous traiterons au § suivant.

Passons maintenant au calcul des facteurs invariants d'une matrice X sur un anneau principal A :

<u>Proposition 5</u> - <u>Soit</u> X <u>une matrice non nulle de rang</u> r <u>sur un anneau principal</u> A , <u>et soit</u> (a_i) $(1 \leqslant i \leqslant r)$ <u>la suite de ses facteurs invariants. Alors</u> a_1 <u>est le pgcd des éléments de</u> X ; <u>et le pgcd des mineurs d'ordre</u> p <u>de</u> X <u>est</u> $a_1 \ldots a_p$ <u>pour</u> $p \leqslant r$, <u>et</u> 0 <u>pour</u> $p > r$.

Les mineurs d'ordre p de X sont les éléments de la puissance extérieure p-ème de X (chap.III, §6, n°3) ; si f est une application linéaire ayant X pour matrice (par rapport à des bases convenables), $\bigwedge^p X$ sera la matrice de $\bigwedge^p f$ (par rapport à des bases dont la nature, qui ne

nous importe pas ici, est précisée au chap.III, § 6, n°3). Si donc la première assertion ("égalité du pgcd des éléments d'une matrice et de son premier facteur invariant") est démontrée, nous en conclurons que le pgcd des mineurs d'ordre p de X ne dépend que de f, et donc ne change pas si on remplace X par une matrice équivalente. Nous pourrons donc calculer ce pgcd sur la matrice X_0 du cor. de la prop.4 . On voit aussitôt que les seuls mineurs non nuls de X_0 sont les mineurs "diagonaux" $X_{K,H}$ où K=H est une partie de $[1,r]$, tous les autres ayant au moins une ligne nulle ; or, parmi les mineurs d'ordre p ($\leqslant r$) de cette nature, celui où $H=[1,p]$ divise tous les autres en vertu des relations de divibilité des a_i, et est bien égal à $a_1 a_2 \ldots a_p$.

Reste donc à démontrer l'égalité du pgcd des éléments d'une matrice et de son premier facteur invariant. Reprenons les notations de la prop.4 X étant la matrice de f pour des bases (u_i) et (v_j) de L et L'. Il est clair que $f(L) \subset a_1 L'$, et que $f(L) \subset aL'$ entraîne que a divise a_1 (en effet ceci entraîne $a_1 e'_1 = ax$ avec $x \in L'$). Donc a_1 est le pgcd des coordonnées, par rapport à (v_j) de tous les éléments de f(L), donc aussi le pgcd de toutes les coordonnées, par rapport à (v_j), des éléments d'un système de générateurs de f(L). Or les éléments d'un tel système sont, par exemple, ceux dont les coordonnées sont données par les <u>colonnes</u> de la matrice X (chap.III, § 6, n°3), d'où le résultat.

8 - <u>Diviseurs élémentaires</u>.

Soit E un module de torsion de type fini sur un anneau principal A . Le th.1 (n°3) et le cor.2 du th.3 (n°6) nous fournissent <u>deux décompositions</u> de E en somme directe, l'une en facteurs locaux E_p (déf.5) qui sont déterminés de façon unique, -l'autre en facteurs monogènes $A/(a_i)$ où $a_i \neq 0$, $(a_i) \neq A$, et où a_{i+1} divise a_i pour tout i ; ici les facteurs $A/(a_i)$ sont seulement déterminés à un isomorphisme près.

De ces décompositions de E nous pouvons déduire des décompositions plus fines de deux manières différentes :

1) On applique à chaque facteur local E_p le cor.2 du th.3 : E_p est donc somme directe de modules monogènes $A/(b_i)$; comme il existe un entier n tel que $p^n E_p = (0)$, tous les b_i sont des diviseurs de p^n, donc des puissances de p .

On remarquera que, si A_p désigne le sous-anneau du corps des fractions de A formé des x/y où $x \in A$, $y \in A$, $y \notin (p)$, E_p est muni d'une structure de A_p-module, et admet les mêmes sous-modules qu'on le considère comme module sur A ou sur A_p. Comme A_p est un anneau principal dont les seuls idéaux sont les (a^s) et forment une suite totalement ordonnée par inclusion, la démonstration du th.3 se simplifie considérablement dans ce cas.

2) On applique à chaque facteur monogène $A/(a_1)$ la décomposition en facteurs locaux du th.1 . Or l'ensemble des $x \in A$ tels que $p^n x \mid a_1$ pour certaine puissance p^n d'un entier irréductible donné p est l'idéal $(p^{-n(p)}a_1)$ où $n(p)$ est l'exposant de p dans la décomposition de a_1 en facteurs irréductibles (§ 2, th.2). Donc le facteur p-local de $A/(a_1)$ est $(p^{-n(p)}a_1)/(a_1)$, qui est un A-module isomorphe à $A/(p^{n(p)})$ par l'isomorphisme induit par $x \to p^{n(p)}a_1^{-1}.x$.

Dans les deux cas le module E est <u>somme directe de modules de la forme</u> $A/(p^n)$ où p est un entier irréductible de A . Pour montrer l'unicité (à un isomorphisme près) des facteurs de cette décomposition, nous poserons d'abord la définition suivante :

<u>Définition</u> 8 - <u>Un module</u> M <u>sur un anneau</u> A <u>quelconque est dit décomposable s'il est somme directe de deux sous-modules distincts de</u> E <u>et de</u> (0), <u>indécomposable dans le cas contraire.</u>

Remarquons (chap.I, § 6, n°6) que, pour qu'un module monogène A/I soit décomposable, il faut et il suffit qu'il existe des idéaux I' et I", distinct de A et tels que $I = I' \cap I''$ et $A = I' + I''$, A/I étant alors isomorphe à la somme directe de A/I' et A/I" . Dans le cas où A est anneau d'intégrité, l'idéal l=(0) ne peut avoir cette propriété, sinon I' et I" se composeraient de diviseurs de zéro ; A est donc alors un A-module indécomposable. Dans le cas où A est un anneau principal, on a I=(a), I'(a'), I"=(a"), et les conditions ci-dessus expriment que a est un ppcm et 1 un pgcd de a' et a" ; donc (chap.VI, § 1, n°8, prop.7, DIV) a est associé au produit a'a" des deux éléments étrangers a' et a" ; ceci ne sera possible que si plusieurs entiers irréductibles distincts divisent a . Par conséquent :

Proposition 6 - Sur un anneau principal A les seuls modules indécomposables sont isomorphes à A ou $A/(p^n)$ où p est un entier irréductible de A et n un entier naturel.

L'analyse du début de ce n° nous montre donc que, par les méthodes 1) et 2), nous obtenons des décompositions de E comme somme directe de modules indécomposables.

Proposition 7 - Sur un anneau principal A tout module de torsion de type fini E est somme directe de modules indécomposables $A/(p^n)$ où les p sont irréductibles. Dans de telles décompositions le nombre $m(p^n)$ de fois où figure $A/(p^n)$ est déterminé de façon unique.

Définition 9 - Les puissances p^n d'éléments irréductibles de A telles que $m(p^n) > 0$ sont appelées les diviseurs élémentaires du module E , et les entiers $m(p^n)$ leurs multiplicités.

E étant de type fini ne peut être somme directe d'une infinité de modules non réduits à (0), puisque chaque élément de E n'a qu'un nombre fini de composants non nuls ; donc les facteurs $A/(p^n)$ sont en nombre fini.

Considérons la somme F_p de tous ces facteurs relatifs à un même élément irréductible p ; il est clair que F_p est un sous-module du facteur p-local E_p de E ; mais, comme E est à la fois somme directe des E_p et des F_p, on a $F_p = E_p$. Enfin, comme F_p est somme directe de modules $A/(p^n)$ tels que la famille des idéaux (p^n) correspondants soit totalement ordonnée par inclusion, on déduit l'unicité de ceux ci au moyen du cor. de la prop.2 .

Remarques - 1) Si E est un groupe abélien fini, on note la nature de ce groupe en écrivant à la file ses diviseurs élémentaires. On dira par exemple que le groupe E est "du type (2,2,4,27,27,25)" (ou que c'est un groupe (2,2,4,27,27,25)) s'il est isomorphe à la somme directe de deux groupes $Z/(2)$, d'un groupe $Z/(2^2)$, de deux groupes $Z/(3^3)$, et d'un groupe $Z/(5^2)$.

2) La proposition 7 s'étend à un A-module de type fini quelconque M car celui-ci est somme directe de son sous-module de torsion E et d'un module libre isomorphe à A^r ; celui-ci est bien somme directe de r modules isomorphes à A , et donc indécomposables (prop.6). Leur nombre qu'on appelle quelquefois la <u>multiplicité du diviseur élémentaire</u> 0) est déterminé de façon unique, car c'est le rang du module libre M/E .

3) Avec les notations de la prop.7 soient $p^{n(p,1)}, p^{n(p,2)}, \ldots, p^{n(p,s)}, \ldots$ les diviseurs élémentaires du module de torsion E, figurant chacun autant de fois que l'indique sa multiplicité, les exposants $n(p,i)$ formant une suite <u>décroissante</u> d'entiers ; on pose $n(p,i)=0$ pour $i > \sum_n m(p^n)$. Considérons alors les éléments $a_i = \prod_p p^{n(p,i)}$. Il est clair que a_{i+1} divise a_i, et que E est somme directe des modules $A/(a_i)$. Par conséquent les a_i sont les <u>facteurs invariants</u> du module E . Ainsi pour le groupe (2,2,4,27,27,25) de l'exemple 2), les suites $p^{n(p,i)}$ s'écrivant (4,2,2,1,...), (27,27,1,1,...), (25,1,1,1), et les facteurs invariants sont 270, 54 et 2 .

- A -

DIVISIBILITÉ

Plan de l'état 4.

CHAP.VI - GROUPES et CORPS ORDONNES.

§ 1 - Groupes ordonnés ; Divisibilité.
1 - définition des monoïdes et groupes ordonnés.
2 - Monoïdes et groupes préordonnés.
3 - Eléments positifs.
4 - Groupes filtrants.
5 - Relations de divisibilité dans un corps.
6 - Opérations élémentaires sur les groupes ordonnés.
7 - Représentations croissantes de groupes ordonnés.
8 - Bornes supérieure et inférieure dans un groupe ordonné. Groupes réticulés.
9 - Le théorème de décomposition.
10 - Partie positive et partie négative.
11 - Eléments étrangers.
12 - Eléments minimaux.

§ 2 - Corps ordonnés. (pour mémoire).

CHAP.VII - MODULES SUR LES ANNEAUX PRINCIPAUX.

§ 1 - Modules et anneaux noethériens.
Repoussé dans un chapitre ultérieur.

§ 2 - Anneaux principaux.
1 - Divisibilité dans les anneaux principaux.
2 - Anneau des entiers rationnels.
3 - Anneaux de polynomes à une indéterminée sur un corps.

§ 3 - Modules sur les anneaux principaux.
1 - Sommes directes finies de modules monogènes.
2 - Facteurs directs et projecteurs.
3 - Modules de torsion sur un anneau principal.
4 - Décomposition canonique des nombres rationnels et des fractions rationnelles à une indéterminée.
5 - Modules libres sur un anneau principal.
6 - Modules de type fini sur un anneau principal.
7 - Applications linéaires de modules libres, et matrices sur un anneau principal.
8 - Diviseurs élémentaires.

§ 4 - Endomorphismes des espaces vectoriels.
1 - Endomorphismes semblables sur un anneau
2 - Endomorphismes et matrices semblables sur un corps.
3 - Application ; base normale d'une extension cyclique.
4 - Propriétés du polynome caractéristique.
5 - Matrices sur un corps algèbriquement clos. Valeurs et vecteurs propres.
6 - Réduction des matrices à la forme triangulaire.

- B -

Commentaire

Le rédacteur livre sans commentaires à la fureur de Son Maître le § des groupes ordonnés, pour lequel il avait des instructions très explicite Il n'en était, hélas, pas de même des deux derniers paragraphes. L'ordre adopté ne satisfait pas le moins du monde le rédacteur, qui ne voit cependant pas de solution nettement meilleure.

Pour le § des "modules sur les anneaux principaux", les n° 3 et 4 (Modules de torsion, décomposition locale, et application) forment un bloco indépendant du reste. Il serait peut être indiqué d'en faire un court § , qui précéderait celui des facteurs invariants (ou le suivrait ??) ; naturellement le n° des diviseurs élémentaires viendrait à la fin du second de ces deux § : Pour la démonstration du th. des facteurs invariants, le rédacteur a essayé à nouveau la méthode des contenus, et, après comparaison avec l'état 3, se range à l'avis de Weil, et trouve aussi que les contenus viennent compliquer les choses inutilement ; si on veut en dire des choses qui ne soient pas partielles, il faut attendre la démonstration du grand théorème ; le mieux, si quelqu'un tient absolument à ce qu'on parle de ces contenus, est de les introduire après le grand théorème (démontré par la méthode Weil).

Pour le § des endomorphismes, le rédacteur a débuté par un mirificque laïus (inspiré de l'état 2), qui annonce des résultats qu'il a ensuite été jugé préférable de mettre en petits caractères (lignes précédant la forme de Jordan). Les résultats demandés par Chevalley ont été insérés. Pour l'ordre des matières, la base normale d'une extension cyclique a été donnée dès que possible ; si on trouve que çà coupe le fil des idées, on peut permuter ce n° avec le n°4 (le N°5 introduisent un autre point de vue, celui des facteurs locaux et des valeurs propres), soit le mettre en fin de § (comme précédemment). Une bonne partie des n° 5 et 6 (facteurs locaux et valeurs propres) réduction à la forme triangulaire ou

ou diagonale) est bien plus élémentaire que les n° 1,2 et 4, et pourrait les précéder ; on caserait alors la forme de Jordan à la fin de l'actuel n°2 ; mais le rédacteur fait l'objection suivante contre ce procédé : la seule "bonne réduction" des matrices est la réduction à la forme diagonale, et c'est une honte que les racines multiples viennent empêcher de faire toujours cette réduction (Que le rédacteur est donc ingrat envers son gagne pain !); il faut donc pouvoir donner au lecteur, dès qu'on parlera de la décomposition diagonale, la condition pour que celle-ci soit possible (prop.9) (il est vrai qu'on pourrait définir le polynome minimal comme annulateur de E_f, mais c'est un peu canularesque de ne pas savoir le calculer, et de ne pas connaître ses relations avec le polynome caractéristique). Enfin on pourrait ajouter au § 6, une remarque disant que la réduction simultannée s'applique aussi bien à un anneau commutatif de matrices (mais c'est si trivial !).

---

§ 4 - Endomorphismes des espaces vectoriels.

Soit E un espace vectoriel de dimension finie n sur un corps K et f un endomorphisme de E . Nous nous proposons de décomposer E en une somme directe de sous-espaces, globalement invariants pour f, et de plus petites dimensions possible, - et de ramener ainsi l'étude de f à celle d'endomorphismes plus simples. Alors, par rapport à une base convenable de E (une base "adaptée à la décomposition directe"), la matrice $\underline{A}$ de f se mettra sous la forme d'un "tableau diagonal" de matrices (chap.II, § 6), et réciproquement. Notre problème équivaut donc à celui de trouver, étant donnée une matrice carrée $\underline{B}$ d'ordre n, une matrice $\underline{A}$ semblable à $\underline{B}$ (c'est-à-dire telle que $\underline{B} = \underline{PAP}^{-1}$, $\underline{P}$ étant une matrice inversible d'ordre n ; chap.II, § 6, n°11), et se présentant sous la forme d'un tableau diagonal de matrices. Ceci nous amène donc à étudier le problème de la similitude de deux matrices, et, plus généralement, de deux applications linéaires de modules sur un anneau commutatif quelconque.

1 - Endomorphismes semblables sur un anneau.

Nous considèrerons dans ce n° des modules unitaires sur un anneau commutatif A ayant un élément unité.

Définition 1 - On dit que deux endomorphismes f, f' de deux A-modules E, E' sont semblables s'il existe un isomorphisme g de E sur E' tel que $f' = g \circ f \circ g^{-1}$.

On observera que si E et E' ont des bases de n éléments, il revient au même de dire que les matrices $\underline{X}$ et $\underline{X}'$ de f et f' par rapport à ces bases sont semblables (chap.II, § 6, n°9, prop.6) .

Pour tout endomorphisme $f \in \mathcal{L}(E)$ et tout $x \in E$, nous conviendrons de noter multiplicativement la loi externe $(f,x) \to f(x)$, c'est-à-dire d'écrire $f.x$ au lieu de $f(x)$, - et aussi la loi de composition interne $(f,g) \to f \circ g$, c'est-à-dire d'écrire $fg.x$ au lieu de $(f \circ g)(x)$.

En particulier, pour $f \in \mathscr{L}(E)$, f^0 désignera l'automorphisme identique de E (qui est élément unité de l'anneau $\mathscr{L}(E)$), et f^n désignera l'endomorphisme de E défini par récurrence par $f^{n+1} = f \circ f^n$. Dans ces conditions E devient, par la loi externe $(f,x) \longrightarrow f.x$, un module à gauche sur l'anneau (en général non commutatif) $\mathscr{L}(E)$, et, par conséquent, sur tout sous-anneau de celui-ci.

En particulier, si f est un endomorphisme donné de E, E admet une structure de module à gauche sur le sous-anneau de $\mathscr{L}(E)$ engendré par f et les homothéties, c'est-à-dire sur $A[f]$. $A[f]$ est un anneau commutatif, et E est un A_f-module normal (ou fidèle ; chap.II, § 1, n°1). Mais, comme on préfère l'intégrité à la fidélité, on considère A_f comme un anneau quotient de l'anneau de polynomes $B = A[X]$ (f étant la classe de X ; chap.IV, § 2, n°3) ; au moyen de la loi externe $(p,x) \longrightarrow p(f).x$ $(p \in B,\ x \in E)$ on peut donc définir sur E une structure de module (à gauche) sur l'anneau commutatif $B = A[X]$; on désignera par E_f l'ensemble E muni de cette structure de B-module ainsi définie à partir de l'endomorphisme f.

Proposition 1 - *f et f' étant des endomorphismes des A-modules E et E', une condition nécessaire et suffisante pour que f et f' soient semblables, est que E_f et $E'_{f'}$ soient des $A[X]$-modules isomorfes.*

En vertu de la déf.1 la similitude de f et f' veut dire qu'il existe un isomorphisme g de E sur E' tel que $f' = g \circ f \circ g^{-1}$, et on en déduit aussitôt la prop.1 par transport de structures.

La prop.1 se laisse ainsi généraliser :

Proposition 2 - *f et f' étant des endomorphismes des A-modules E et E', une condition nécessaire et suffisante pour qu'une application A-linéaire g de E dans E' soit telle que $g \circ f = f' \circ g$ est que g soit une application $A[X]$-linéaire de E_f dans $E'_{f'}$.*

En effet, le fait que g soit $A[X]$-linéaire veut dire que l'on a $g(p(f).x) = p(f').g(x)$ pour tout $p \in A[X]$; or ceci sera vérifié dès que ce le sera pour p de degré 0 et pour $p=X$. Pour p de degré 0, on a $p=a \in A$, et la condition veut dire que g est A-linéaire ; pour $p=X$, la condition s'écrit $g \circ f = f' \circ g$.

Remarquons que l'application $(p,x) \to p(f).x$ est <u>bilinéaire</u> (sur A) et définit donc une application linéaire Φ du produit tensoriel $A[X] \otimes E$ dans E (chap.III, § 1, n°2, scholie). Posant $B = A[X]$, on voit aussitôt que Φ est l'application B-linéaire du B-module $E_{(B)}$, déduit de E par extension en B de l'anneau d'opérateurs A , sur E_f définie par $\Phi(1 \otimes x) = x$. Nous allons étudier le <u>noyau</u> N de Φ . N est, par définition, le A-module engendré par les éléments $p \otimes x - 1 \otimes p(f).x$, où $p \in B$ et $x \in E$; comme ceux-ci sont nuls lorsque p est un polynome de degré 0, on peut, par linéarité, se borner au cas où p est un multiple qX de X ; comme $qX \otimes x - 1 \otimes q(f)f.x = q(X \otimes x - 1 \otimes f(x))$ au sens de la structure de B-module de $B \otimes E$, le noyau N est le B-module engendré par les éléments $X \otimes x - 1 \otimes f(x)$, où x parcourt E . On a ainsi démontré le résultat suivant :

<u>Proposition 3</u> - <u>Soient</u> : f <u>un endomorphisme d'un</u> A-<u>module</u> E, - $B = A[X]$, - E_f <u>l'ensemble</u> E <u>muni de la structure de</u> B-<u>module définie par la loi</u> $(p,x) \to p(f).x$ $(p \in B , x \in E)$, - $E_{(B)}$ <u>le</u> B-<u>module déduit de</u> E <u>par extension en</u> B <u>de l'anneau d'opérateurs</u> A <u>de</u> E , - Φ <u>l'application</u> B-<u>linéaire de</u> $E_{(B)}$ <u>sur</u> E_f <u>déterminée par</u> $\Phi(1 \otimes x) = x$ <u>pour</u> $x \in E$, - $\mathcal{H}$ <u>le</u> B-<u>endomorphisme de</u> $E_{(B)}$ <u>défini par</u> $\mathcal{H}(1 \otimes x) = X \otimes x - 1 \otimes f(x)$ <u>pour</u> $x \in E$. <u>Alors</u> $\Phi^{-1}(0) = \mathcal{H}(E_{(B)})$ <u>et</u> E_f <u>est isomorphe à</u> $E_{(B)} / \mathcal{H}(E_{(B)})$.

<u>Corollaire</u> - <u>Les hypothèses étant les mêmes que dans la prop.3, soient</u> f' <u>un endomorphisme du</u> A-<u>module</u> E', <u>et</u> $\mathcal{H}$ <u>le</u> B-<u>endomorphisme de</u> $E'_{(B)}$

déduit de f' comme $\mathcal{H}$ l'est de f . Alors, pour que f et f' soient semblables, il faut et il suffit qu'il existe deux B-isomorphismes Ω , Ω_1 de $E_{(B)}$ sur $E'_{(B)}$ tels que $\mathcal{H}' = \Omega \circ \mathcal{H} \circ \Omega_1^{-1}$.

En effet l'existence de ces deux isomorphismes montre, par passage aux quotients, que E_f et $E'_{f'}$ sont isomorphes, donc que f et f' sont semblables (prop.1). Si réciproquement f et f' sont semblables, il existe un isomorphisme g de E sur E' tel que $f' = g \circ f \circ g^{-1}$ (déf.1), dont le prolongement G est un isomorphisme de $E_{(B)}$ sur $E'_{(B)}$ qui satisfait évidemment à $\mathcal{H} = G \circ \mathcal{H} \circ G^{-1}$.

Par extension de la terminologie utilisée pour les matrices (chap.II, § 6, n°10, déf.6) on dit parfois que deux endomorphismes tels que $\mathcal{H}$ et $\mathcal{H}'$ sont équivalents. Il résulte de la démonstration du cor. que, si $\mathcal{H}$ et $\mathcal{H}'$ sont équivalents, ils sont semblables ; bien entendu cette propriété tient à la manière très particulière dont $\mathcal{H}$ et $\mathcal{H}'$ ont été définis, car l'équivalence n'entraîne pas la similitude pour des endomorphismes quelconques.

Corollaire 2 ("théorème de Hamilton-Cayley"). - Les notations étant celles de la prop.3, on suppose que E admet une base de n éléments ; alors $E_{(B)}$ admet une base de n éléments (sur B), et le déterminant de l'endomorphisme est un polynome $\chi_f(X)$ de $A[X]$ tel que $\chi_f(f) = 0$.

Il est clair que, si (e_i) est une base de E (sur A), $(1 \otimes e_i)$ est une base de $E_{(B)}$ sur B (Chap.III, § 2, n°2, th.1). Par définition du déterminant d'un endomorphisme (chap.III, § 6, déf.1), on a, dans la puissance extérieure n-ème de $E_{(B)}$

$$\chi_f(X)((1 \otimes x_1) \wedge \ldots \wedge (1 \otimes x_n)) = (X \otimes x_1 - 1 \otimes f(x_1)) \wedge \ldots \wedge (X \otimes x_n - 1 \otimes f(x_n))$$

Or le premier membre est égal à $(\chi_f(X) \otimes x_1) \wedge (1 \otimes x_2) \wedge \ldots \wedge (1 \otimes x_n)$.

Or l'application g de $E_{(B)}$ sur E définie par $p(X) \otimes x \longrightarrow p(f).x$ pour $x \in E$ est linéaire pour les structures de A-modules de $E_{(B)}$ et E ; l'algèbre extérieure de $E_{(B)}$ se déduisant de celle de E par extension de A en B de l'anneau d'opérateurs, on peut transformer par g les deux membres de l'identité ci-dessus ; comme $g(X \otimes x - 1 \otimes f(x))$ est nul, on en déduit dans $\bigwedge^n E$, l'identité (2)

$$(\chi_f(f).x_1) \wedge x_2 \wedge \dots \wedge x_n = 0 \quad \text{pour tous } x_1, \dots, x_n \text{ de } E .$$

Si $\chi_f(f).x_1$ n'était pas nul, on pourrait choisir $x_2, \dots, x_n$ de telle sorte que les éléments $\chi_f(f).x_1, x_2, \dots, x_n$ soient linéairement indépendants, en contradiction avec l'identité (2) ; on a donc $\chi_f(f).x_1 = 0$ pour tout $x_1 \in E$, c'est-à-dire $\chi_f(f) = 0$.

Remarque - Si $U = (u_{ij})$ est la matrice de f par rapport à une base (e_i) de E, celle de Ⓜ par rapport à la base $(1 \otimes e_i)$ de $E_{(B)}$ est la matrice $X.1_n - U = (\delta_{ij}X - u_{ij})$; $\chi_f(X)$ est alors le déterminant $\det(X.1_n - U) = \boxed{\delta_{ij}X - u_{ij}}$; on l'appelle le polynome caractéristique de f (ou de U) .

2 - Endomorphismes et matrices semblables sur un corps.

Le résultat essentiel du n° précédent (cor.1 de la prop.3) est le suivant : la similitude des endomorphismes f et f' sur l'anneau A équivaut à l'équivalence des endomorphismes Ⓜ et Ⓝ sur l'anneau de polynomes $A[X]$. Dans le cas où A est un corps commutatif K, E est un espace vectoriel sur K, que nous supposerons de dimension finie; alors $E_{(B)}$ (où $B = K[X]$) est un B-module libre à base finie. Comme B est un anneau principal, nous sommes dans les conditions d'application des critères d'équivalence de n°7, § 3, ce qui va nous permettre d'obtenir des résultats assez complets.

Définition 2 - Soit f un endomorphisme d'un espace vectoriel E de dimension finie n sur un corps commutatif K , et U la matrice de f par rapport à une base (e_i) de E . Les facteurs invariants p_i de la matrice $X.1_n - U$ sur l'anneau $K[X]$ sont appelés les facteurs invariants de l'endomorphisme f , ou de la matrice carrée U sur le corps K .

Conformément aux conventions du § 2, n°3, les facteurs invariants seront des polynomes unitaires, ce qui les détermine sans ambiguité.

Le cor.1 de la prop.3 du n°1 se traduit alors ainsi :

Théorème 1 - Pour que deux endomorphismes f,f' de deux espaces vectoriels E,E' soient semblables (ou pour que les matrices U, U' de f,f' par rapport à des bases quelconques de E,E' soient semblables), il faut et il suffit qu'elles aient mêmes facteurs invariants.

La matrice $X.1_n - U$ est (remarque au cor.2, prop.3, n°1) celle de l'endomorphisme Φ de $E_{(S)}$ défini à la prop.3 du n°1. Si $U = (a_{ij})$, son déterminant $\det(\delta_{ij}X - u_{ij})$ est évidemment un polynome unitaire de degré n , donc $\neq 0$. Ainsi la matrice $X.1_n - U$ est de rang n . Par conséquent les facteurs invariants p_i de f (ou de U) sont n polynomes unitaires de X , de degrés $\geqslant 0$, dont chacun divise le suivant. On peut les déterminer au moyen de la prop.5 (§ 3, n°7). En particulier leur produit est égal au déterminant de la matrice $X.1_n - U$, et la somme de leurs degrés est n .

Définition 3 - Les hypothèses et les notations étant celles de la déf.2, on appelle polynome caractéristique de f , ou de U, et on note $\chi_f = \chi_f(X)$, ou $\chi_U = \chi_U(X)$, le déterminant de la matrice $X.1_n - U$:

$$\chi_f = \chi_U = \det(X.1_n - U) = \boxed{\det(\delta_{ij}X - u_{ij})} .$$

Les racines de ce polynome, dans une cloture algèbrique de K (ou dans une extension algèbrique de K ou il se décompose en facteurs de degré 1), sont appelées les racines caractéristiques, ou les valeurs

propres de f , ou U . Le facteur invariant de plus haut degré p_n est appelé le polynome minimal de f , ou de U .

Le polynome caractéristique χ_f est ainsi un polynome unitaire de degré n , égal au produit $p_1 \cdots p_n$ des facteurs invariants de f . Toute racine de l'un des p_i , dans K ou dans une extension, est donc une racine caractéristique. D'ailleurs, comme chaque p_i divise le polynome minimal p_n , χ_f divise $(p_n)^n$; le polynome caractéristique et le polynome minimal de f ont donc mêmes racines, dans K ou dans toute extension.

Proposition 4 - Pour que deux endomorphismes f,f' de deux espaces vectoriels soient semblables, il faut qu'ils aient même polynome caractéristique ; cette condition est suffisante si ce polynome est sans facteurs multiples (dans $K[X]$).

La nécessité résulte du th.1 . D'autre part, comme p_i divise p_n et que $\chi_f = p_1 \cdots p_n$, χ_f est multiple de p_i^2 pour $1 \leqslant i \leqslant n-1$; si donc il n'a pas de facteur multiple dans $K[X]$, on a $p_i = 1$ pour $1 \leqslant i \leqslant n-1$, et $p_n = \chi_f$; la suite des facteurs invariants est donc déterminée par la donnée de χ_f , d'où la suffisance par le th.1 .

Remarque - Le polynome caractéristique est attaché d'une manière invariante à la classe des endomorphismes semblables à f (ou des matrices semblables à U). On peut d'ailleurs vérifier facilement ceci par calcul direct : si P est une matrice inversible et si $U' = PUP^{-1}$, on a aussi $X.1_n - U' = P(X.1_n - U)P^{-1}$. Les coefficients de ce polynome sont donc aussi de tels invariants ; nous les étudierons au n°suivant

Proposition 5 - Soit f un endomorphisme d'un espace vectoriel de dimension finie n sur un corps K ; pour qu'on ait $p(f)=0$, p étant un polynome de $K[X]$, il faut et il suffit que p soit multiple du polynome minimal p_n de f .

En effet, dire que $p(f)=0$, équivaut à dire que p est élément de l'annulateur du $K[X]$-module E_f. Or E_f est somme directe des modules $K[X]/(p_i)$ $(1 \leqslant i \leqslant n)$, et tous les p_i divisent p_n.

Remarque - Comme le polynome caractéristique χ_f est un multiple de p_n, on retrouve un cas particulier du th. de Hamilton-Cayley (cor.2 de la prop.3, n°1) : $\chi_f(f)=0$. On peut d'ailleurs retrouver le cas général (relatif à un anneau A commutatif quelconque) à partir de ce cas particulier (relatif à un corps K), en remarquant que ce théorème s'exprime par des identités algèbriques à coefficients entiers entre les éléments de la matrice carrée étudiée U ; ces identités étant vraies pour la matrice $G = (X_{ij})$, les X_{ij} étant n^2 indéterminées, dont les éléments sont considérés comme éléments du corps de fractions rationnelles $\mathbb{Q}(X_{11},\ldots,X_{nn})$, le principe de prolongement des identités algèbriques (chap.IV, § 2, n°5) montre qu'elles sont vraies pour n^2 éléments quelconques d'un anneau commutatif (avec élément unité) quelconque.

Proposition 6 - Si $p_1,\ldots,p_n$ sont les facteurs invariants d'une matrice carrée U sur un corps K, ce sont encore les facteurs invariants de U sur tout surcorps K' de K.

En effet p_i est le pgcd des mineurs d'ordre i de $X.1_n - U$ (§ 3, n°7, prop.5) et un pgcd de polynomes est indépendant du corps de base choisi (prop.5, n° 3, § 2).

Corollaire - Si deux matrices carrées U et U' sur un corps K sont semblables sur un surcorps K' de K, elles le sont sur K.

Remarque - Si K est un corps infini, on peut démontrer comme suit le cor. de la prop.6. Par hypothèse il existe une matrice carrée inversible P sur K' telle que $PU = U'P$; si n est l'ordre de U, U', P, cette relation s'exprime par un système de n^2 équations linéaires

à coefficients dans K, par rapport aux n^2 coefficients de P ; et il s'agit d'en trouver une solution P', à coefficients dans K, et telle que P' soit inversible. Or d'après le th.1, n°3, § 5, chap.II, il existe des matrices P_i sur K telles que toute solution P' de $P'U = U'P'$ sur K' soit combinaison linéaire des P_i ; en particulier on aura $P = \sum_i x_i P_i$ avec $x_i \in K'$. Si les X_i sont des indéterminées, soit $D(X)$ le déterminant de la matrice $\sum_i X_i P_i$ sur $K[X_i]$; comme le déterminant $D(x)$ de P n'est pas nul le polynome $D(X)$ est $\neq 0$, et, puisque K est infini, il existe des éléments x'_i de K tels que $D(x') \neq 0$ (chap.IV, § 2, n°5, th.3), et la matrice $P' = \sum_i x'_i P_i$ répond à la question.

3 - Application : base normale d'une extension cyclique.

Nous avons démontré (chap.V, § 10, n°9, th.5) que toute extension galoisienne finie N d'un corps infini K, admet une base normale. Nous allons maintenant démontrer ce théorème dans le cas où K est quelconque (fini ou non) et où N est une extension cyclique de K, ce qui s'appliquera à une extension quelconque N d'un corps fini, puisqu'une telle extension est cyclique (chap.V, § 11, n°4, prop.5). Cette démonstration est due à Artin.

Soit $\mathcal{G}$ le groupe de Galois (cyclique) de N, n son ordre, f un générateur de $\mathcal{G}$; f est un endomorphisme de N considéré comme espace vectoriel de dimension n sur K ; il lui correspond donc (n°1) un $K[X]$-module N_f, le produit $p.x$, où $p = \sum_k a_k X^k$ appartient à $K[X]$, étant égal à $\sum_k a_k f^k(x)$. Comme, par hypothèse, on a $f^n = 1$, $X^n - 1$ est multiple de l'annulateur p_n de N_f, c'est-à-dire du polynome minimal de f (n°2, prop.5) ; or le degré m de celui-ci est $\geqslant n$, sinon on aurait $\sum_{k=0}^{n-1} b_k f^k(x) = 0$ pour tout $x \in N$, contrairement à l'indépendance linéaire des automorphismes distincts f^k $(0 \leqslant k \leqslant m < n)$ (chap.V, § 7, th.3)

Par conséquent X^n-1 est le polynome minimal de f ; comme il est de degré n , il est égal au polynome caractéristique de f (qui en est un multiple), et les autres facteurs invariants de f sont égaux à 1 ($n^o 2$). Ainsi N_f est isomorphe au $K[X]$-module monogène $K[X]/(X^n-1)$; si $a \in N$ est un générateur de N_f , les n éléments $f^k(a)$ $(0 \leqslant k \leqslant n-1)$ sont, par définition, linéairement indépendants sur K , et forment donc bien une base normale de N .

4 - Propriétés du polynome caractéristique.

Soit f un endomorphisme d'un espace vectoriel E sur K , U la matrice de f par rapport à une base de E , et $\chi_f = \chi_U = \det(X;1_n-U)$ le polynome caractéristique de f . Comme on l'a vu au $n^o 2$, ce polynome et ses coefficients sont attachés de manière invariante à la classe des endomorphismes semblables à f (ou des matrices semblables à U). Les n coefficients de ce polynome sont donc aussi de tels invariants, en particulier le terme constant, qui est $\chi_U(0) = (-1)^n \det.U$, et le coefficient de X^{n-1} ; pour calculer ce dernier remarquons que, dans le développement total d'un déterminant (Chap.III, § 6,$n^o 2$), tout terme co ntenant n-1 facteurs diagonaux les contient tous ; donc, dans $\det.(X.1_n - U) = \det(\delta_{ij} X-u_{ij})$ les termes en X^{n-1} ne proviennent que du produit $\prod_{i=1}^{n} (X-u_{ii})$, et le coefficient de X^{n-1} est par conséquent $-\sum_i u_{1i} = -\mathrm{Tr}(U)$. On a donc :

$$(1) \qquad \chi_U = X^n - \mathrm{Tr}(U)X^{n-1} + \ldots + (-1)^n \det(U) .$$

Proposition 7 - Soit U une matrice carrée d'ordre n sur un corps K et $\chi_U(X) = \prod_{i=1}^{n} (X-a_i)$ la décomposition en facteurs linéaires de son polynome caractéristique (dans une extension convenable Ω de K). Si q est un polynome à coefficients dans K , le polynome caractéristique de la matrice q(U) est donné par

$$(2) \qquad \chi_{q}(U) = \prod_{i=1}^{n} (X - q(a_i))$$

et la trace et le déterminant de $q(U)$ par

$$(3) \qquad Tr(q(U)) = \sum_{i=1}^{n} q(a_i) , \quad det(q(U)) = \prod_{i=1}^{n} q(a_i) .$$

Nous pouvons supposer que Ω contienne un élément t transcendant sur K , et il nous suffira donc de montrer que l'on a $\chi_{q(U)}(t) = det(t.1_n - q(U)) = \prod_{i=1}^{n} (t - q(a_i))$. Autrement dit, en posant $p = t - q$, nous sommes ramenés à montrer que, pour tout polynome p de $\Omega[X]$, on a $det(p(U)) = \prod_{i=1}^{n} p(a_i)$. Nous pouvons supposer que, dans $\Omega[X]$, p(X) se décompose en facteurs linéaires $p(X) = c \prod_{j=1}^{m} (X - b_j)$. On a donc $p(U) = c \prod_{j=1}^{m} (U - b_j)$, l'ordre des facteurs étant indifférent puisque l'anneau $\Omega[U]$ est commutatif en tant qu'image homomorphe de $\Omega[X]$. En prenant le déterminant, il vient $det(p(U)) = c^n \prod_{j=1}^{m} det(U - b_j.1_n) =$ $= c^n \prod_{i,j} (a_i - b_j) = \prod_{i} p(a_i)$. La relation (2) est ainsi démontrée, et les relations (3) s'en suivent aussitôt.

Corollaire 1 - Si $q \in K[X]$, une condition nécessaire et suffisante pour q(U) soit inversible est que q soit étranger à χ_U .

En effet, dire que q est étranger à χ_U , équivaut à dire que q et χ_U n'ont aucune racine commune dans une extension algèbriquement close de K (§ 2, prop.5), c'est-à-dire que $det(q(U)) \neq 0$ d'après la formule (3).

Corollaire 2 - Si $r \in K(X)$ est une fraction rationnelle à coefficients dans K , une condition nécessaire et suffisante pour que U soit substituable dans r , est que chacune des racines caractéristiques a_i le soit; lorsqu'il en est ainsi on a les formules :

$$\chi_{r(U)} = \prod_{i} (X - r(a_i)) , \quad Tr(r(U)) = \sum_{i} r(a_i), \quad det(r(U)) = \prod_{i} r(a_i) .$$

Soit $r = p/q$ où p et q sont des polynomes étrangers. La première assertion résulte du cor.1 . Soit donc q étranger à χ_U ; il existe alors, d'après l'identité de Bézout, des polynomes g et h tels que $1 = qg + h\chi_U$;

on a alors $1 = q(a_i)g(a_i)$, et $1_n = q(U)g(U)$ (cor.2 de la prop.3) ; d'où $q(U)^{-1} = g(U)$ et $r(U) = p(U)g(U)$. Les racines caractéristiques de $r(U)$, comptées avec leurs multiplicités, sont donc les $p(a_i)g(a_i) = r(a_i)$.

Corollaire 3 - *On a, pour tout entier* $s \geqslant 0$, $\mathrm{Tr}(U^s) = \sum_{i=1}^{n} a_i^s$; *cette formule est valable pour* $s < 0$ *pourvu que* U *soit inversible*.

C'est un cas particulier de (3) appliqué au polynome ou à la fraction rationnelle X^s.

Si K est un corps de caractéristique nulle, la résolution des "formules de Newton" (chap.V,app.I,n°3) permet donc d'exprimer les fonctions symétriques des a_i en fonction des nombres $\mathrm{Tr}(U^s)$ pour $1 \leqslant s \leqslant n$.

Corollaire 4 - *La matrice* $X.1_n - U$ *est inversible dans l'anneau des matrices carrées sur le corps, et on a* (χ'_U désignant la dérivée du polynome χ_U) : $\mathrm{Tr}((X.1_n - U)^{-1}) = \chi'_U(X)/\chi_U(X)$.

Ceci est un cas particulier de (3).

5 - *Matrices sur un corps algébriquement clos. Valeurs et vecteurs propres*

Définition 4 - *f étant un endomorphisme d'un espace vectoriel E sur K, et U la matrice de f relative à une base de E, on dit qu'un élément* $x \in E$ *est un vecteur propre de f* (ou de U) *s'il existe* $a \in K$ *tel que* $f(x) = ax$.

Cherchons les éléments $a \in K$ tels qu'il existe un vecteur propre non nul $x \in E$ satisfaisant à $f(x) = ax$; ceci veut dire que x est dans le noyau de l'endomorphisme 1-f (1:automorphisme identique de E), donc que ce noyau des $\neq 0$; autrement dit (chap.III, § 6, n°5, th.2) le déterminant de $1.a - f$ est nul. Par conséquent donc les éléments $a \in K$ cherchés ne sont autres que les racines du polynome caractéristique de f, c'est-à-dire les valeurs propres (ou racines caractéristiques de f)

qui appartiennent à K . a étant une valeur propre de f , tout élément $x \in E$ tel que $f(x)=ax$ est appelé un vecteur propre de f attaché à la valeur propre a . Les vecteurs propres attachés à a forment évidemment un sous-espace V_a de E , appelé sous-espace propre relatif à a ; la restriction de f à V_a est une homothétie de rapport a. V_a étant le noyau de $a.1 - f$, sa dimension est n-r si $a.1 - f$ est de rang r .

Nous supposerons désormais que toutes les valeurs propres (a_i) appartiennent à K , ce qui est en particulier le K si cas est algèbriquement clos. Si nous munissons E de la structure de $K[X]$- module définie par $(p,x) \longrightarrow p(f).x$ $(p \in K[X])$ (cf.n°1), le module E_f ainsi défini est un module de torsion (prop.5), dont l'annulateur est le polynome minimal p_n de f . Appliquons à ce module la décomposition en facteurs locaux du th.1 (n°3, § 3) : E_f est alors somme directe des modules locaux M_{m_i} où les m_i sont les facteurs irréductibles du polynome minimal p_n de f . Comme le polynome caractéristique χ_f divise $(p_n)^n$ (n°2), les m_i sont les facteurs irréductibles de χ_f , et sont donc de la forme $X-a_i$ en vertu des hypothèses faites sur K. M_{m_i} , étant l'ensemble des $x \in E$ tels que $(a_i;1 - f)^s(x) = 0$ pour certain exposant s , contient le sous-espace propre V_{a_i} relatif à la valeur propre a_i . Il lui est identique si, et seulement si, l'exposant s peut toujours être pris égal à 1, c'est-à-dire si a_i est une racine simple du polynome minimal p_n .

D'autre part, comme E_f est isomorphe à la somme directe des modules $K[x]/(p_j)$ (les p_j étant les facteurs invariants de f ; cf. n°2), et comme χ_f est le produit des p_i , il résulte de la décomposition de $K[X]/(p_j)$ en facteurs locaux que la dimension (sur K) du module M_{m_i} (où $m_i = X - a_i$) est égale à la multiplicité de a_i considérée comme racine de χ_f . Nous avons donc démontré les résultats suivants.

Proposition 8 - Soit f un endomorphisme d'un espace vectoriel de dimension n sur un corps algèbriquement clos K ; pour toute valeur propre a_i de f, le sous-espace propre V_{a_i} relatif à a_i est contenu dans le sous-espace M_i des vecteurs $x \in E$ annulés par $(1.a_i - f)^s$ pour s assez grand ; E est somme directe des M_i ; la dimension de M_i sur K est égale à la multiplicité de a_i considérée comme racine du polynome caractéristique de f. Pour que l'on ait $M_i = V_{a_i}$, il faut et il suffit que a_i soit racine simple du polynome minimal de f.

Remarque - La conclusion de la prop.8 reste vraie toutes les fois que K contient toutes les valeurs propres de f.

Dans le cas où le polynome minimal de f n'a que des racines simples, E est somme directe des sous-espaces propres V_{a_i}. En choisissant une base (e_j) $(1 \leqslant j \leqslant n)$ de E "adaptée à cette décomposition directe" (c'est-à-dire, n_i désignant la dimension de V_{a_i}, telle que $e_j \in V_{a_i}$ pour $n_1+\ldots+n_{i-1} < j \leqslant n_1+\ldots+n_i$), la matrice U de f par rapport à cette base est la matrice diagonale $(a_j \delta_{jk})$ où $a_j = a_i$ pour $n_1+\ldots+n_{i-1} < j \leqslant n_1+\ldots+n_i$. Nous dirons qu'un endomorphisme g de E est diagonal s'il existe une base de E par rapport à laquelle la matrice de f soit diagonale. Si g est un endomorphisme diagonal, et si $(a_1,\ldots,a_m)$ sont ses valeurs propres distinctes, on déduit, du fait que $V_{a_i} \subset M_i$ et que E est somme directe des V_{a_i}, que l'on a $V_{a_i} = M_i$ pour $1 \leqslant i \leqslant m$, d'où, en vertu de la prop.8.

Proposition 9 - Pour qu'un endomorphisme f d'un espace vectoriel E de dimension n sur un corps algèbriquement clos K soit diagonal, il faut et il suffit que son polynome minimal ait toutes ses racines simples.

Cette condition sera, en particulier, remplie si le polynome caractéristique de f à toutes ses racines distinctes.

Mais cette condition suffisante pour que f soit diagonal n'est nullement nécessaire, comme le montre le cas où f est l'automorphisme identique. (Ah! la jolie scurillité !).

Nous allons maintenant étudier le cas où f n'est plus nécessairement un endomorphisme diagonal de E . Nous aurons besoin pour cela du résultat suivant :

Proposition 10 - Soient f un endomorphisme d'un espace vectoriel E sur un corps (commutatif quelconque) K , et $E_f = \sum_i M_i$ la décomposition du $K[X]$-module E_f en somme directe de sous-modules locaux M_i , le sous-module M_i étant relatif au facteur irréductible m_i du polynome caractéristique de f . Alors le projecteur de E sur M_i relatif à cette décomposition directe est de la forme $q_i(f)$ où $q_i \in K[X]$.

Soit en effet $m_i^{s_i}$ l'annulateur de M_i ; le produit $\prod_i m_i^{s_i}$ est le polynome minimal p_n de f ; et, si l'on pose $p_n = r_i m_i^{s_i}$, les polynomes r_i et $m_i^{s_i}$ sont étrangers. Ecrivons donc l'identité de Bézout $1 = g_i r_i + h_i m_i^{s_i} = q_i + t_i$ où $q_i = g_i r_i$ et posons $u = q_i(f)$ et $v = t_i(f)$. L'endomorphisme v s'annule sur M_i , et u sur $\sum_{j \neq i} M_j$; on a $u+v = 1$ et $uv=0$. En multipliant la relation $u+v = 1$ membre à membre par u (resp. v), on obtient $u^2 = u$ (resp. $v^2 = v$) ; u et v sont donc des projecteurs (§ 3, n°2, déf.2), évidemment associés à M_i et $\sum_{j \neq i} M_j$ dans la décomposition de E en somme directe de ces deux sous-modules.

Revenons maintenant au cas où K est algèbriquement clos. Alors le polynome irréductible m_i est de la forme $X-a_i$ où a_i est une valeur propre de f . Considérons alors le polynome $\sum_i a_i q_i$ et l'endomorphisme $d = \sum_i a_i q_i(f)$; d est évidemment un endomorphisme diagonal, dont la restriction à M_i est l'homothétie de rapport a_i . Posons $n = f-d$; pour tout $x \in M_i$ on a $n^{s_i}(x) = (f-1.a_i)^{s_i}(x) = 0$, s_i désignant l'exposant de $X-a_i$ dans la décomposition du polynome minimal de f en

on facteurs irréductibles. En posant $s = \max(s_i)$, on a donc $n^s(x)=0$ pour tout $x \in E$, donc $n^s = 0$. Par conséquent :

Proposition 11 - Tout endomorphisme f d'un espace vectoriel de dimension finie sur un corps algébriquement clos K peut s'écrire sous la forme $f = d+n$, où d est un endomorphisme diagonal et n un endomorphisme nilpotent de E, appartenant tous deux au sous-anneau $K[f]$ de l'anneau des endomorphismes de E (et, par conséquent, permutables entre eux et avec f).

Forme normale de Jordan - Soit f un endomorphisme d'un espace vectoriel E de dimension n sur un corps algébriquement clos K. Considérons ($n^o 2$) le $K[X]$-module E_f obtenu en munissant E de la loi externe $(p,x) \longrightarrow p(f).x$ ($x \in E$, $p \in K[X]$), et décomposons E_f en somme directe de sous-modules indécomposables (§ 3, $n^o 8$) N_k. Chaque N_k est un sous-espace vectoriel de E stable pour f, et donc, par rapport à une base (e_j) de E adaptée à cette décomposition directe, la matrice U de f se met sous la forme d'un "tableau diagonal de matrices"

$$U = \begin{pmatrix} U_1 & 0 & \dots & 0 \\ 0 & U_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & U_m \end{pmatrix}$$

Or $N_k = N$ est un $K[X]$-module monogène, de la forme $K[X]/(p^s)$ où p est un polynome irréductible (p^s étant un diviseur élémentaire de E_f). Mais, d'après l'hypothèse faite sur K, p est de la forme X-a (a étant une valeur propre de f) et N est isomorphe à $K[X]/(X-a)^s$. Soit u l'homomorphisme de $K[X]$ sur N composé de l'homomorphisme canonique de $K[X]$ sur $K[X]/(X-a)^s$ et de l'isomorphisme de ce module quotient sur N. Les éléments $e_i = u((X-a)^{s-i})$ $(1 \leqslant i \leqslant s)$ forment une base de N sur K

Et on a $f(e_i) = X.u((X-a)^{s-i}) = u(X(X-a)^{s-i} = u((X-a)^{s-i+1} + a(X-a)^{s-i}) = u((X-a)^{s-i+1}) + ae_i$. On a donc $f(e_i)=e_{i+1}+a.e_i$ pour $1 \leqslant i \leqslant s-1$, et $f(e_s)=a.e_s$. Par rapport à la base (e_i) de $M = N_k$, la matrice U_k de la restriction de f à N_k est donc

$$U_k = \begin{pmatrix} a & 1 & 0 & \dots & 0 & 0 \\ 0 & a & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & a & 1 \\ 0 & 0 & 0 & \dots & 0 & a \end{pmatrix}$$

Une telle matrice est appelée "matrice de Jordan".

On remarquera que, dans le cas où le polynome minimal de f n'a que des racines simples, tous les diviseurs élémentaires de E_f sont de la forme $(X-a_k)$; alors tous les N_k sont de dimension 1, U_k se réduit à a_k, et la matrice U est une matrice diagonale.

6 - Réduction des matrices à la forme triangulaire.

Définition 5 - On dit qu'une matrice carrée $U = (u_{ij})$ d'ordre n sur un anneau A est triangulaire si on a $u_{ij}=0$ pour $i > j$. (Autrement dit les éléments de U situés en dessous de la diagonale sont nuls).

Si U est la matrice d'un endomorphisme f d'un A-module par rapport à une base (e_i) $(1 \leqslant i \leqslant n)$, le fait que U est triangulaire veut dire que, pour tout i, $f(e_i)$ est élément du sous-module engendré par $(e_1,\dots,e_i)$.

Proposition 12 - Soient $f_1,\dots,f_s$ s endomorphismes permutables d'un espace vectoriel M de dimension finie n sur un corps algébriquement clos K. Il existe alors une base (e_i) de M par rapport à laquelle les s matrices $U_1,\dots,U_s$ de $f_1,\dots,f_s$ soient triangulaires.

Nous démontrerons d'abord le lemme suivant :

Lemme - Si a est une valeur propre de l'endomorphisme f , le sous-espace propre V_a relatif à a est stable pour tout endomorphisme g permutable avec f .

En effet, pour tout $x \in V_a$, on a $f(g(x)) = g(f(x)) = g(ax) = a.g(x)$, ce qui exprime que $g(x) \in V_a$.

Revenons à la prop.12, et montrons d'abord que $f_1,\dots,f_s$ admettent un vecteur propre ($\neq 0$) commun. Ceci est évident pour $s = 1$, puisque K est algèbriquement clos. Procédons alors par récurrence sur s , et supposons que $x \in E$ soit vecteur propre de $f_1,..,f_{s-1}$, relativement aux valeurs propres $a_1,\dots,a_{s-1}$ respectivement ; désignons par $V_1,\dots,V_{s-1}$ les sous-espaces propres correspondants. Ils sont tous stables pour f_s en vertu du lemme ; donc leur intersection V est aussi stable pour f_s . Or V n'est pas réduit à (0) puisqu'il contient x . La restriction de f_s à V admet alors un vecteur propre y, puisque K est algèbriquement clos, et y est le vecteur propre commun cherché.

Ceci étant, nous démontrerons la prop.12 par récurrence sur n , le cas $n=1$ étant trivial. Prenons une base (e_i) de E dont le premier vecteur e_1 soit un vecteur propre commun à $f_1,\dots,f_s$. Par rapport à cette base, la matrice U_j de f_j est de la forme $U_j = \begin{pmatrix} a_j & M_j \\ 0 & P_j \end{pmatrix}$ où a_j est la valeur propre de f_j correspondant à e_1 , où M_j est une matrice à 1 ligne et n-1 colonnes, et où P_j est une matrice carrée d'ordre n-1. En écrivant l'égalité des produits U_jU_k et U_kU_j effectués "par blocs" (chap.II, § 6, n°4), on vérifie aussitôt que l'on a $P_jP_k = P_kP_j$ pour $1 \leqslant j , k \leqslant s$. Considérant alors $P_1,\dots,P_s$ comme matrices de s endomorphismes ~~g~~ permutables $g_1,..,g_s$ de l'espace W de dimension n-1 engendré par $(e_2,\dots,e_n)$, l'hypothèse de récurrence montre qu'il existe une base $(e'_2,\dots,e'_n)$ de W par rapport à laquelle les matrices de $g_1,..g_s$

sont triangulaires. Alors il est clair que par rapport à la base $(e_1, e_2', \ldots, e_n')$ de E, les matrices de $f_1, \ldots, f_s$ sont triangulaires.

Remarque - Si $U=(u_{ij})$ est une matrice triangulaire, il en est de même de $X.1_n - U$; donc le polynome caractéristique $\chi_U = \det(X.1_n - U)$ est égal à $\prod_i (X-u_{ii})$. Ceci montre que, si une matrice carrée M sur un corps (quelconque) K est semblable à une matrice triangulaire sur K, son polynome caractéristique χ_M se décompose en facteurs linéaires dans $K[X]$.

Dans le cas où $f_1, \ldots, f_s$ sont tous des endomorphismes diagonaux (prop.9), on peut préciser la prop.12 :

Proposition 13 - Soient $f_1, \ldots, f_s$ endomorphismes diagonaux et permutables d'un espace vectoriel E de dimension finie n sur un corps algébriquement clos K. Il existe alors une base (e_i) de E par rapport à laquelle les s matrices $U_1, \ldots, U_s$ de $f_1, \ldots, f_s$ soient diagonales.

La proposition étant triviale pour $s=1$, nous procèderons par récurrence sur s. D'après l'hypothèse de récurrence, il existe une base (e_i') de E telle que l'on ait $f_j(e_i') = a_{ji}.e_i'$ pour $1 \leqslant j \leqslant s-1$ avec $a_{ji} \in K$. La relation "$a_{ji}=a_{ji'}$ pour tout $j, 1 \leqslant j \leqslant s-1$" entre les indices i et i' est une relation d'équivalence ; soit L(i) la classe d'équivalence de i. Dire qu'un vecteur $x \in E$ est vecteur propre de $f_1, \ldots, f_{s-1}$ pour les valeurs propres $a_{1i}, \ldots, a_{s-1,i}$ respectivement, équivaut à dire que x appartient au sous-espace $V_{L(i)}$ de E engendré par les vecteurs (e_k') $(k \in L(i))$. Ainsi E est somme directe des $V_{L(i)}$, chaque $V_{L(i)}$ étant intersection de s-1 sous-espaces, propres pour $f_1, \ldots, f_{s-1}$ respectivement. Donc, en vertu du lemme à la prop.12, $V_{L(i)}$ est stable pour f_s. Comme le polynome minimal p_n de f_s n'a pas de racines multiples par hypothèse (prop.9), il en est de même du polynome minimal de la restriction de f_s à L(i), qui est un facteur de

de p_n puisque c'est l'annulateur du sous-module $V_{L(i)}$ du $K[X]$-module E_{f_s} dont p_n est l'annulateur (prop.5, n°2). Il existe donc (prop.9) une base (e_k) $(k \in L(i))$ de $V_{L(i)}$ par rapport à laquelle la matrice de la restriction de f_s soit diagonale. Comme les restrictions de $f_1, \ldots, f_{s-1}$ à $V_{L(i)}$ sont, par construction, des homothéties, leurs matrices par rapport à n'importe quelle base de $V_{L(i)}$, et par rapport à (e_k) en particulier, sont des multiples scalaires de la matrice unité, c'est-à-dire des matrices diagonales. Par conséquent la base (e_i) de E, obtenue par réunion des bases (e_k) $(k \in L(i))$ des $V_{L(i)}$ qui viennent d'être construites, répond aux conditions de l'énoncé.

Nous allons, pour terminer, donner une application de la prop.12 aux produits tensoriels :

<u>Proposition</u> 14 - <u>Soient</u> U <u>et</u> V <u>deux matrices carrées sur un corps</u> K, <u>et</u> $\chi_U = \prod_{i=1}^{n}(X-a_i)$ <u>et</u> $\chi_V = \prod_{j=1}^{m}(X-b_j)$ <u>les décompositions en facteurs linéaires des polynomes caractéristiques</u> χ_U <u>et</u> χ_V <u>de</u> U <u>et</u> V <u>dans une extension convenable</u> Ω <u>de</u> K. <u>Alors le polynome caractéristique</u> $\chi_{U\otimes V}$ <u>du produit tensoriel</u> $U\otimes V$ <u>de</u> U <u>et</u> V <u>est donné par</u>

$$\chi_{U\otimes V} = \prod_{i,j}(X - a_i b_j).$$

Si U' est semblable à U, U'⊗V est semblable à U⊗V (chap.III, § 1, n°6). Sur Ω, U est semblable à une matrice triangulaire (prop.12). Comme le polynome caractéristique d'une matrice reste tel par toute extension du corps de base, il suffit de faire la démonstration dans le cas où $U = (u_{ij})$ est une matrice triangulaire. Dans ce cas, en vertu de la remarque à la prop.12, les a_i ne sont autres que les u_{ii}, à une permutation près ; après avoir au besoin fait une permutation sur les a_i, on peut donc supposer que l'on a $u_{ii} = a_i$, c'est-à-dire que U est de la forme

$$U = \begin{pmatrix} a_1 & u_{12} & \dots & u_{1n} \\ 0 & a_2 & \dots & u_{2n} \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a_n \end{pmatrix}$$

Alors (chap.III, § 1, n°6) $U \otimes V$ peut s'écrire sous la forme du "tableau triangulaire de matrices"

$$U \otimes V = \begin{pmatrix} u_1 V & u_{12} V & \dots & u_{1n} V \\ 0 & a_2 V & \dots & u_{2n} V \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a_n V \end{pmatrix}$$

Ainsi on a $\chi_{U \otimes V}(X) = \det(X.1_{mn} - U \otimes V) = \prod_{i=1}^{n} \det(X.1_m - a_i V) =$

$$\prod_{i=1}^{n} \chi_{a_i V}(X) = \prod_{i=1}^{n} \left(\prod_{j=1}^{m} (X - a_i b_j) \right). \quad \text{CQ.F.D.}$$

E FINITA LA COMMEDIA !!
