LIVRE II
ALGEBRE
CHAPITRE VI
RELATION D'ORDRE DANS LES GROUPES, ANNEAUX ET CORPS. DIVISIBILITE (ETAT 2)

Rédaction n° 077

Nombre de pages : 119

Nombre de feuilles : 119

A 77 Delsarte

2

LIVRE II

ALGÈBRE

CHAPITRE VI (Etat 2)

RELATIONS D'ORDRE DANS LES GROUPES, ANNEAUX ET CORPS. DIVISIBILITÉ

Sommaire.

§ 4. Modules de type fini sur un anneau principal. 1 : Modules de type fini et modules noetheriens. 2 : Modules réguliers de type fini sur un anneau principal. 3 : Modules indécomposables de type fini sur un anneau principal. 4 : Facteurs invariants. 5 : Calcul des facteurs invariants. 6 : Structure des groupes abéliens de type fini.

§ 5. Applications de la théorie des diviseurs élémentaires. 1 : Forme canonique d'une matrice sur un anneau principal. 2 : Réduction d'une matrice carrée sur un corps commutatif. 3 : Polynome caractéristique d'une matrice carrée sur un corps commutatif. 4 : Réduction d'une matrice carrée sur un corps algèbriquement fermé. 5 : Application aux équations linéaires sur un corps algèbriquement fermé. 6 : Base normale d'une extension cyclique.

§ 6. Anneaux noetheriens. 1 : Le théorème de Hilbert. 2 : Produit d'idéaux. 3 : Transporteurs d'idéaux. 4 : Idéaux premiers radical d'un idéal. 5 : Idéaux primaires. 6 : Intersections d'idéaux primaires. 7 : Le théorème de Lasker-E.Noether. 8 : Le théorème de Krull.

Commentaires.

Le rédacteur a borné ce chapitre aux questions envisagées dans le plan d'Algèbre "étroite" adopté au Congrès de Nöel 1947. En tout état de cause, les 5 premiers §§ doivent (quant à leur contenu) être substantiellement conservés dans toute rédaction future. En ce qui concerne le § 6 (anneaux noetheriens), il faudrait faire la preuve qu'il appartient bien à l'"Algèbre étroite", ce qui reste douteux aux yeux du rédacteur.

La place du § sur les corps ordonnés est évidemment assez fâcheuse, car il vient interrompre la suite naturelle des idées des §§ 1 et 3 par des considérations dont le lien avec le § 1 est assez ténu. D'autre part, on ne voit absolument pas où mettre ce § dans un autre chapitre (étant donné qu'il a été vomi déjà du chap. sur les corps) ; une suggestion intéressante de Samuel consisterait à mettre ledit § en Appendice à ce chapitre.

N-B - Par économie de temps et de papier, les exercices de ce § n'ont pas été tirés ; ils le seront avec l'état 3 .

LIVRE II

CHAPITRE VI

RELATIONS D'ORDRE DANS LES GROUPES, ANNEAUX ET CORPS. DIVISIBILITÉ (Etat 2)

§ 1. Groupes ordonnés.

Les notions et résultats exposés dans ce paragraphe concernent des groupes abéliens, et plus généralement, des monoïdes commutatifs (chap.I, § 1, n°3) ; dans les applications qu'on en fait en Algèbre, la loi de composition des groupes (ou monoïdes) considérés est le plus souvent notée multiplicativement ; au contraire, les applications à la théorie des espaces vectoriels topologiques, et en particulier à l'Intégration (cf.Livre VII) concernent des groupes additifs. Dans ce paragraphe, nous emploierons exclusivement la notation additive pour la loi de composition des monoïdes considérés, et la notation $x \leqslant y$ pour les relations d'ordre qu'on y considère ; dans la suite du chapitre, la traduction des résultats du § 1 en d'autres notations sera faite chaque fois qu'il y aura lieu.

1. Définition des groupes ordonnés.

DEFINITION 1.- Etant donné un monoïde commutatif E , on dit qu'une structure d'ordre sur E (définie par une relation d'ordre notée $x \leqslant y$) et la structure de monoïde de E sont compatibles si elles satisfont à l'axiome suivant (en notation additive) :

(GO) La relation $x \leqslant y$ entraîne que, pour tout $z \in E$, $x+z \leqslant y+z$.

Un ensemble E muni d'une structure de monoïde commutatif et d'une structure d'ordre compatibles, est appelé monoïde ordonné.

On exprime encore l'axiome (GO) en disant que l'ordre se conserve par toute translation.

Si une structure d'ordre est compatible avec la structure algèbrique d'un monoïde E , il en est de même de la structure d'ordre opposée.

Nous étudierons surtout dans ce paragraphe les groupes ordonnés.

Exemples.- Le groupe additif des nombres rationnels et celui des nombres entiers sont des groupes ordonnés, quand on les munit des structures d'ordre définies au chap.I, § 2, n°5 et § 9, n°5 . En traduisant l'axiome (GO) en notation multiplicative, on voit de même que le groupe multiplicatif des nombres rationnels > 0 est un groupe ordonné (pour la même relation d'ordre).

PROPOSITION 1.- Dans un groupe ordonné G , les relations $x \leqslant y$ et $x+z \leqslant y+z$ sont équivalentes.

En effet, d'après (GO), la relation $x+z \leqslant y+z$ entraîne $(x+z)-z \leqslant (y+z)-z$, c'est-à-dire $x \leqslant y$.

COROLLAIRE 1.- Dans un groupe ordonné, les relations $x < y$ et $x+z < y+z$ sont équivalentes.

En effet, $x < y$ entraîne $x+z \leqslant y+z$ d'après (GO) ; d'autre part, $x+z = y+z$ entraîne $x=y$, donc $x < y$ entraîne $x+z < y+z$; on en déduit comme dans la prop.1 que $x+z < y+z$ entraîne $x < y$.

COROLLAIRE 2.- Dans un groupe ordonné, les quatre relations $x \leqslant y$ $0 \leqslant y-x$, $x-y \leqslant 0$, $-y \leqslant -x$ sont équivalentes.

PROPOSITION 2.- Dans un monoïde ordonné E , soient (x_i), (y_i) deux suites finies de n éléments chacune $(1 \leqslant i \leqslant n)$ telles que $x_i \leqslant y_i$ pour tout indice i ; on a alors $\sum_{i=1}^{n} x_i \leqslant \sum_{i=1}^{n} y_i$ (addition membre à membre des inégalités).

En raisonnement par récurrence sur n , on se ramène aussitôt à prouver la proposition pour $n=2$, c'est-à-dire à montrer que les relations $x \leqslant y$ et $x' \leqslant y'$ entraînent $x+x' \leqslant y+y'$. Or, de $x \leqslant y$, on tire, d'après (GO) $x+x' \leqslant y+x'$, et de $x' \leqslant y'$ on tire de même $y+x' \leqslant y+y'$;

par transitivité, on a donc $x+x' \leqslant y+y'$.

COROLLAIRE.- Dans un groupe ordonné, si on a $x_i \leqslant y_i$ pour tout i , et $x_j < y_j$ pour un indice j au moins, on a $\sum_{i=1}^{n} x_i < \sum_{i=1}^{n} y_i$.

En effet, de $\sum_{i=1}^{n} x_i = \sum_{i=1}^{n} y_i$, on déduirait $y_j - x_j = \sum_{i \neq j} x_i - \sum_{i \neq j} y_i \leqslant 0$ puisque $x_i \leqslant y_i$ pour tout $i \neq j$; ce qui est absurde.

En particulier, les relations $0 \leqslant x_i$ $(1 \leqslant i \leqslant n)$, et $\sum_{i=1}^{n} x_i = 0$ entraînent $x_i = 0$ pour $1 \leqslant i \leqslant n$.

2. Eléments positifs dans un groupe ordonné.

DÉFINITION 2.- Dans un groupe ordonné G (noté additivement), on appelle élément positif (resp. négatif, strictement positif, strictement négatif) tout élément $x \in G$ tel que $x \geqslant 0$ (resp. $x \leqslant 0$, $x > 0$, $x < 0$).

L'ensemble des éléments positifs de G se note G_+ .

Comme les relations $x \geqslant 0$ et $-x \leqslant 0$ sont équivalentes, l'ensemble des éléments négatifs de G n'est autre que $-G_+$.

Les relations $x \geqslant 0$, $y \geqslant 0$ entraînent $x+y \geqslant 0$ (prop.2), autrement dit, on a

$$(1) \qquad G_+ + G_+ \subset G_+ .$$

En particulier, la relation $x \geqslant 0$ entraîne $2x \geqslant 0$, et plus généralement (prop.2) $nx \geqslant 0$ pour tout entier $n > 0$; de même (cor. de la prop.2) $x > 0$ entraîne $nx > 0$.

Il faut noter qu'inversement, la relation $nx \geqslant 0$ pour un entier $n > 1$ n'entraîne pas nécessairement $x \geqslant 0$ (voir ex.1 ci-dessous).

D'autre part, les relations $x \geqslant 0$ et $x \leqslant 0$ entraînent $x = 0$, donc on a

$$(2) \qquad G_+ \cap (-G_+) = \{0\} .$$

Nous allons voir que les propriétés (1) et (2) sont caractéristiques pour l'ensemble des éléments positifs d'un groupe ordonné. De façon précise

PROPOSITION 3.- Soit P une partie d'un groupe abélien G (noté additivement) satisfaisant aux axiomes :

(GP_I) $\quad P+P \subset P$.

(GP_{II}) $\quad P \cap (-P) = \{0\}$.

Il existe alors sur G une structure d'ordre et une seule, compatible avec la structure de groupe de G , et telle que P soit l'ensemble des éléments positifs de G pour cette structure d'ordre.

En effet, s'il existe une structure d'ordre notée $x \leqslant y$ ayant cette propriété, la relation $x \leqslant y$ étant équivalente à $y-x \geqslant 0$, doit être équivalente à $y-x \in P$, ce qui prouve qu'il existe au plus une structure d'ordre répondant à la question. Montrons qu'effectivement, la relation $y-x \in P$ est une relation d'ordre sur G : de (GP_{II}) on déduit que $0 \in P$, donc on a $x-x \in P$ pour tout $x \in G$; les relations $y-x \in P$ et $x-y \in P$ entraînent $x=y$ d'après (GP_{II}) ; enfin, de $y-x \in P$ et $z-y \in P$, on déduit $z-x = (z-y)+(y-x) \in P$ d'après (GP_I). Reste à vérifier que, pour cette relation d'ordre, l'axiome (GO) est satisfait, ce qui est immédiat, puisque $(y+z)-(x+z) = y-x$.

Exemples.- 1) Dans le groupe $\mathbb{Z}$ des entiers rationnels, l'ensemble P formé de 0 et des entiers $\geqslant 2$ satisfait aux axiomes (GP_I) et (GP_{II}) ; pour la structure d'ordre qu'il définit sur $\mathbb{Z}$, on notera qu'on a $2 \geqslant 0$, mais $1 \not\geqslant 0$.

2) Dans le "plan rationnel" $\mathbb{Q} \times \mathbb{Q}$ (ou le plan numérique $\mathbb{R} \times \mathbb{R}$), si on considère l'intersection P de deux "demi-plans fermés", définis respectivement par les inégalités $ax+by \geqslant 0$, $cx+dy \geqslant 0$ (avec $ad-bc \neq 0$), il est immédiat que cet ensemble satisfait à (GP_I) et (GP_{II}). On obtient ainsi une infinité de structures d'ordre compatibles avec la structure de groupe de $\mathbb{Q} \times \mathbb{Q}$ (resp. $\mathbb{R} \times \mathbb{R}$) ; on peut d'ailleurs prendre de même pour P

l'intersection de deux "demi-plans ouverts" $ax+by > 0$, $cx+dy > 0$, ou l'intersection d'un demi-plan ouvert et d'un demi-plan fermé. Le lecteur aura avantage à illustrer par des exemples de cette nature, qui se prêtent à un langage géométrique évident (fig.1) les propriétés générales des groupes ordonnés.

COROLLAIRE.- Pour que la structure d'ordre définie par P soit une structure d'ensemble totalement ordonné, il faut et il suffit que P satisfasse en outre à l'axiome

(GP_{III}) $\quad P \cup (-P) = G$.

On dit alors que G, muni de la structure d'ordre définie par P, est un groupe totalement ordonné.

Exemple.- Considérons, dans le groupe $G = \mathbb{Q} \times \mathbb{Q}$, l'ensemble P formé des points (x,y) tels que $ax+by > 0$, et de ceux tels que $ax+by=0$, $ay-bx \geqslant 0$ ("demi-plan ouvert" augmenté d'une des demi-droites qui le limitent) (fig.2) ; il est clair que P satisfait aux axiomes (GP_I), (GP_{II}) et (GP_{III}), donc définit sur G une structure de groupe totalement ordonné. Lorsque $a=1$, $b=0$, on retrouve l'ordre "lexicographique" dans G (Ens., chap.IV).

3. Semi-groupes et groupes préordonnés.

DÉFINITION 3.- On appelle semi-groupe un monoïde commutatif, ayant un élément neutre, et dont tout élément est régulier.

Toute partie stable d'un groupe abélien, contenant l'élément neutre de ce groupe, est un semi-groupe ; réciproquement, on sait (chap.I, § 2, n°4, th.1) que tout semi-groupe S peut être plongé par symétrisation (d'une seule manière, à une isomorphie près) dans un groupe abélien, dans lequel S est une partie stable, et où tout élément se met sous la forme $y-x$; où $x \in S$ et $y \in S$.

La prop.3 montre que les structures d'ordre compatibles avec la structure de groupe d'un groupe abélien G (noté additivement) correspondent biunivoquement aux <u>semi-groupes</u> P contenus dans G et tels que $P \cap (-P) = \{0\}$.

Si maintenant S est un semi-groupe <u>quelconque</u> contenu dans G la relation $y-x \in S$ n'est plus une relation d'ordre sur G ; mais elle est encore <u>réflexive</u> et <u>transitive</u>, et par suite (<u>Ens</u>. R, § 6, n° 1) on peut en déduire une structure d'ordre sur l'ensemble quotient de G par la relation d'équivalence "$y-x \in S$ et $x-y \in S$" , qui s'écrit aussi "$y-x \in S \cap (-S)$" ; mais $H=S \cap (-S)$ n'est autre que le <u>plus grand sous-groupe</u> de G contenu dans S , ou encore le groupe des éléments <u>symétrisables</u> de S ; l'ensemble quotient dont nous venons de parler est donc le <u>groupe quotient</u> G/H . La relation d'ordre définie sur G/H par passage au quotient n'est autre que la relation $\dot{y}-\dot{x} \in S/H$; comme S/H est un semi-groupe de G/H et que $(S/H) \cap (-S/H)$ est réduit à l'élément neutre de G/H , on obtient ainsi sur G/H une structure de <u>groupe ordonné</u>, pour laquelle S/H est l'ensemble des éléments positifs. On dit que l'ensemble G , muni de la structure de groupe et de la structure définie par la relation $y-x \in S$, est un <u>groupe préordonné</u>.

Pour que la structure d'ordre sur G/H soit une structure d'ensemble <u>totalement ordonné</u>, il faut et il suffit que $S \cup (-S) = G$. On dit alors que G est un groupe <u>totalement préordonné</u>.

Considérons maintenant un semi-groupe S , et soit G le groupe obtenu par symétrisation de S . Si $x \leqslant y$ est une relation d'ordre définie sur S et compatible avec la structure de monoïde de S , l'ensemble P des éléments de S qui sont $\geqslant 0$ satisfait évidemment à (GP_I) et à (GP_{II});

il définit donc sur G une structure d'ordre compatible avec la structure de groupe de G , et induisant sur S la structure d'ordre donnée ; et il est clair que c'est la seule structure d'ordre sur G qui possède ces propriétés.

On notera que c'est de cette manière que nous avons défini la structure d'ordre sur le groupe $\mathbb{Z}$ des entiers rationnels, à partir de la structure d'ordre du semi-groupe $\mathbb{N}$ des entiers naturels (chap.I, § 2, n° 5).

4. Sous-groupes et groupes produits de groupes ordonnés.

Il est évident que la structure d'ordre induite sur un sous-groupe H d'un groupe ordonné G est compatible avec la structure de groupe de H . Lorsque nous considèrerons un tel sous-groupe H comme un groupe ordonné, c'est toujours de cette structure d'ordre induite qu'il sera supposé muni, sauf mention expresse du contraire ; l'ensemble des éléments $\geqslant 0$ dans H est $H \cap G_+$.

Soit (G_ι) une famille de groupes ordonnés ; dans le groupe produit $G = \prod_\iota G_\iota$, considérons la relation "quel que soit ι , $x_\iota \leqslant y_\iota$" entre deux éléments arbitraires (x_ι), (y_ι) ; il est immédiat que cette relation est une relation d'ordre compatible avec la structure de groupe de G ; on la notera $(x_\iota) \leqslant (y_\iota)$. Le groupe ordonné G ainsi défini est appelé le produit des groupes ordonnés G_ι ; l'ensemble G_+ des éléments positifs de G n'est autre que le produit $\prod_\iota (G_\iota)_+$.

Dans le cas où tous les facteurs G_ι sont identiques à un même groupe ordonné G , c'est-à-dire où il s'agit d'un produit de la forme G^E , on voit que ce groupe n'est autre que le groupe des applications de E dans G , où la relation $f \leqslant g$ est équivalente à "quel que soit $x \in E$, $f(x) \leqslant g(x)$" .

Un sous-groupe important du groupe produit $\prod_\iota G_\iota$ est la <u>somme directe</u> des groupes G_ι (chap.II, § 1), identique au produit lorsque l'ensemble d'indices est fini : l'ensemble des éléments $\geqslant 0$ dans ce sous-groupe est formé des (x_ι) tels que $x_\iota = 0$ sauf pour un nombre fini d'indices, et $x_\iota \geqslant 0$ pour ces derniers.

<u>5. Représentations et isomorphismes de groupes ordonnés.</u>

Soient G, G' deux groupes ordonnés. Parmi les représentations f de G dans G', il y a lieu de considérer particulièrement celles pour lesquelles la relation $x \geqslant 0$ dans G entraîne $f(x) \geqslant 0$ dans G' ; comme on a par hypothèse $f(y-x)=f(y)-f(x)$, la condition précédente équivaut à dire que f est une représentation <u>croissante</u> de G sur G', pour les structures d'ordre de ces deux groupes.

Conformément aux définitions générales (<u>Ens.</u> R, § 8) un <u>isomorphisme</u> de la structure de groupe ordonné de G sur celle de G' est un isomorphisme f de la structure de groupe de G sur celle de G', tel que les relations $x \leqslant y$ et $f(x) \leqslant f(y)$ soient <u>équivalentes</u> ; il revient au même de dire que la représentation biunivoque f et la représentation réciproque doivent être toutes deux <u>croissantes</u>.

Une représentation biunivoque de G sur G' peut être croissante sans que la représentation réciproque le soit. Prenons par exemple pour G et G' le groupe $\mathbb{Q} \times \mathbb{Q}$, pour G_+ l'ensemble des (x,y) tels que $y \geqslant 2|x|$, pour G'_+ l'ensemble des (x,y) tels que $y \geqslant |x|$; si f est l'application identique de G sur G', f est croissante, mais sa réciproque ne l'est pas.

<u>6. Groupes filtrants.</u>

Rappelons (<u>Ens.</u> R, § 6) qu'un monoïde ordonné E est <u>filtrant à droite</u> (resp. <u>filtrant à gauche</u>) si, pour tout couple (x,y) d'éléments de E ,

il existe $z \in E$ tel que $x \leqslant z$ et $y \leqslant z$ (resp. $x \geqslant z$ et $y \geqslant z$). Si G est un <u>groupe ordonné filtrant à droite</u>, il est aussi <u>filtrant à gauche</u>, et réciproquement ; en effet, si x,y sont deux éléments quelconques de G , et s'il existe z tel que $-x \leqslant z$ et $-y \leqslant z$, on en déduit $-z \leqslant x$ et $-z \leqslant y$. Nous dirons simplement dans ce cas que G est un <u>groupe filtrant</u>.

PROPOSITION 4.- <u>Pour qu'un groupe ordonné G soit filtrant, il faut et il suffit qu'il soit engendré par l'ensemble G_+ de ses éléments positifs</u> (ou, ce qui revient au même, que tout $x \in G$ puisse s'écrire sous la forme $y-z$, avec $y \geqslant 0$ et $z \geqslant 0$).

En effet, si G est filtrant, pour tout $x \in G$, il existe $y \in G$ tel que $0 \leqslant y$ et $x \leqslant y$, donc $z=y-x \geqslant 0$, et $x=y-z$, où $y \geqslant 0$ et $z \geqslant 0$. Inversement, si G est engendré par G_+ , pour deux éléments quelconques x,y de G , il existe $u \geqslant 0$ et $v \geqslant 0$ tels que $y-x=v-u$, ou $u+y=v+x=z$; comme $u \geqslant 0$ et $v \geqslant 0$, on a $z \geqslant x$ et $z \geqslant y$, donc G est filtrant.

Lorsque G n'est pas filtrant, soit H le sous-groupe de G engendré par G_+ (c'est-à-dire formé par les $y-z$, où $y \geqslant 0$ et $z \geqslant 0$) ; il est clair que H est <u>le plus grand sous-groupe filtrant</u> de G . En outre, si x et y appartiennent à deux classes <u>distinctes</u> modulo H , x et y n'ont ni majorant, ni minorant commun. L'étude de la relation d'ordre dans un tel groupe G se réduit donc à l'étude de la relation d'ordre dans le groupe filtrant H .

Il est immédiat que tout <u>produit</u> et toute <u>somme directe</u> de groupes filtrants est filtrant ; par contre, en général un sous-groupe d'un groupe filtrant n'est pas nécessairement filtrant.

Par exemple, soit G le groupe $\mathbb{Q} \times \mathbb{Q}$, où G_+ est l'ensemble des (x,y) tels que $y \geqslant |x|$; le sous-groupe $H = \mathbb{Q} \times \{0\}$ de G n'est pas filtrant.

7. Groupes réticulés.

Nous dirons qu'un groupe ordonné G est réticulé si sa structure d'ordre est une structure d'ensemble réticulé (Ens. R, § 6) c'est-à-dire si tout couple (x,y) d'éléments de G a une borne supérieure notée sup(x,y) et une borne inférieure notée inf(x,y).

Tout groupe totalement ordonné est évidemment réticulé. Les groupes additifs $\mathbb{Z}$, $\mathbb{Q}^*$ et $\mathbb{R}_*$ sont des groupes de cette nature ; il en est de même des groupes multiplicatifs des nombres rationnels* (resp. réels)$_*$ strictement positifs. Rappelons que pour un ensemble totalement ordonné, on écrit souvent Max (x,y), $\operatorname{Max}_{i \in I} x_i$ (resp. Min (x,y), $\operatorname{Min}_{i \in I} x_i$) au lieu de sup(x,y), $\sup_{i \in I} x_i$ (resp. inf (x,y) ; $\inf_{i \in I} x_i$), lorsque I est un ensemble fini (Ens. R, § 6).

Le produit (resp. la somme directe) d'une famille quelconque (G_ι) de groupes réticulés est un groupe réticulé, car on vérifie aussitôt que l'élément $(\sup(x_\iota, y_\iota))$ est la borne supérieure des éléments (x_ι), (y_ι), et l'élément $(\inf(x_\iota, y_\iota))$ leur borne supérieure. En particulier, tout produit (resp. somme directe) d'une famille (G_ι) de groupes totalement ordonnés est un groupe réticulé, mais non totalement ordonné s'il y a au moins deux G_ι qui ne se réduisent pas à l'élément neutre.

Comme exemple de groupe filtrant non réticulé, citons le groupe $G = \mathbb{Z}$, où on a pris pour G_+ l'ensemble formé de 0 et des entiers $n \geqslant 2$: l'ensemble des x qui sont à la fois $\geqslant 0$ et $\geqslant 1$ a deux éléments minimaux distincts, 3 et 4, donc les deux éléments 0,1 n'ont pas de borne supérieure dans G.

Remarque.- On notera qu'un sous-groupe d'un groupe réticulé n'est pas nécessairement réticulé ; par exemple, le groupe $G = Q \times Q$, où G_+ est formé des couples (x,y) tels que $y \geqslant |x|$, est un groupe réticulé (isomorphe aux produit de deux groupes totalement ordonnés identiques à Q, comme on le vérifie sans peine) ; mais le sous-groupe filtrant $Z \times Z$ de G n'est pas réticulé, car l'ensemble des majorants des deux éléments $(0,0)$ et $(1,0)$ dans ce sous-groupe a deux éléments minimaux distincts $(0,1)$ et $(1,1)$ (fig.2).

PROPOSITION 5.- Dans un groupe réticulé G, on a

$$\inf(x,y) = -\sup(-x,-y). \tag{3}$$

En effet, soit $z=\sup(-x,-y)$; on a $z \geqslant -x$, $z \geqslant -y$, d'où $-z \leqslant x$, $-z \leqslant y$; réciproquement, si $u \leqslant x$ et $u \leqslant y$, on a $-u \geqslant -x$, $-u \geqslant -y$, donc $z \leqslant -u$ ou $u \leqslant -z$, ce qui montre que $-z = \inf(x,y)$.

La proposition peut aussi se démontrer en remarquant que, dans tout groupe ordonné G, $x \to -x$ est un isomorphisme de G sur le groupe ordonné obtenu en munissant G de l'ordre opposé à l'ordre donné.

Comme dans tout ensemble réticulé, les lois de composition sup et inf dans G sont associatives et commutatives (chap.I, §1, n^os 3 et 5) ; plus généralement (Ens., chap.IV), rappelons que, si, dans un ensemble ordonné, une famille $(a_\iota)_{\iota \in I}$ (finie ou non) d'éléments admet une borne supérieure, et si, pour une partition $(I_\lambda)_{\lambda \in L}$ de I, chacune des familles $(a_\iota)_{\iota \in I_\lambda}$ admet aussi une borne supérieure, alors $\sup_{\lambda \in L} (\sup_{\iota \in I_\lambda} a_\iota)$ existe et on a

$$\sup_{\iota \in I} a_\iota = \sup_{\lambda \in L} (\sup_{\iota \in I_\lambda} a_\iota) \tag{4}$$

Inversement, si le second membre de (4) est défini, il en est de même du premier, et on a la relation (4) ; il en est toujours ainsi dans un ensemble réticulé si L est fini et si chacune des bornes supérieures $\sup_{\iota \in I_\lambda} a_\iota$ existe.

On a des propriétés analogues pour les bornes inférieures de parties de G . Rappelons aussi que, si deux familles (x_ι), (y_ι) ont toutes deux une borne supérieure (resp. inférieure) et si on a $x_\iota \leqslant y_\iota$ pour tout ι , on en déduit $\sup_\iota x_\iota \leqslant \sup_\iota y_\iota$ (resp. $\inf_\iota x_\iota \leqslant \inf_\iota y_\iota$).

PROPOSITION 6.- Pour qu'un groupe ordonné filtrant G soit réticulé, il suffit qu'il satisfasse à l'une des deux conditions suivantes :

a) Tout couple d'éléments de G_+ a une borne supérieure (dans G_+).

b) Tout couple d'éléments de G_+ a une borne inférieure (dans G_+) .

a) Il suffit de montrer que tout couple d'éléments (x,y) de G admet une borne supérieure ; en appliquant ce résultat $-x$ et $-y$ on en déduira que $-\sup(-x,-y)$ est la borne inférieure de x et y .

Par hypothèse, on peut écrire $x=z-z'$, $y=t-t'$, où z,z',t,t' sont $\geqslant 0$; on peut en outre supposer $z'=t'$, puisqu'on a aussi $x=(z+t')-(z'+t')$ et $y=(t+z')-(z'+t')$. Les relations $u \geqslant x$, $u \geqslant y$ sont alors équivalentes à $u+z' \geqslant z$, $u+z' \geqslant t$, et en vertu de l'hypothèse, à $u+z' \geqslant \sup(z,t)$; il en résulte que $\sup(z,t)-z'$ est borne supérieure de x et y .

b) Montrons que la condition b) de l'énoncé entraîne a). Soient x,y deux éléments de G_+ ; il existe $a \in G_+$ tel que $a \geqslant x$ et $a \geqslant y$ (par exemple $a=x+y$), donc $a-x \in G_+$ et $a-y \in G_+$; soit b la borne inférieure de $a-x$ et $a-y$; on a $b \leqslant a$ et $x \leqslant a-b$, $y \leqslant a-b$; d'autre part, si $x \leqslant u$ et $y \leqslant u$, on a aussi $x \leqslant \inf(a,u)$, $y \leqslant \inf(a,u)$, d'où $a-\inf(a,u) \leqslant a-x$ et $a-\inf(a,u) \leqslant a-y$; on en tire $a-\inf(a,u) \leqslant b$, c'est-à-dire $a-b \leqslant \inf(a,u) \leqslant u$, ce qui prouve que $a-b$ est borne supérieure de x et y .

La propriété la plus importante des groupes réticulés est la distributivité de l'addition par rapport à chacune des lois sup et inf.

De façon plus générale :

PROPOSITION 7.- Si deux parties non vides A,B d'un groupe ordonné G ont chacune une borne supérieure, A+B a une borne supérieure et on a

(5) $$\sup(A+B) = \sup A + \sup B$$

En effet, soit a=sup A , b=sup B ; quels que soient $x \in A$, $y \in B$, on a $x \leqslant a$, $y \leqslant b$, donc $x+y \leqslant a+b$. D'autre part, si $x+y \leqslant c$ quels que soient $x \in A$ et $y \in B$, on a, pour un $y_0 \in B$ quelconque, $x \leqslant c-y_0$ pour tout $x \in A$, donc $a \leqslant c-y_0$, et par suite $y \leqslant c-a$ quel que soit $y \in B$; cela entraîne $b \leqslant c-a$, autrement dit $a+b \leqslant c$, ce qui achève la démonstration.

COROLLAIRE 1.- Si A_i $(1 \leqslant i \leqslant n)$ sont des parties de G en nombre fini, admettant chacune une borne supérieure, l'ensemble somme $\sum_{i=1}^{n} A_i$ admet une borne supérieure, et on a

(6) $$\sup\left(\sum_{i=1}^{n} A_i\right) = \sum_{i=1}^{n} (\sup A_i)$$

Il suffit d'appliquer la prop.7 par récurrence sur n .

La prop.7 et le cor.1 donnent deux résultats analogues pour les bornes inférieures, que nous laissons au lecteur le soin d'énoncer.

COROLLAIRE 2.- Dans un groupe réticulé l'addition est distributive par rapport à la borne supérieure et à la borne inférieure.

Autrement dit, on a les identités

(7) $$\begin{cases} \sup(x+z,\ y+z) = z+\sup(x,y) \\ \inf(x+z,\ y+z) = z+\inf(x,y) \end{cases}$$

C'est une conséquence immédiate de la prop.7, appliquée aux deux ensembles $\{z\}$ et $\{x,y\}$.

DEFINITION 4.- On dit qu'un monoïde ordonné E est semi-réticulé inférieurement (resp. supérieurement) si tout couple d'éléments (x,y) de E admet une borne inférieure (resp. supérieure), et si l'addition est distributive par rapport à la borne inférieure (resp. borne supérieure).

Cette notion généralise évidemment la notion de <u>groupe réticulé</u> ; au § 6 , nous rencontrerons d'importants exemples de monoïdes semi-réticulés qui ne sont pas des groupes réticulés.

Nous ne considèrerons dans ce qui suit que des monoïdes semi-réticulés <u>inférieurement</u>, que nous appellerons simplement monoïdes <u>semi-réticulés</u> ; on passe aux monoïdes semi-réticulés supérieurement en remplaçant la structure d'ordre par la structure opposée.

Dans un monoïde semi-réticulé, on a

$$\inf(x,z)+\inf(y,z) = \inf(x+\inf(y,z),z+\inf(y,z)) =$$
$$= \inf(\inf(x+y,x+z),\inf(y+z,2z)) = \inf(x+y,x+z,y+z,2z)$$

ou finalement

$$\inf(x,z)+\inf(y,z) = \inf(x+y,z+\inf(x,y,z)) . \tag{8}$$

PROPOSITION 8.- <u>Dans un monoïde semi-réticulé, les relations</u> $x \leqslant z$ <u>et</u> $y \leqslant z$ <u>entraînent</u> $x+y \leqslant z+\inf(x,y)$.

On a en effet alors, dans (8), $\inf(x,z)=x$, $\inf(y,z) = y$ et $\inf(x,y,z) = \inf(x,y)$, d'où la proposition.

COROLLAIRE.- <u>Dans un groupe réticulé</u> G , <u>on a</u>

$$\sup(x,y)+\inf(x,y) = x+y . \tag{9}$$

En effet, la prop.8 montre que $x+y \leqslant \sup(x,y)+\inf(x,y)$. Si on change x en -x et y en -y dans cette inégalité, on obtient l'inégalité opposée d'après la prop.5 .

PROPOSITION 9.- <u>Dans un groupe réticulé</u> G , <u>on a, pour tout entier</u> $n>0$

$$\begin{cases} \sup(nx, ny) = n.\sup(x,y) \\ \inf(nx, ny) = n.\inf(x,y) \end{cases} \tag{10}$$

Il suffit de démontrer la seconde formule (10). En général, dans un monoïde semi-réticulé, on a, d'après la formule générale de distributivité

$$n.\inf(x,y) = \inf(nx,(n-1)x+y,(n-2)x+2y,\dots,x+(n-1)y,ny)$$

d'où, en appliquant de nouveau la distributivité

$$n.\inf(x,y)+\inf(nx,ny)=\inf(2nx,(2n-1)x+y,\dots,x+(2n-1)y,2ny)=2n.\inf(x,y)$$

d'où aussitôt la seconde relation (10) lorsque G est un groupe.

COROLLAIRE 1.- Dans un groupe réticulé G , la relation $nx=0$ pour un entier $n > 0$, entraîne $x=0$ (autrement dit, dans G tout élément est d'ordre infini). (cf. exerc. 3)

On peut se borner au cas où $n > 1$. Alors, on a, d'après (10) et la distributivité de l'addition par rapport à sup

$$x+(n-1)\sup(x,0)=x+\sup((n-1)x,0) = \sup(nx,x) = \sup(x,0)$$

donc $x+(n-1)\sup(x,0) \leqslant (n-1)\sup(x,0)$, c'est-à-dire $x \leqslant 0$; mais alors $\sup(x,0)=0$, et de la relation $x=(2-n)\sup(x,0)$, on tire $x=0$.

COROLLAIRE 2.- Dans un groupe réticulé G , la relation $nx \geqslant 0$ pour un entier $n > 0$, entraîne $x \geqslant 0$.

En effet, on a $nx=\sup(nx,0)=n.\sup(x,0)$, d'où $x=\sup(x,0)$ d'après le cor.1, ce qui entraîne $x \geqslant 0$.

8. Partie positive, partie négative, valeur absolue.

DÉFINITION 5.- Dans un groupe réticulé G , on appelle partie positive (resp. partie négative) d'un élément x , et on note x^+ (resp. x^-) l'élément $\sup(x,0)$ (resp. $\sup(-x,0)$). On appelle valeur absolue de x et on note $|x|$ l'élément $\sup(x,-x)$.

On a évidemment $(-x)^+ = x^-$, $(-x)^-=x^+$. Lorsque G est totalement ordonné, on a $x^+=x$, $x^-=0$, $|x| = x$ si $x \geqslant 0$, $x^+ = 0$, $x^-=-x$, $|x| = -x$ si $x \leqslant 0$.

D'après la prop.5, on a $x^-=-\inf(x,0)$; en remplaçant y par 0 dans (9), on a donc

$$x = x^+ - x^- \quad . \tag{11}$$

En outre :

PROPOSITION 10.- Pour toute décomposition $x=y-z$ d'un élément x d'un groupe réticulé, telle que $y \geqslant 0$ et $z \geqslant 0$, on a $y \geqslant x^+$, $z \geqslant x^-$.

En effet, comme $y=x+z$, on a $y \geqslant x$ et $y \geqslant 0$, donc $y \geqslant x^+ = \sup(x,0)$; d'où $z=y-x \geqslant x^+-x = x^-$.

De la définition de $|x|$, on tire que $|x| \geqslant x$ et $|x| \geqslant -x$, donc $2|x| \geqslant 0$; d'après le cor.2 de la prop.9, il en résulte que $|x| \geqslant 0$. D'autre part, $x^+ + x^- = \sup(x,0)+\sup(-x,0)=\sup(x,-x,0)$ par la distributivité, d'où $x^+ + x^- = \sup(\sup(x,-x),0)=\sup(|x|, 0)$; comme $|x| \geqslant 0$, on a

$$|x| = x^+ + x^- \quad . \tag{12}$$

De cette relation, on déduit que $|x| =0$ entraîne $x=0$ (et que les deux relations sont par suite équivalentes), car de $x^+ + x^- =0$ on déduit $x^+ = -x^- \leqslant 0$, et comme $x^+ \geqslant 0$, on a $x^+=0$, $x^-=0$ et $x=0$ par (11).

On a évidemment d'après la définition de $|x|$, $x+y \leqslant |x|+|y|$ et $-x-y \quad x+y$, d'où (inégalité du triangle)

$$|x+y| \leqslant |x| + |y| \quad . \tag{13}$$

Comme $|-x| = |x|$, on déduit de (13) que $|y| = |x+(y-x)| \leqslant |x|+|y-x|$, et de même $|x| \leqslant |y| + |y-x|$, d'où

$$\big||y| - |x|\big| \leqslant |y-x| \quad . \tag{14}$$

La prop.9 entraîne, pour tout entier $n > 0$

$$(nx)^+ = n.x^+ \quad , \quad (nx)^- = n.x^- \quad , \quad |nx| = n.|x| \quad . \tag{15}$$

Notons enfin que, d'après (7), on peut écrire

$$\begin{cases} \sup(x,y)=x+(y-x)^+= y+(x-y)^+=x+(x-y)^-=y+(y-x)^- \\ \inf(x,y)=x-(y-x)^- =y-(x-y)^- =x-(x-y)^+=y-(y-x)^+ \end{cases} \tag{16}$$

et par suite

$$\begin{cases} 2.\sup(x,y) = x+y+|x-y| \\ 2.\inf(x,y) = x+y-|x-y| \end{cases} \quad . \tag{17}$$

d'où $|x-y| = \sup(x,y)-\inf(x,y)$

PROPOSITION 11.- Dans un groupe réticulé G , si une famille (x_ι) admet une borne inférieure, la famille (x_ι^+) admet aussi une borne inférieure, et on a

$$(18) \qquad (\inf_\iota(x_\iota))^+ = \inf_\iota (x_\iota^+) .$$

Posons $a=\inf_\iota(x_\iota)$; on a $a \leqslant x_\iota$ pour tout ι , donc $a^+ \leqslant x_\iota^+$ pour tout ι . D'autre part, la famille des éléments $-x_\iota^- = \inf(x_\iota,0)$ admet évidemment une borne inférieure, savoir $\inf(\inf_\iota(x_\iota),0)=\inf(a,0)=-a^-$; il en résulte que la famille (x_ι^-) admet une borne supérieure égale à a^- ; or, on a $x_\iota^+ = x_\iota + x_\iota^- \leqslant x_\iota^- + a^-$ pour tout ι ; donc, pour tout élément b tel que $b \leqslant x_\iota^+$ pour tout ι , on a $b \leqslant x + a^-$ pour tout ι , ou $b-a^- \leqslant x_\iota$, et puisque (x_ι) a pour borne inférieure a , $b-a^- \leqslant a$ ou $b \leqslant a+a^- = a^+$, ce qui démontre la proposition.

COROLLAIRE 1.- Dans un groupe réticulé G, si une famille (x_ι) admet une borne inférieure (resp. une borne supérieure), pour tout $z \in G$ la famille $(\sup(z,x_\iota))$ (resp. la famille $(\inf(z,x_\iota))$) admet une borne inférieure (resp. supérieure) égale à $\sup(z,\inf_\iota(x_\iota))$ (resp. $\inf(z,\sup_\iota(x_\iota))$).

En effet, on a $\sup(z,x_\iota)=z+(x_\iota-z)^+$, et la famille $(x_\iota-z)$ admet une borne inférieure.

COROLLAIRE 2.- Dans un groupe réticulé, chacune des lois de composition sup et inf est distributive par rapport à l'autre.

Autrement dit, on a

$$(19) \qquad \begin{cases} \sup(z,\inf(x,y))=\inf(\sup(z,x),\sup(z,y)) \\ \inf(z,\sup(x,y))=\sup(\inf(z,x),\inf(z,y)) \end{cases}$$

C'est une conséquence immédiate du cor.1 appliqué à une famille de deux éléments.

Delsarte 22

9. Eléments étrangers.

Nous considèrerons dans ce n° un monoïde semi-réticulé E , ayant un élément neutre 0 ; nous désignerons par E_+ l'ensemble des éléments $\geqslant 0$ de E ; c'est une partie stable de E pour l'addition et pour la loi de composition inf .

DEFINITION 6.- On dit que n éléments x_i $(1 \leqslant i \leqslant n)$ de E_+ sont étrangers si $\inf(x_1, x_2, \ldots, x_n) = 0$.

Il est clair que si $p < n$ des x_i sont étrangers, les n éléments x_i le sont a fortiori ; mais n éléments de E_+ peuvent être étrangers sans que n-1 quelconques de ces éléments le soient ; pour éviter toute confusion, on dira parfois que n éléments sont "étrangers dans leur ensemble" au lieu de dire simplement qu'ils sont étrangers.

Lorsque deux éléments x,y de E_+ sont étrangers, on dit encore que x est étranger à y et que y est étranger à x .

Si les x_i $(1 \leqslant i \leqslant n)$ sont étrangers, et si (y_i) est une famille de n éléments de E_+ telle que $y_i \leqslant x_i$ pour tout i , on a $0 \leqslant \inf(y_i) \leqslant \inf(x_i)$, donc les y_i sont aussi étrangers.

PROPOSITION 12.- Si x,y,z sont trois éléments de E_+ , on a

(20) $$\inf(x+y, z) \leqslant \inf(x, z) + \inf(y, z)$$

C'est une conséquence immédiate de la formule (8), puisqu'on a $\inf(x, y, z) \geqslant 0$.

PROPOSITION 13.- Si x,y,z sont trois éléments de E_+ étrangers (dans leur ensemble), on a

(21) $$\inf(x+y, z) = \inf(x, z) + \inf(y, z)$$

Cela résulte encore de la formule (8), puisqu'on a $\inf(x, y, z) = 0$.

COROLLAIRE 1.- Si x et y sont étrangers, $x+y$ est la borne supérieure de x et y .

En effet, les relations $z \geqslant x$ et $z \geqslant y$ entraînent, d'après (21) $\inf(x+y,z)=x+y$, donc $z \geqslant x+y$.

COROLLAIRE 2.- Si x et z sont étrangers, on a, pour tout $y \in E_+$

(22) $$\inf(x+y,z) = \inf(y,z)$$

En effet, la formule (21) est applicable, et $\inf(x,z)=0$.

PROPOSITION 14.- Si x,y,z sont trois éléments de E_+ tels que z soit étranger à x et étranger à y , z est étranger à $x+y$.

Cela résulte aussitôt de la formule (22).

COROLLAIRE 1.- Si x et y sont deux éléments étrangers de E_+ , mx et ny sont étrangers quels que soient les entiers $m>0$ et $n>0$.

Il suffit d'appliquer la prop.14 par récurrence sur m et n .

COROLLAIRE 2.- Si $(x_i)_{1 \leqslant i \leqslant m}$ est une famille d'éléments de E_+ deux à deux étrangers, $(y_j)_{1 \leqslant j \leqslant n}$ une famille d'éléments de E_+ deux à deux étrangers, on a

(23) $$\inf\Big(\sum_{i=1}^{m} x_i, \sum_{j=1}^{n} y_j\Big) = \sum_{i,j} \inf(x_i,y_j)$$

Il suffit de raisonner par récurrence sur m et n , en appliquant la prop.13, et remarquant, d'après la prop.14, que x_m est étranger à $\sum_{i=1}^{m-1} x_i$.

PROPOSITION 15 (lemme d'Euclide).- Soient x,y,z trois éléments de E_+ ; si z est étranger à x et si $z \leqslant x+y$, on a $z \leqslant y$.

C'est une conséquence immédiate de la formule (22).

COROLLAIRE.- Si z est étranger à x , l'inégalité $x+z \leqslant x+y$ est équivalente à $z \leqslant y$.

En effet, elle entraîne $z \leqslant x+y$, donc $z \leqslant y$ d'après le prop.15 .

Dans un groupe réticulé, la condition $\sup(x,y)=x+y$, qui, d'après le cor.1 de la prop.13, est toujours nécessaire pour que les éléments positifs x,y soient étrangers, est aussi suffisante, car en vertu de l'identité (9), elle entraîne $\inf(x,y)=0$. On a en outre les propriétés suivantes :

PROPOSITION 16.- Pour tout couple d'éléments x,y d'un groupe réticulé G , $x-\inf(x,y)$ et $y-\inf(x,y)$ sont étrangers.

En effet, ces éléments sont $\geqslant 0$, et on a

$$\inf(x-\inf(x,y),y-\inf(x,y))=\inf(x,y)-\inf(x,y)=0$$

d'après (7).

COROLLAIRE.- Pour tout élément $x\in G$, x^+ et x^- sont étrangers.

En effet, d'après (11), $x^+=x-\inf(x,0)$ et $x^-=0-\inf(x,0)$.

PROPOSITION 17.- Dans un groupe réticulé G , soit (x_ι) une famille d'éléments $\geqslant 0$ admettant une borne supérieure. Si $z\geqslant 0$ est étranger à chacun des x_ι , z est étranger à $\sup_\iota(x_\iota)$.

C'est une conséquence de la formule $\inf(z,\sup_\iota(x_\iota))=\sup_\iota(\inf(z,x_\iota))$ (cor.1 de la prop.11).

10. Eléments minimaux ; éléments premiers ; éléments indécomposables.

Nous considèrons dans ce n° un monoïde ordonné E , ayant un élément neutre 0, et nous désignons toujours par E_+ la partie stable de E formée des éléments $x\geqslant 0$.

DEFINITION 7.- Dans un monoïde ordonné E , on dit qu'un élément $x>0$ est minimal s'il est élément minimal de l'ensemble des éléments >0 de E .

Autrement dit, x est minimal si la relation $0<y\leqslant x$ entraîne $y=x$, ou encore si la relation $0\leqslant y\leqslant x$ entraîne "$y=0$ ou $y=x$" .

Si E est semi-réticulé, deux éléments minimaux distincts sont nécessairement étrangers.

Dans un monoïde totalement ordonné, il y a au plus un élément minimal ; dans le groupe totalement ordonné $\mathbb{Z}$, $+1$ est effectivement un élément minimal ; par contre il n'y a pas d'élément minimal dans le groupe additif $\mathbb{Q}$.

DÉFINITION 8.- Dans un monoïde ordonné E, on dit qu'un élément $x > 0$ est premier si la relation $x \leqslant y+z$, où $y \geqslant 0$ et $z \geqslant 0$, entraîne "$x \leqslant y$ ou $x \leqslant z$".

On en déduit par récurrence sur n que, si $x \leqslant \sum_{i=1}^{n} y_i$, où $y_i \geqslant 0$, il existe un indice i tel que $x \leqslant y_i$.

PROPOSITION 18.- Dans un monoïde semi-réticulé E, tout élément minimal est premier.

En effet, supposons que x soit minimal et que $x \leqslant y+z$, avec $y \geqslant 0$ et $z \geqslant 0$. On a $0 \leqslant \inf(x,y) \leqslant x$, donc $\inf(x,y)=x$ ou $\inf(x,y)=0$; dans le premier cas on a $x \leqslant y$; dans le second x et y sont étrangers et $x \leqslant y+z$, donc (prop.15), on a $x \leqslant z$.

Au contraire, dans un groupe ordonné mais non réticulé un élément minimal pout ne pas être premier. Par exemple, le groupe $G = \mathbb{Z} \times \mathbb{Z}$, où G_+ est l'ensemble des (m,n) tels que $n \geqslant |m|$, est non réticulé; l'élément $(0,1)$ est évidemment un élément minimal (ainsi d'ailleurs que $(1,1)$ et $(-1,1)$) ; mais on a $(0,1) \leqslant (0,2)=(1,1)+(-1,1)$, donc $(0,1)$ n'est pas premier.

PROPOSITION 19.- Dans un groupe ordonné G, tout élément premier est minimal.

En effet, supposons que $x > 0$ soit premier, et soit tel que $0 \leqslant y \leqslant x$; on peut écrire $x=y+(x-y)$, avec $y \geqslant 0$ et $x-y \geqslant 0$; donc on a, soit $x \leqslant y$, et alors $y=x$, soit $x \leqslant x-y$, et alors $y \leqslant 0$, donc $y=0$.

Dans un groupe réticulé, les notions d'élément minimal et d'élément premier sont donc identiques.

Au § 6, nous étudierons d'importants exemples de monoïdes semi-réticulés où il y a des éléments premiers non minimaux ; nous verrons aussi que deux éléments premiers x,y peuvent être tels que $0 < x < y$ dans un tel monoïde.

DÉFINITION 9.- Dans un monoïde semi-réticulé E , un élément $x > 0$ est dit indécomposable si les relations $x=y+z$, $\inf(y,z)=0$ entraînent "$x=y$ ou $x=z$" .

On notera que la relation $x=y+z$ entraîne alors $y=0$ ou $z=0$. En effet, si $x=y$, on a $\inf(x,z)=0$; mais $z \leqslant y+z=x$, donc $z=0$; de même si $x=z$, on a $y=0$.

Il résulte aussitôt des définitions que si x est premier il est indécomposable ; plus généralement :

PROPOSITION 20.- Dans un monoïde semi-réticulé E , si x est premier, nx est indécomposable pour tout entier $n > 0$.

En effet, supposons qu'on ait $nx=y+z$, avec $\inf(y,z)=0$; on a $x \leqslant nx = y+z$, donc $x=\inf(x,y+z)=\inf(x,y)+\inf(x,z)$ (prop.13) ; comme x est premier, on a $x = \inf(x,y)$ ou $x = \inf(x,z)$; supposons par exemple $x = \inf(x,y)$, c'est-à-dire $x \leqslant y$, et par suite $\inf(x,z)=0$; comme z est étranger à x , il est étranger à nx (cor.1 de la prop.14) ; la relation $nx = y+z$ entraîne alors $nx \leqslant y$ (prop.14), d'où $nx=y$ et $z=0$.

11. Groupes décomposables.

Un groupe réticulé G qui est monogène et non réduit à l'élément neutre, est nécessairement infini d'après le cor.1 de la prop.9 . Si a est un élément engendrant G , comme G_+ n'est pas réduit à 0 par hypothèse, il existe un entier n , positif ou négatif, tel que $na > 0$; si $n > 0$, on en déduit $a > 0$ (cor.2 de la prop. 9), et si $n < 0$, $a < 0$, et dans ce dernier cas, on a $-a > 0$, et $-a$ engendre G . Donc, G est isomorphe au groupe totalement ordonné $\mathbb{Z}$ des entiers rationnels.

DÉFINITION 10.- On dit qu'un groupe ordonné est décomposable s'il est somme directe ($n^o 4$) d'une famille de sous-groupes totalement ordonnés isomorphes à $\mathbb{Z}$.

Autrement dit, un groupe décomposable est un groupe ordonné isomorphe à un groupe de la forme $\mathbb{Z}^{(I)}$, où I est un ensemble d'indices quelconque.

Le groupe $\mathbb{Z}^{(I)}$ est réticulé, comme toute somme directe de groupes réticulés ; soit (e_ι) sa base canonique quand on le considère comme $\mathbb{Z}$-module, c'est-à-dire (chap.II, §1, n°8) que e_ι est l'élément de $\mathbb{Z}^{(I)}$ dont toutes les coordonnées sont nulles, à l'exception de celle d'indice ι, qui est égale à 1 ; tout élément $x \in \mathbb{Z}^{(I)}$ se met d'une manière et d'une seule sous la forme $x = \sum_{\iota \in I} n_\iota e_\iota$, où $n_\iota \in \mathbb{Z}$ ($n_\iota = 0$ sauf pour un nombre fini d'indices), et la relation $x \geqslant 0$ est équivalente à "quel que soit $\iota \in I$, $n_\iota \geqslant 0$". On en déduit aussitôt que les e_ι sont les éléments minimaux (ou les éléments premiers, ce qui revient au même (prop.18 et 19)) de $\mathbb{Z}^{(I)}$.

THÉORÈME 1.- *Pour qu'un groupe ordonné G soit décomposable, il faut et il suffit que tout élément minimal de G soit premier, et que G satisfasse à la condition suivante :*

(T) *Toute suite minorée décroissante (x_n) d'éléments de G n'a qu'un nombre fini de termes distincts* (autrement dit, on a $x_{n+1} = x_n$ à partir d'un certain rang).

Les conditions sont nécessaires ; la première résulte en effet de la prop.18. D'autre part, pour montrer que $\mathbb{Z}^{(I)}$ vérifie la condition (T), il suffit de prouver que pour deux éléments quelconques a,b de $\mathbb{Z}^{(I)}$ tels que $a \leqslant b$, le nombre des éléments x tels que $a \leqslant x \leqslant b$ est fini ; on peut se borner au cas où $a = 0$; alors, si $b = \sum_\iota b_\iota e_\iota$, on a $b_\iota = 0$ sauf pour les ι appartenant à une partie finie H de I ; la relation $0 \leqslant x \leqslant b$ équivaut à $0 \leqslant n_\iota \leqslant b_\iota$ pour tout ι, si $x = \sum_\iota n_\iota e_\iota$; on en tire $n_\iota = 0$ pour $\iota \notin H$ et $0 \leqslant n_\iota \leqslant b_\iota$ pour $\iota \in H$; il n'y a donc qu'un nombre fini de familles (n_ι) d'entiers satisfaisant à ces conditions.

Les conditions sont suffisantes. Soit x un élément >0 quelconque de G ; si x n'est pas minimal, il existe $x_1 \in G$ tel que $0<x_1<x$; s'il n'existait aucun élément minimal y tel que $0<y<x$ on pourrait donc définir par récurrence une suite (x_n) telle que $0<x_{n+1}<x_n<x$ pour tout entier n , ce qui contredit l'axiome (T). Il existe donc un élément minimal $p_1<x$. Si $x-p_1$ n'est pas minimal, il existe de même p_2 minimal tel que $p_2<x-p_1$; on définit ainsi par récurrence une suite (p_i) d'éléments minimaux telle que $p_1+p_2+\ldots+p_k<x$ pour tout indice k ; cela n'est possible que si la suite (p_i) est finie, sans quoi la suite des $y_n=x-(p_1+\ldots+p_n)$ contredirait l'axiome (T).

Soit $(p_\iota)_{\iota\in I}$ la famille des éléments minimaux distincts de G ; ce qui précède montre que tout $x \geqslant 0$ peut se mettre sous la forme $x=\sum_\iota n_\iota p_\iota$, où les n_ι sont des entiers $\geqslant 0$, nuls à l'exception d'un nombre fini d'entre eux ; tout $x\in G$ peut donc se mettre sous la même forme, où les entiers n_ι sont cette fois de signe quelconque. Reste à montrer que tout $x\in G$ ne peut se mettre sous cette forme que d'une seule manière, car G sera alors isomorphe à $\mathbf{Z}^{(I)}$. Pour cela, on peut se limiter au cas où les n_ι sont tous $\geqslant 0$, car en supposant la proposition démontrée dans ce cas, une relation de la forme $\sum_\iota (m'_\iota-m''_\iota)p_\iota = \sum_\iota (n'_\iota-n''_\iota)p_\iota$, où les $m'_\iota, m''_\iota, n'_\iota, n''_\iota$ sont $\geqslant 0$, s'écrit $\sum_\iota (m'_\iota+n''_\iota)p_\iota = \sum_\iota (n'_\iota+m''_\iota)p_\iota$, et donne donc $m'_\iota+n''_\iota=n'_\iota+m''_\iota$, d'où $n'_\iota-n''_\iota = m'_\iota-m''_\iota$ pour tout ι .

Si on tient compte de l'hypothèse que tout élément minimal de G est premier, on voit que le théorème sera conséquence de la proposition suivante :

PROPOSITION 21.- *Si $(x_i)_{1\leqslant i\leqslant m}$ est une famille d'éléments premiers $(y_j)_{1\leqslant j\leqslant n}$ une famille d'éléments minimaux, dans un groupe ordonné G, et si on a $\sum_{i=1}^{m} x_i \leqslant \sum_{j=1}^{n} y_j$, on a $m\leqslant n$, et il existe une*

une application biunivoque φ de $[1,m]$ dans $[1,n]$ telle que $x_i = y_{\varphi(i)}$ pour tout indice i .

Il suffit de raisonner par récurrence sur m et n , la proposition étant triviale pour m=0 . De $\sum_{i=1}^{m} x_i \leqslant \sum_{j=1}^{n} y_j$, on déduit $x_m \leqslant \sum_{j=1}^{n} y_j$; comme x_m est supposé premier, il existe un indice j tel que $0 \leqslant x_m \leqslant y_j$; mais comme y_j est minimal, on a nécessairement $x_m = y_j$; en retranchant x_m des deux membres de $\sum_{i=1}^{m} x_i \leqslant \sum_{j=1}^{n} y_j$, on est ramené à la proposition pour m-1 et n-1 .

Le théorème 1 est ainsi complètement démontré.

Remarques.- 1) L'axiome(T) est équivalent, pour un ensemble ordonné quelconque E , au suivant :

(T') Toute partie minorée et non vide de E admet un élément minimal.

Montrons d'abord que (T) entraîne (T'). Soit A une partie minorée de E . Si $x \in A$ n'est pas un élément minimal de A , il existe $x_1 \in A$ tel que $x_1 < x$; comme on ne peut définir par récurrence une suite strictement décroissante (x_n) d'éléments de A , en vertu de (T), il existe dans A un élément minimal $\leqslant x$. Réciproquement, (T') entraîne (T), en l'appliquant à l'ensemble des éléments d'une suite décroissante et minorée (x_j) d'éléments de E .

2) Dans un groupe décomposable, la réciproque de la prop.20 est vraie : les seuls éléments indécomposables sont les éléments de la forme nx , où x est minimal, puisque deux éléments minimaux distincts sont toujours étrangers.

12. Sommes d'éléments premiers dans un groupe réticulé.

D'après la prop.18 et le th.1, l'axiome (T) est une condition nécessaire et suffisante pour qu'un groupe réticulé G soit décomposable. Nous allons retrouver ce résultat par une autre voie, en étudiant de façon générale les sommes d'éléments premiers d'abord dans un monoïde semi-réticulé, puis dans un groupe réticulé.

PROPOSITION 22.- Si, dans un monoïde semi-réticulé E, l'axiome (T) est vérifié, pour tout élément $x > 0$ de E, il existe une suite finie $(x_i)_{1 \leqslant i \leqslant n}$ d'éléments premiers $\leqslant x$, tels que $x \leqslant \sum_{i=1}^{n} x_i$.

La proposition est évidente si $x > 0$ est premier. Supposons donc x non premier ; il existe donc deux éléments u,v tels que $u > 0$, $v > 0$, $x \not\leqslant u$, $x \not\leqslant v$ et $x \leqslant u+v$; de la prop.12, on tire $x \leqslant \inf(x,u) + \inf(x,v)$. Par hypothèse, $y = \inf(x,u) \neq x$ et $z = \inf(x,v) \neq x$; en outre $y \neq 0$, sinon x et u seraient étrangers, et de $x \leqslant u+v$ on déduirait $x \leqslant v$ (prop.15), contrairement à l'hypothèse ; on a donc $0 < y < x$, $0 < z < x$ et $x \leqslant y+z$. Supposons maintenant que, pour chaque k tel que $1 \leqslant k \leqslant n$, il existe une suite $(u_{ik})_{1 \leqslant i \leqslant m_k}$ d'éléments tels que : 1° $0 < u_{ik} < x$; 2° $x \leqslant \sum_{i=1}^{m_k} u_{ik}$; 3° chacun des éléments u_{ik} non premiers est le k-ème terme d'une suite strictement décroissante dont chaque terme d'indice h est un u_{ih} $(1 \leqslant h \leqslant k)$. Si, dans la suite $(u_{in})_{1 \leqslant i \leqslant m_n}$ il y a des termes non premiers u_{in}, pour chacun d'eux il existe, d'après ce qui précède, deux éléments u'_{in}, u''_{in} tels que $0 < u'_{in} < u_{in}$, $0 < u''_{in} < u_{in}$, et $u_{in} \leqslant u'_{in} + u''_{in}$; il est clair que les u'_{in}, u''_{in} et les u_{in} qui sont premiers forment une suite $(u_{i,n+1})$ satisfaisant aux mêmes conditions que les suites (u_{ik}) d'indice $k \leqslant n$. On en conclut que si on pouvait poursuivre ce procédé de récurrence pour tout n, c'est-à-dire s'il n'y avait aucun indice n tel que tous les u_{in} soient premiers, il existerait une suite infinie strictement décroissante d'éléments > 0 de E, contrairement à l'axiome (T), d'où la proposition.

Avant d'étudier les sommes d'éléments premiers dans un groupe réticulé, nous démontrerons pour un tel groupe l'importante propriété suivante :

THÉORÈME 2 (théorème de décomposition).- Dans un groupe réticulé G, soient $(x_i)_{1\leqslant i\leqslant p}$, $(y_j)_{1\leqslant j\leqslant q}$ deux suites finies d'éléments positifs de G, telles que $\sum_{i=1}^{p} x_i = \sum_{j=1}^{q} y_j$. Il existe alors une suite double $(z_{ij})_{1\leqslant i\leqslant p,1\leqslant j\leqslant q}$ d'éléments positifs de G telle que pour tout i, $x_i = \sum_{j=1}^{q} z_{ij}$, et pour tout j, $y_j = \sum_{i=1}^{p} z_{ij}$.

1° Si le théorème est vrai pour $p<m$ et $q=n$ $(m>2, n\geqslant 2)$, il est vrai pour $p=m$ et $q=n$. En effet, supposons que $\sum_{i=1}^{m-1} x_i + x_m = \sum_{j=1}^{n} y_j$; le théorème étant vrai pour $p=2$ et $q=n$, il existe deux suites finies (z'_j), (z''_j) de n termes positifs, telles que $\sum_{i=1}^{m-1} x_i = \sum_{j=1}^{n} z'_j$, $x_m = \sum_{j=1}^{n} z''_j$ et $y_j = z'_j + z''_j$ pour $1\leqslant j\leqslant n$. D'autre part, le théorème étant vrai pour $p=m-1$ et $q=n$, il existe une suite double $(u_{ij})_{1\leqslant i\leqslant m-1;1\leqslant j\leqslant n}$ telle que $x_i = \sum_{j=1}^{n} u_{ij}$ pour $1\leqslant i\leqslant m-1$, et $z'_j = \sum_{i=1}^{m-1} u_{ij}$ pour $1\leqslant j\leqslant n$; en posant $z_{ij}=u_{ij}$ pour $1\leqslant i\leqslant m-1$, et $z_{mj}=z''_j$ $(1\leqslant j\leqslant n)$, on obtient bien une suite double satisfaisant aux conditions du théorème.

2° Si le théorème est vrai pour $p=n$ et $q<n$ $(m\geqslant 2, n>2)$, il est vrai pour $p=m$ et $q=n$; même raisonnement.

3° Il reste uniquement à démontrer le théorème pour $p=q=2$. Supposons donc que les éléments positifs x_1, x_2, y_1, y_2 soient tels que $x_1+x_2=y_1+y_2$; posons $a_{11}=x_1+y_1$, $a_{12}=y_1$, $a_{21}=x_1$, $a_{22}=x_1+x_2=y_1+y_2$; on a $a_{12}\leqslant a_{11}$, $a_{12}\leqslant a_{22}$, $a_{21}\leqslant a_{11}$, $a_{21}\leqslant a_{22}$; si $c=\inf(a_{11},a_{22})$, on a donc $a_{12}\leqslant c$, $a_{21}\leqslant c$, et $c\leqslant a_{11}$, $c\leqslant a_{22}$. En prenant $z_{ij}=c-a_{ij}$ pour $i\neq j$, $z_{ij}=a_{ij}-c$ pour $i=j$ $(1\leqslant i\leqslant 2$, $1\leqslant j\leqslant 2)$, on voit aussitôt que l'on satisfait aux conditions du théorème.

Remarque.- Si les x_i sont deux à deux étrangers, les y_j deux à deux étrangers, les z_{ij} sont aussi deux à deux étrangers. En effet, si $h\neq i$, on a $z_{hk}\leqslant x_h$ et $z_{ij}\leqslant x_i$, donc z_{hk} et z_{ij} sont étrangers quels que soient k et j ; de même, si $j\neq k$,

$z_{hk} \leqslant y_k$ et $z_{ij} \leqslant y_j$, donc z_{hk} et z_{ij} sont étrangers quels que soient h et i .

COROLLAIRE.- Soient $y, x_1, x_2, \ldots, x_n$ $n+1$ éléments $\geqslant 0$ de G , tels que $y \leqslant \sum_{i=1}^{n} x_i$; il existe n éléments $y_i \geqslant 0$ $(1 \leqslant i \leqslant n)$ tels que $y_i \leqslant x_i$ et $y = \sum_{i=1}^{n} y_i$.

Il suffit d'appliquer le th. de décomposition à la suite (x_i) et à la suite formée des deux éléments y et $z = \sum_{i=1}^{n} x_i - y$.

Soit alors $(p_\iota)_{\iota \in I}$ la famille des éléments minimaux (ou des éléments premiers, ce qui revient au même) dans un groupe réticulé G , et soit G' le sous-groupe de G engendré par les p_ι , c'est-à-dire l'ensemble des $x = \sum_\iota n_\iota p_\iota$ (n_ι entiers rationnels) ; la prop.21 montre que G' est un groupe décomposable pour la structure d'ordre induite par celle de G , car la relation $\sum_\iota n_\iota p_\iota \geqslant 0$ entraîne $n_\iota \geqslant 0$ pour tout ι (sans quoi il existerait deux suites finies $(x_i), (y_j)$ d'éléments minimaux, tels qu'aucun des x_i ne soit égal à un y_j , et que $\sum_i x_i \leqslant \sum_j y_j$, contrairement à la prop.21). En outre :

PROPOSITION 23.- Soit G' le sous-groupe d'un groupe réticulé G engendré par les éléments premiers de G ; pour tout élément $x \geqslant 0$ de G' , tout $y \in G$ tel que $0 \leqslant y \leqslant x$ appartient à G' .

En effet, on a $x = \sum_{i=1}^{n} x_i$, où (x_i) est une suite finie d'éléments premiers de G ; d'après le cor. du th. 2, il existe une suite (y_i) de n éléments de G telle que $y = \sum_{i=1}^{n} y_i$ et $0 \leqslant y_i \leqslant x_i$; comme les x_i sont minimaux, on a nécessairement $y_i = 0$ ou $y_i = x_i$ pour tout i , d'où la proposition.

Si maintenant on suppose que le groupe réticulé G satisfait à (F) les prop.22 et 23 montrent que $G = G'$, donc que G est décomposable.

2. Corps ordonnés.

1. Anneaux ordonnés.

DÉFINITION 1.- Etant donné un anneau commutatif A, on dit qu'une structure d'ordre sur A (définie par une relation d'ordre notée $x \leqslant y$) et la structure d'anneau de A sont compatibles si cette structure d'ordre est compatible avec la structure de groupe additif de A, et satisfait en outre à l'axiome suivant

(AO) Les relations $x \geqslant y$ et $z \geqslant 0$ entraînent $xz \geqslant yz$.

Un ensemble A muni d'une structure d'anneau commutatif et d'une structure d'ordre compatibles, est appelé anneau ordonné.

Exemples.- L'anneau $\mathbb{Z}$ des entiers rationnels et le corps $\mathbb{Q}$ des nombres rationnels sont des anneaux ordonnés. Il en est de même de l'anneau $\mathbb{Z}^E$ (ou $\mathbb{Q}^E$) des applications d'un ensemble E dans $\mathbb{Z}$ (ou $\mathbb{Q}$) lorsqu'on définit dans cet anneau la relation d'ordre "$f \leqslant g$" comme équivalente à "quel que soit $x \in E$, $f(x) \leqslant g(x)$".

D'après (AO), les relations $x \geqslant y$ et $z \leqslant 0$ entraînent $xz \leqslant yz$; on peut donc dire qu'une homothétie de rapport > 0 conserve l'ordre, et une homothétie de rapport < 0 le change en l'ordre opposé.

Il est évident que tout sous-anneau d'un anneau ordonné est un anneau ordonné pour l'ordre induit.

L'ensemble $P = A_+$ des éléments $\geqslant 0$ d'un anneau ordonné A satisfait aux trois conditions :

(AP_I) $\quad P + P \subset P$.

(AP_{II}) $\quad P \cdot P \subset P$.

(AP_{III}) $\quad P \cap (-P) = \{0\}$.

En effet (AP_I) et (AP_{III}) ont été démontrées au § 1, n° 2, et (AP_{II}) résulte de l'axiome (AO) appliqué au cas $y = 0$. Inversement si P est une partie d'un anneau A satisfaisant à ces trois conditions,

il existe sur A une structure d'ordre et une seule, compatible avec la structure d'anneau de A , et telle que P soit l'ensemble des éléments positifs pour cette structure d'ordre.

En effet, P définit sur A une structure d'ordre compatible avec la structure de groupe additif de A , et pour laquelle P est l'ensemble des éléments $\geqslant 0$ (§1,n°2,prop.3) ; en outre, d'après (AP_{II}), les relations $x \geqslant 0$, $z \geqslant 0$ entraînent $xz \geqslant 0$; par suite, comme $x \geqslant y$ est équivalente à $x-y \geqslant 0$, les relations $x \geqslant y$, $z \geqslant 0$ entraînent $z(x-y) \geqslant 0$, c'est-à-dire $zx \geqslant zy$.

On déduit aussitôt de (AP_{II}) que $P.(-P)=-(P.P) \subset -P$ et $(-P)(-P) = P.P \subset P$ (règle des signes).

Considérons maintenant le cas particulier où la structure d'ordre de A est une structure d'ensemble totalement ordonné ; A est alors appelé anneau totalement ordonné ; l'ensemble $P=A_+$ vérifie alors la condition supplémentaire

(AP_{IV}) $P \cup (-P) = A$;

et réciproquement, si P vérifie (AP_I),(AP_{II}),(AP_{III}) et (AP_{IV}), la structure d'ordre définie par P sur l'anneau A est une structure d'ensemble totalement ordonné (1,n°2).

Dans un anneau totalement ordonné A , on a $|x| = x$ si $x \geqslant 0$, $|x| = -x$ si $x \leqslant 0$; on déduit donc de la règle des signes que

(1) $$|xy| = |x| \cdot |y| .$$

D'autre part, la règle des signes montre aussi que pour tout $x \in A$, on a alors $x^2 \geqslant 0$; par suite :

PROPOSITION 1.- Dans un anneau totalement ordonné A , on a $\sum_{i=1}^{n} x_i^2 \geqslant 0$ pour toute suite finie (x_i) d'éléments de A , et la relation $\sum_{i=1}^{n} x_i^2 = 0$ entraîne $x_i^2 = 0$ pour tout i .

Si A admet un élément unité 1 , on a $1=1^2 \geqslant 0$, et comme $1 \neq 0$, $1 > 0$; pour tout $n > 0$, on a donc $n.1 > 0$ (§ 1,cor.de la prop.2). D'autre part, comme dans tout groupe totalement ordonné, la relation $nx > 0$ entraîne $x > 0$ (§ 1,cor.1 et 2 de la prop.9) ; en d'autres termes :

PROPOSITION 2.- Un anneau totalement ordonné est de caractéristique 0.

2. Corps ordonnés.

Lorsqu'un corps commutatif K est muni d'une structure d'ordre pour laquelle K est un anneau totalement ordonné (n°1), nous dirons, par abus de langage, que K est un corps ordonné (cf. exerc. 3 et 6). Par abus de langage, nous dirons aussi qu'une structure d'ordre et une structure de corps sur K sont compatibles si K est un corps ordonné pour cette structure d'ordre (une structure d'ordre sur K peut donc être compatible avec la structure d'anneau de K , sans qu'elle le soit avec la structure de corps de K ; pour qu'elle ait cette dernière propriété, il faut en outre que K soit totalement ordonné pour cette structure).

Le corps $\mathbb{Q}$ des nombres rationnels est un corps ordonné ; en outre (prop.2) un corps ordonné est de caractéristique 0 , donc contient un corps isomorphe à $\mathbb{Q}$, qu'on identifie à $\mathbb{Q}$.

Dans un corps ordonné les relations $x > 0$, $y > 0$ entraînent $xy > 0$ puisque $xy \neq 0$; la relation $x > 0$ entraîne $x^{-1} > 0$, car $x.x^{-1}=1 > 0$, ce qui prouve qu'on ne peut avoir $x^{-1} < 0$; on en déduit que si $0 < x < y$, on a $y^{-1} < x^{-1}$, car on a $x^{-1} > 0$, $y^{-1} > 0$, donc $x^{-1}y^{-1} > 0$, et par suite $x(x^{-1}y^{-1}) < y(x^{-1}y^{-1})$; si on désigne par K_+^* l'ensemble des éléments > 0 de K , on voit que l'application $x \to x^{-1}$ est une permutation involutive de K_+^* , strictement décroissante.

Par suite, K_+^* est un sous-groupe du groupe multiplicatif K^* des éléments $\neq 0$ de K ; en outre la structure d'ordre induite sur K_+^* par celle de K est compatible avec la structure de groupe multiplicatif de K_+^*, d'après (AO) ; autrement dit, le groupe K_+^*, muni de cette structure d'ordre, est un groupe multiplicatif totalement ordonné.

PROPOSITION 3.- Soit A un anneau d'intégrité totalement ordonné, K son corps des quotients ; il existe sur K une structure d'ordre et une seule, induisant sur A la structure d'ordre de A, et pour laquelle K est un corps (totalement) ordonné.

En effet, tout élément de K est de la forme $\frac{x}{y}$, où $x \in A$, $y \in A$ et $y \neq 0$; s'il existe une structure d'ordre sur K ayant les propriétés de l'énoncé, la relation $\frac{x}{y} \geqslant 0$ est équivalente à $y^2 \cdot \frac{x}{y} \geqslant 0$, c'est-à-dire $xy \geqslant 0$, donc x et y doivent être de même signe, et comme $\frac{x}{y} = \frac{-x}{-y}$, on peut toujours supposer que $x \geqslant 0$ et $y > 0$. Inversement soit P l'ensemble des éléments $\frac{x}{y}$ tels que $x \in A$, $y \in A$, $x \geqslant 0$, $y > 0$; on vérifie aussitôt que P satisfait aux axiomes (AP_I) et (AP_{II}) ; si $\frac{x}{y} = -\frac{x'}{y'}$, on a $xy' + yx' = 0$ et comme $xy' \geqslant 0$, $yx' \geqslant 0$, on en tire $xy' = yx' = 0$; les hypothèses $y > 0$, $y' > 0$ entraînent donc $x = x' = 0$, ce qui prouve que P satisfait à (AP_{III}) ; enfin, si $\frac{a}{b}$ est un élément quelconque de K ($a \in A$, $b \in A$), on peut toujours supposer que $b > 0$; alors si $a \geqslant 0$, on a $\frac{a}{b} \in P$, et si $a \leqslant 0$, $\frac{a}{b} \in -P$, d'où (AP_{IV}).

En particulier, on retrouve ainsi la structure d'ordre du corps $\mathbb{Q}$ des rationnels à partir de la structure d'ordre de l'anneau $\mathbb{Z}$ (chap. I, § 9, n° 5). On remarquera d'ailleurs qu'il n'existe sur $\mathbb{Q}$ qu'une seule structure d'ordre pour laquelle $\mathbb{Q}$ est un corps ordonné, car pour une telle structure on doit avoir $n = n.1 > 0$ pour tout entier naturel $n \neq 0$, donc la

la structure induite sur $\mathbb{Z}$ est nécessairement la structure d'ordre définie au chap.I, § 2, n°5) .

3. Corps ordonnables.

DÉFINITION 2.- *On dit qu'un corps commutatif* K *est ordonnable s'il existe une structure d'ordre sur* K *compatible avec la structure de corps de* K .

Nous allons voir qu'on peut donner une caractérisation algébrique simple des corps ordonnables :

THÉORÈME 1 (Artin-Schreier).- *Pour qu'un corps commutatif* K *soit ordonnable, il faut et il suffit qu'il vérifie l'axiome suivant :*

(KO) *La relation* $x_1^2+x_2^2+\ldots+x_n^2=0$ *entraîne* $x_1=x_2=\ldots=x_n=0$.

Il est immédiat que l'axiome (KO) est équivalent à

(KO') *Dans* K , -1 *n'est pas égal à une somme de carrés.*

Un corps ne peut évidemment satisfaire à (KO) que s'il est de caractéristique 0 ; mais il y a des corps de caractéristique 0 qui ne satisfont pas à (KO), par exemple tous ceux dans lesquels -1 est un carré, donc tout corps obtenu en adjoignant à un corps quelconque K_0 une racine de X^2+1 .

D'après la prop.1, la condition est *nécessaire*. Pour voir qu'elle est *suffisante*, nous allons montrer qu'il existe dans K une partie P satisfaisant aux axiomes (AP_I), (AP_{II}), (AP_{III}) et (AP_{IV}). Une telle partie doit contenir l'ensemble K^2 des carrés des éléments de K (n°1). Considérons l'ensemble $\mathfrak{M}$ des parties P de K qui contiennent K^2 et satisfont aux conditions (AP_I), (AP_{II}) et (AP_{III}). Montrons en premier lieu que $\mathfrak{M}$ *n'est pas vide*. Pour cela, soit P_0 l'ensemble des *sommes de carrés* $\sum_i x_i^2$ dans K ; il est immédiat que P_0 contient K^2 et satisfait à (AP_I) et (AP_{II}). Il satisfait à (AP_{III}) car la relation $\sum_i x_i^2 = -\sum_j y_j^2$ s'écrit $\sum_i x_i^2 + \sum_j y_j^2 = 0$, et donne en vertu de

(K0) $x_i=0$ pour tout i et $y_j=0$ pour tout j , d'où $\sum_i x_i^2=0$. P_0 appartient donc à $\mathfrak{M}$, et est évidemment contenu dans tout $P\in\mathfrak{M}$.

Cela étant, $\mathfrak{M}$, ordonné par inclusion, est un ensemble <u>inductif</u> (Ens.R, § 6, n°9) : en effet, si $\mathfrak{G}$ est une partie totalement ordonnée de $\mathfrak{M}$, la réunion Q des ensembles $P\in\mathfrak{G}$ appartient à $\mathfrak{M}$, car si x et y sont deux éléments de Q , il existe P et P' dans $\mathfrak{G}$ tels que $x\in P$, $y\in P'$; si par exemple $P\subset P'$ on a aussi $x\in P'$, donc $x+y\in P'\subset Q$ et $xy\in P'\subset Q$, et la relation $x+y=0$ entraîne $x=y=0$.

Il existe donc, d'après le th. de Zorn (Ens.R, § 6, n°10) un élément <u>maximal</u> Q de $\mathfrak{M}$; nous allons montrer que l'on a $Q\cup(-Q)=K$, ce qui établira le théorème. Cette dernière relation est une conséquence immédiate du fait que Q est maximal, et du lemme suivant :

<u>Lemme.-</u> <u>Soit</u> $P\in\mathfrak{M}$, <u>et x un élément de K tel que</u> $x\notin P$. <u>Il existe alors un ensemble</u> $P'\in\mathfrak{M}$ <u>tel que</u> $P\subset P'$ <u>et</u> $-x\in P'$.

Désignons en effet par P' l'ensemble des éléments de la forme $a_0-a_1x+a_2x^2-\ldots+(-1)^p a_p x^p$, où les a_i appartiennent tous à P (p étant un entier $\geqslant 0$ arbitraire) ; on a évidemment $P\subset P'$, $-x\in P$, et P satisfait à (AP_I) et (AP_{II}) ; montrons que P' satisfait aussi à (AP_{III}) ; en effet, si $u\in P'\cap(-P')$, il existe deux suites finies (a_i), (b_i) de p éléments $(1\leqslant i\leqslant p)$ appartenant à P , telles que $u=a_0-a_1x+\ldots+(-1)^p x^p=-(b_0-b_1x+\ldots+(-1)^p x^p)$, autrement dit $c_0-c_1x+c_2x^2-\ldots+(-1)^p c_p x^p=0$, avec $c_i=a_i+b_i\in P$ pour $1\leqslant i\leqslant p$. Or, cette relation s'écrit $c_0+c_2x^2+\ldots=x(c_1+c_3x^2+\ldots)$, ou encore $y=xz$, en posant $y=c_0+c_2x^2+\ldots$, $z=c_1+c_3x^2+\ldots$; comme P contient K^2 , y et z appartiennent à P d'après (AP_I) et (AP_{II}) ; si $y=0$, on a $z=0$ puisque $x\neq 0$; on en conclut que tous les c_i sont nuls, d'où $a_i=b_i=0$ pour $1\leqslant i\leqslant p$, et $u=0$; si $x\,y\neq 0$, on a $z\neq 0$ et on en déduit

$x=yz^{-1}=yz(z^{-1})^2$, et comme $K^2 \subset P$, on aurait $x \in P$, contrairement à l'hypothèse. La relation $u \in P' \cap (-P')$ entraîne donc $u=0$, ce qui achève la démonstration du lemme, et par suite aussi du th.1 .

On remarquera en outre que si on applique le lemme en y remplaçant P par P_0 , on voit que pour tout $x \notin P_0$, il existe $P \in \mathfrak{M}$ tel que $-x \in P$; d'après le th. de Zorn, il existe un élément <u>maximal</u> Q de $\mathfrak{M}$, contenant P , donc tel que $-x \in Q$, ce qui entraîne $x \notin Q$. On voit donc que P_0 est l'<u>intersection des éléments maximaux de</u> $\mathfrak{M}$; en d'autres termes :

PROPOSITION 4.- <u>Pour qu'un élément x d'un corps ordonnable K soit positif pour toutes les structures d'ordre sur</u> K (compatible avec la structure de corps de K), <u>il faut et il suffit que x soit somme de carrés d'éléments de</u> K .

<u>4. Extensions des corps ordonnables.</u>

PROPOSITION 5.- <u>Une extension transcendante pure d'un corps ordonnable est ordonnable</u>.

Il suffit évidemment de démontrer que si K est ordonnable, il en est de même d'un corps de fractions rationnelles $K(X_1,X_2,\dots,X_n)$ à un nombre fini quelconque d'indéterminées ; or, supposons qu'il y ait une suite finie $(f_i)_{1 \leqslant i \leqslant m}$ de fractions rationnelles de ce corps telles que $-1 = \sum_{i=1}^{m} f_i^2$; comme K est de caractéristique 0 , il est infini, par suite (chap.IV, §), il existe n éléments x_k $(1 \leqslant k \leqslant n)$ de K tels que $f_i(x_1,x_2,\dots,x_n)$ soit défini pour $1 \leqslant i \leqslant m$; on aurait donc $-1 = \sum_{i=1}^{m} (f_i(x_1,x_2,\dots,x_n))^2$ contrairement à l'hypothèse que K est ordonnable.

PROPOSITION 6.- <u>Une extension algébrique de degré impair d'un corps ordonnable est ordonnable</u>.

Soit $E=K(a_1,a_2,..,a_p)$ une extension de degré impair d'un corps ordonnable K ; le degré $[E:K]$ étant le produit des degrés $[K(a_1):K]$ et $[K(a_1,..,a_{i+1}):K(a_1,..,a_i)]$ pour $1 \leqslant i \leqslant p-1$, tous ces degrés sont impairs, et il suffit donc de faire la démonstration pour une extension <u>simple</u> $E=K(\theta)$ de degré n sur K . Nous raisonnerons par récurrence sur n , la proposition étant triviale pour n=1 . Soit $f \in K[X]$ le polynome minimal de θ ; tout élément de K s'écrivant d'une seule manière sous la forme $\varphi(\theta)$, où $\varphi \in K[X]$ est de degré $\leqslant n-1$, si K n'était pas ordonnable, on aurait une relation de la forme $-1 = \sum_{k=1}^{m} (\varphi_k(\theta))^2$; cette relation est équivalente à $-1 \equiv \sum_{k=1}^{m} (\varphi_k(X))^2 \pmod{f(X)}$, ou encore à

$$(2) \qquad -1 = \sum_{k=1}^{m} (\varphi_k(X))^2 + f(X)g(X)$$

où $g \in K[X]$. Soit $\mu \leqslant n-1$ le plus grand des degrés des φ_k ; le coefficient de $X^{2\mu}$ dans $\sum_{k=1}^{m} (\varphi_k(X))^2$ est somme de carrés d'éléments $\neq 0$ de K , donc n'est pas nul d'après (K0) ; donc $\sum_{k=1}^{m} \varphi_k^2$ est de degré 2μ ; l'identité (2) prouve alors que g est de degré $2\mu-n$, donc de degré <u>impair</u> et $\leqslant n-2$; parmi les facteurs irréductibles g_h de g , il y en a donc un au moins de degré impair et $< n$ (puisque le degré de g est la somme des degrés des g_h). Soit a une racine d'un tel facteur ; d'après l'hypothèse de récurrence, K(a) est ordonnable ; mais on déduit de (2) la relation $-1 = \sum_{k=1}^{m} (\varphi_k(a))^2$, et les $\varphi_k(a)$ appartiennent à K(a) , ce qui est absurde.

PROPOSITION 7.- <u>Soit</u> K <u>un corps ordonnable,</u> (a_ι) <u>une famille d'éléments de</u> K ; <u>pour tout</u> ι , <u>soit</u> $\sqrt{a_\iota}$ <u>une racine du polynome</u> X^2-a_ι ("racine carrée" de a_ι). <u>Pour que le corps</u> E <u>obtenu par adjonction à</u> K <u>des éléments</u> $\sqrt{a_\iota}$ <u>soit ordonnable, il faut et il suffit qu'il existe sur</u> K <u>une structure d'ordre</u> (compatible avec la structure de corps de K) <u>telle que tous les</u> a_ι <u>soient positifs pour cette structure.</u>

La condition est évidemment nécessaire, car $a_\nu = (\sqrt{a_\nu})^2$ est positif pour toute structure d'ordre sur E (faisant de E un corps ordonné), donc aussi pour la structure d'ordre qu'elle induit sur K .

Pour montrer que la condition est suffisante, nous allons voir qu'elle entraîne l'impossibilité d'une relation de la forme

$$(3) \qquad -1 = \sum_{i=1}^{n} c_i x_i^2$$

où les $c_i \in K$ sont des éléments positifs (pour la structure d'ordre pour laquelle tous les a_ν sont $\geqslant 0$), et les x_i des éléments de E ; comme les x_i appartiennent à un corps obtenu en adjoignant à K un nombre fini des éléments $\sqrt{a_\nu}$, on peut d'emblée se restreindre au cas où E s'obtient en adjoignant à K une famille finie $(\sqrt{a_k})_{1 \leq k \leq r}$ de racines carrées d'éléments $a_k \geqslant 0$ de K . Pour démontrer dans ce cas l'impossibilité de la relation (3), nous procéderons par récurrence sur r , la proposition étant triviale pour r=0. Soit F le corps obtenu par adjonction à K de $\sqrt{a_1}$, $\sqrt{a_2}$, ..., $\sqrt{a_{r-1}}$; on a $E = F(\sqrt{a_r})$; si $\sqrt{a_r} \in F$, la relation (3) est impossible par l'hypothèse de récurrence ; sinon, on peut écrire $x_i = y_i + z_i \sqrt{a_r}$, où les y_i et les z_i appartiennent à F ; (3) s'écrit donc

$$(4) \qquad -1 = \sum_{i=1}^{n} c_i y_i^2 + \sum_{i=1}^{n} c_i a_i z_i^2 + 2\sqrt{a_r} \sum_{i=1}^{n} c_i y_i z_i$$

ce qui entraîne d'abord $\sum_{i=1}^{n} c_i y_i z_i = 0$, sans quoi on tirerait de cette relation que $\sqrt{a_r} \in F$, contrairement à l'hypothèse ; mais alors, comme $a_r \geqslant 0$, la relation (4) est de la même forme que (3), mais les éléments y_i et z_i appartiennent à F , ce qui est encore contraire à l'hypothèse ; la proposition est ainsi démontrée.

5. Corps ordonnables maximaux.

DÉFINITION 3.- On dit qu'un corps ordonnable K est maximal s'il n'existe aucune extension algébrique ordonnable de K .

Nous allons donner aussi une caractérisation algébrique des corps ordonnables maximaux :

THÉORÈME 2 (Artin-Schreier).- Pour qu'un corps commutatif K soit ordonnable maximal, il faut et il suffit qu'il vérifie l'axiome (KO) et les deux axiomes suivants :

(KM_I) Tout polynome de $K[X]$ de degré impair a une racine dans K .

(KM_{II}) Pour tout $x \in K$, x ou -x est le carré d'un élément de K .

En outre, si K est un corps ordonnable maximal, le corps $K(i)$, obtenu par adjonction à K d'une racine i de X^2+1 , est algébriquement fermé.

Montrons en premier lieu que les conditions sont nécessaires ; si K est un corps ordonnable maximal, muni d'une structure d'ordre compatible avec sa structure de corps, tout élément $x \geqslant 0$ de K est nécessairement le carré d'un élément de K ; sans quoi, le corps $K(\sqrt{x})$ extension algèbrique de K , distincte de K serait ordonnable (prop.7) contrairement à l'hypothèse ; il en résulte que K vérifie (KM_{II}) . De même, s'il existait un polynome de degré impair $f \in K[X]$ n'ayant aucune racine dans K , f a au moins un facteur irréductible g de degré impair > 1 ; en adjoignant à K une racine a de g , $K(a)$ serait une extension algèbrique de K , distincte de K et ordonnable (prop.6) contrairement à l'hypothèse ; donc K vérifie (KM_I) .

Nous démontrerons que les conditions sont suffisantes en prouvant que $K(i)$ est algèbriquement fermé ; en effet, il en résultera que K n'admet aucune extension algèbrique distincte de K et de $K(i)$, et $K(i)$ n'est pas ordonnable puisque $i^2 = -1$ dans ce corps.

Pour montrer que $K(i)$ est algèbriquement fermé, il suffit d'établir que tout polynome de $K(i)[X]$ admet une racine dans $K(i)$. Montrons d'abord que l'on peut se borner à prouver que tout polynome de $K[X]$ admet une racine dans $K(i)$. En effet, $K(i)$ est une extension

galoisienne de degré 2 de K ; soit $x \to \bar{x}$ l'unique automorphisme de K(i) relativement à K , distinct de l'automorphisme identique ; soit $f \to \bar{f}$ l'extension de cet automorphisme à $K(i)[X]$ (autrement dit, si $f = \sum_{k=0}^{n} a_k X^k$, $\bar{f} = \sum_{k=0}^{n} \bar{a}_k X^k$). Soit f un polynome quelconque de $K(i)[X]$; $g=f\bar{f}$ est un polynome de $K[X]$, car ses coefficients sont invariants par l'automorphieme $x \to \bar{x}$; si $x_0 \in K(i)$ est une racine de g , on a $f(x_0)=0$ ou $\bar{f}(x_0)=0$; et dans le second cas, on a aussi $\overline{\bar{f}(x_0)}=0$, c'est-à-dire $f(\bar{x}_0)=0$, donc dans tous les cas, f a une racine dans K(i) .

Soit donc f un polynome quelconque de $K[X]$, $n=2^m q$ son degré, q étant impair ; si m=0, la proposition à démontrer est une conséquence de (KM_I), donc est vraie par hypothèse. Nous allons raisonner par <u>récurrence sur m</u> . Si $f=f_1 f_2 \ldots f_p$, où les f_k $(1 \leqslant k \leqslant p)$ sont irréductibles, un au moins des degrés des f_k n'est pas divisible par 2^{m+1}, sans quoi n le serait, contrairement à l'hypothèse ; s'il existe un des f_k dont le degré est de la forme $2^r q'$, où $r < m$ et q' est impair, la proposition résulte de l'hypothèse de récurrence ; nous pouvons donc nous restreindre au cas où f est <u>irréductible</u> dans $K[X]$.

Nous utiliserons le lemme suivant :

<u>Lemme</u>.- <u>Soient</u> a_i $(1 \leqslant i \leqslant n)$ <u>les racines d'un polynome irréductible</u> $f \in K[X]$ <u>de degré n</u> (dans une extension algèbriquement fermée de K). <u>Si</u> $\lambda \in K$ <u>est tel que les</u> $n(n-1)/2$ <u>éléments</u> $\beta_{ij}=a_i a_j+\lambda(a_i+a_j)$ $(1 \leqslant i < j \leqslant n)$ <u>soient tous distincts, chacun des corps</u> $K(\beta_{ij})$ <u>est identique à</u> $K(a_i a_j, a_i+a_j)$.

En effet, soit $\Omega = K(a_1, a_2, \ldots, a_n)$; Ω est une extension galoisienne de K ; cherchons les automorphismes σ de Ω par rapport à K qui laissent invariants β_{ij} ; si $\sigma(a_i)=a_n$, $\sigma(a_j)=a_k$, on a

$\sigma(\beta_{ij})=\beta_{hk}$, ce qui n'est possible que si $h=i$, $k=j$ ou $h=j$, $k=i$, d'après l'hypothèse ; il en résulte que l'on a $\sigma(a_i+a_j)=a_i+a_j$ et $\sigma(a_ia_j)=a_ia_j$ dans les deux cas ; autrement dit, tout automorphisme de Ω par rapport à $K(\beta_{ij})$ est un automorphisme de Ω par rapport à $K(a_ia_j,a_i+a_j)$; la réciproque étant évidente, le lemme est démontré.

Revenons à la démonstration du théorème ; soient a_i $(1\leqslant i\leqslant n)$ les n racines (distinctes) du polynome irréductible f (dans une extension algèbriquement fermée de K) ; avec les notations du lemme, on peut déterminer $\lambda\in K$ tel que les $n(n-1)/2$ éléments β_{ij} soient distincts ; en effet, le polynome $(a_i+a_j-a_h-a_k)X+(a_ia_j-a_ha_k)$ ne peut être identiquement nul que si $a_i+a_j=a_h+a_k$, $a_ia_j=a_ha_k$, ce qui entraîne que a_h et a_k sont racines de $(X-a_i)(X-a_j)$, et l'hypothèse $h<k$ entraîne $a_h=a_i$, $a_j=a_k$; pour que les β_{ij} soient tous distincts, il suffit donc que λ soit distinct des racines d'un nombre fini de polynomes du premier degré non identiquement nuls, et comme K est un corps infini, il existe toujours des $\lambda\in K$ satisfaisant à cette condition. L'élément λ étant ainsi choisi, le polynome $g=\prod_{i<j}(X-\beta_{ij})$ a ses coefficients dans K , car tout automorphisme de Ω par rapport à K permute les β_{ij}, donc laisse invariant g ; or g est de degré $2^{m-1}(2^m q-1)=2^{m-1}q'$, où q' est impair ; l'hypothèse de récurrence prouve qu'il existe une racine de g dans $K(i)$; on peut supposer par exemple que c'est β_{12} ; alors $K(\beta_{12})$ est contenu dans $K(i)$; d'après le lemme, a_1a_2 et a_1+a_2 sont aussi contenus dans $K(i)$. Pour voir que a_1 $K(i)$, on est donc ramené à prouver que tout polynome du second degré X^2+pX+q , à coefficients dans $K(i)$, admet une racine dans $K(i)$; comme $X^2+pX+q=(X+\frac{p}{2})^2+(q-\frac{p^2}{4})$, il suffit de montrer que tout élément $a=b+ci$ de $K(i)$ $(b\in K,\ c\in K)$ est le <u>carré</u> d'un élément $u+vi$ de $K(i)$ $(u\in K,\ v\in K)$. Or, l'équation $(u+vi)^2=b+ci$ équivaut à $u^2-v^2=b$, $2uv=c$, d'où on tire $(u^2+v^2)^2=b^2+c^2$;

d'après (KM_{II}), b^2+c^2 est un carré ou l'opposé d'un carré, et la seconde hypothèse doit être exclue d'après (K0) (sauf dans le cas trivial b=c=0) . Il existe donc d K tel que $d^2=b^2+c^2$; montrons qu'on peut résoudre le système d'équations $u^2+v^2=\varepsilon d$, $u^2-v^2=b$, en prenant soit $\varepsilon=1$, soit $\varepsilon=-1$. En effet, ce système équivaut à $u^2=\frac{1}{2}(\varepsilon d+b)$, $v^2=\frac{1}{2}(\varepsilon d-b)$; or, on a $\frac{1}{2}(d+b).\frac{1}{2}(d-b)=\frac{1}{4}(d^2-b^2)=(\frac{c}{2})^2$, donc, ou bien d+b et d-b sont tous deux des carrés dans K , ou bien tous deux des opposés de carrés, d'après (KM_{II}) ; on prendra $\varepsilon=1$ dans le premier cas, $\varepsilon=-1$ dans le second, et dans tous les cas on voit qu'il existe u_o et v_o dans K tels que $u_o^2=\frac{1}{2}(\varepsilon d+b)$, $v_o^2=\frac{1}{2}(\varepsilon d-b)$; on a $4u_o^2v_o^2=c^2$, d'où $2u_ov_o=\pm c$; on prendra $u=u_o$ et $v=\pm v_o$. C.Q.F.D.

COROLLAIRE 1.- <u>Sur un corps ordonnable maximal</u> K , <u>il existe une seule structure d'ordre compatible avec la structure de corps de</u> K .

En effet, l'ensemble P des éléments $\geqslant 0$ pour une telle structure d'ordre doit contenir l'ensemble K^2 des carrés des éléments de K ; comme K est réunion de K^2 et de $-K^2$, et qu'on doit avoir $P\cap(-P)=\{0\}$, on a nécessairement $P=K^2$.

Quand on considère un corps ordonnable maximal K , on peut donc toujours parler de sa structure d'ordre sans qu'il y ait ambiguité.

COROLLAIRE 2.- <u>Si</u> K <u>est un corps ordonnable maximal, les polynomes de</u> $K[X]$ <u>qui sont irréductibles sont les polynomes du premier degré et les polynomes du second degré</u> X^2+pX+q <u>tels que</u> $q-\frac{p^2}{4}>0$.

En effet, toute extension algébrique de K est au plus du second degré ; d'autre part, si $q-\frac{p^2}{4}\leqslant 0$, il existe $a\in K$ tel que $\frac{p^2}{4}-q=a^2$, d'où $X^2+pX+q=(X+\frac{p}{2}-a)(X+\frac{p}{2}+a)$.

PROPOSITION 8.- Soit K un corps ordonnable maximal f un polynome de $K[X]$. Si a et b sont deux éléments de K tels que $a<b$, $f(a)<0$ et $f(b)>0$, il existe $c\in K$ tel que $a<c<b$ et $f(c)=0$.

La proposition est évidente si f est du premier degré. Dans le cas général, f est produit de polynomes du premier degré et de polynomes de la forme $(x+\alpha)^2+\beta^2$ (cor.2 du th.2) avec $\beta\neq 0$, et un polynome du second degré de cette forme est >0 quel que soit x ; il y a donc au moins un facteur du premier degré g de f tel que $g(a)g(b)<0$, d'où la proposition.

6. Extensions ordonnables maximales d'un corps ordonnable.

THEOREME 3.- Soit K un corps ordonnable, S une extension de K (algébrique ou transcendante) algèbriquement fermée. Pour toute structure d'ordre sur K compatible avec la structure de corps de K , il existe une extension ordonnable maximale R de K , contenue dans S , telle que S=R(i), et que la structure d'ordre de R induise sur K la structure d'ordre donnée.

Soit $\mathfrak{M}$ l'ensemble des extensions ordonnables de K contenues dans S ; il est immédiat (chap.V, § 2, prop.3) que $\mathfrak{M}$, ordonné par inclusion, est un ensemble inductif ; il a donc un élément maximal R_0 , en vertu du th. de Zorn (Ens.R, § 6, n°10). Il ne peut exister d'extension transcendante pure de R_0 contenue dans S , sans quoi, d'après la prop.5, R_0 ne serait pas un élément maximal de $\mathfrak{M}$; donc S est une extension algèbrique de R_0 . D'autre part, R_0 satisfait, pour la même raison, aux conditions (KM_I) et (KM_{II}), en vertu des prop.6 et 7 (la prop.7 montre en effet que, si on munit R_0 d'une structure d'ordre compatible avec sa structure de corps, tout élément $x\geqslant 0$ de R_0 est nécessairement un carré dans R_0). Le th.2 montre donc que R_0 est

un corps ordonnable maximal, et que $R_0(i)$ est une extension algèbriquement fermée de R_0 ; comme elle est contenue dans S , et que S est une extension algèbrique de $R_0(i)$, on a $S=R_0(i)$.

Considérons maintenant le corps K' obtenu par adjonction à K des racines carrées de tous les éléments $\geqslant 0$ de K pour l'ordre donné sur K . D'après la prop.7, K' est un corps ordonnable contenu dans S ; en lui appliquant ce qui précède, on voit qu'il existe une extension ordonnable maximale R de K' , contenue dans S et telle que $S=R(i)$; or, pour l'ordre de R , les éléments de K positifs pour l'ordre donné sur K , sont encore positifs, puisqu'ils sont carrés d'éléments de R . Le théorème est donc complètement démontré.

Il existera en général une infinité d'extensions R possédant les propriétés énoncées dans le th.3 .

7. Notations.

Si K est un corps ordonnable maximal, tout élément $a \geqslant 0$ de K est le carré d'un unique élément $b > 0$ (l'autre racine de $x^2=a$ étant $-b$); on réserve la notation $\sqrt{a}$ à cet élément b .

De même, comme la fonction polynome x^{2n} est strictement croissante pour $x \geqslant 0$, l'équation $x^{2n}=a$ admet, d'après la prop.8, une racine positive et une seule, qu'on désigne par $\sqrt[2n]{a}$ (elle admet aussi la racine négative $-\sqrt[2n]{a}$). La fonction polynome x^{2n+1} est strictement croissante dans K ; quelque soit a K (positif ou non), l'équation $x^{2n+1}=a$, admet donc une seule racine dans K , qui a le signe de a , et qu'on note $\sqrt[2n+1]{a}$.

Si K est un corps ordonné quelconque, l'extension $K(i)$, où i est une racine du polynome X^2+1 , est une extension galoisienne de degré 2 de K (puisque -1 n'est pas un carré dans K) ; tout élément $z \in K(i)$

s'écrit d'une seule manière sous la forme $z=x+iy$, où x et y appartiennent à K ; on pose $x=\mathcal{R}(z)$, $y=\mathcal{I}(z)$; $\mathcal{R}$ et $\mathcal{I}$ sont des formes linéaires sur K(i) (considéré comme espace vectoriel sur K) .

Le seul conjugué de i (relatif à K) distinct de i est $-i$; le groupe de Galois de K(i) par rapport à K se compose donc de l'automorphisme identique, et de l'automorphisme qui fait correspondre à $z=x+iy$ son conjugué $x-iy$, qu'on désigne par $\bar{z}$; on notera que $\mathcal{R}(z)=\frac{1}{2}(z+\bar{z})$, $\mathcal{I}(z)=\frac{1}{2i}(z-\bar{z})$. La <u>norme</u> N(z) de z relative à K (chap.V, § 6, n°7) est égale à $z\bar{z}=x^2+y^2$; elle est <u>positive</u> pour toute structure d'ordre sur K compatible avec la structure de corps de K , et la relation $N(z)=0$ entraîne $z=0$.

Si tout élément $a \geqslant 0$ de K a une racine carrée $\geqslant 0$ dans K (qu'on note encore $\sqrt{a}$), l'élément positif $\sqrt{N(z)}=\sqrt{z\bar{z}}$ se réduit à la valeur absolue de z lorsque $z \in K$; aussi, pour tout $z \in K(i)$, pose-t-on encore $|z| = \sqrt{N(z)}$, et appelle-t-on cet élément la <u>valeur absolue</u> de z ; on a $|zz'|=|z|.|z'|$, d'après la propriété correspondante des normes ; en outre, on a l'<u>inégalité du triangle</u>

$$|z+z'| \leqslant |z| + |z'| \tag{5}$$

En effet, l'inégalité étant évidente si $z=0$ ou $z'=0$, on peut supposer $zz' \neq 0$; en divisant par z , on se ramène à prouver que $|1+u| \leqslant 1 + |u|$, ou, ce qui revient au même $|1+u|^2 \leqslant 1+2|u| + |u|^2$; or, $|1+u|^2 = (1+u)(1+\bar{u}) = 1+|u|^2 + u+\bar{u}$; tout revient donc à prouver que $u+\bar{u} \leqslant 2|u|$; si $u=x+iy$, cette relation s'écrit $x \leqslant \sqrt{x^2+y^2}$, qui est évidente.

§ 3. Divisibilité dans un corps.

Anneaux arithmétiques et anneaux principaux.

1. Relations de divisibilité dans un corps commutatif.

Soit K un corps commutatif, A un anneau contenu dans K , et contenant l'élément unité 1 de K . Dans le groupe multiplicatif K^* des éléments $\neq 0$ de K , considérons l'ensemble $P=A \cap K^*$ des éléments $\neq 0$ de l'anneau A ; on a $1 \in P$ et $P.P \subset P$, donc P est un semi-groupe multiplicatif (§ 1, n°3) contenu dans le groupe K^* ; il définit par suite sur ce dernier une structure de groupe (multiplicatif) préordonné. L'ensemble $E=P \cap P^{-1}$, sous-groupe du groupe multiplicatif K^*, n'est autre que le groupe des éléments inversibles (dans A) de l'anneau A ; on sait (§ 1, n°3) que, dans le groupe quotient K^*/E , le semi-groupe P/E définit une structure de groupe ordonné.

Si x et y sont deux éléments de P , la relation $xy^{-1} \in P$ (qui, par passage au quotient, donne la relation d'ordre dans P/E) est équivalente à "il existe $z \in A$ tel que $x=yz$" , autrement dit signifie que y divise x. Généralisant cette terminologie, nous dirons qu'un élément $y \neq 0$ de K divise un élément $x \in K$ (relativement à l'anneau A) si $xy^{-1} \in A$; restreinte à K^*, cette relation n'est autre que la relation réflexive et transitive qui, par passage au quotient, donne la relation d'ordre sur le groupe K^*/E ; nous la noterons $y|x$, et sa négation $y \nmid x$; nous dirons encore lorsque y divise x , que y est un diviseur de x , et x un multiple de y . On a $x|0$ pour tout $x \in K^*$. L'étude de la relation $y|x$ est ce que nous appellerons la théorie de la divisibilité dans K (par rapport à l'anneau A) . Les éléments de A ne sont autres que les multiples de 1 ; dans la théorie de la divisibilité, on les qualifie d'éléments entiers. Les éléments du groupe E sont les éléments

de A qui sont <u>diviseurs de</u> 1 ; on leur donne souvent ce nom (ou encore, par abus de langage, le nom d'<u>unités</u> de l'anneau A , quand aucune confusion n'en résulte). La relation "$x|y$ et $y|x$" équivaut à dire que $\frac{x}{y}$ est diviseur de 1 (ou encore que, dans le groupe multiplicatif K^*, x et y sont congrus modulo le sous-groupe E) ; on dit encore dans ce cas que x et y sont des <u>éléments associés</u> de K . Lorsque x divise y mais n'est pas associé à y , on dira qu'il <u>divise strictement</u> y ou est un <u>diviseur strict</u> de y (et y un <u>multiple strict</u> de x).

La distributivité de la multiplication par rapport à l'addition dans A entraîne l'importante propriété suivante :

PROPOSITION 1.- <u>Si</u> $x|y$ <u>et</u> $x|z$, <u>alors</u> $x|(y-z)$.

En effet, on a $y=ax$, $z=bx$, où a et b sont dans A , donc $y-z=(a-b)x$ et $a-b \in A$.

<u>Corollaire.-</u> <u>Si</u> $x|y$ <u>et</u> $x \nmid z$, <u>alors</u> $x \nmid (y-z)$.

Sinon, x diviserait $y-(y-z)=z$.

Inversement, toute relation réflexive et transitive $x(\sigma)y$ dans K (où $x=0$), telle que $x(\sigma)y$ entraîne $xz(\sigma)yz$ pour $z \neq 0$, et que "$x(\sigma)y$ et $x(\sigma)z$" entraîne $x(\sigma)(y-z)$ est une relation de divisibilité dans K . En effet, l'ensemble A des $x \in K$ tels que $1(\sigma)x$ satisfait aux relations $A-A \subset A$ et $A.A \subset A$, qui prouvent que A est un <u>anneau</u> contenu dans K et tel que $1 \in A$; d'autre part, si $x(\sigma)y$ et $x \neq 0$, on a $1(\sigma)yx^{-1}$ donc $yx^{-1} \in A$ et réciproquement ; $x(\sigma)y$ est donc identique à la relation de divisibilité dans K , par rapport au sous-anneau A .

Bien entendu, à chaque sous-anneau de K contenant 1 correspondra dans K une théorie de la divisibilité différente.

Nous nous limiterons dans ce qui suit au cas où K est le <u>corps des fractions</u> de l'anneau A ; les éléments de K sont alors dits éléments

fractionnaires ; on sait (chap.I, § 9, n°4) que tout élément de K peut alors s'écrire sous la forme $\frac{a}{b}$, où a et b sont entiers ($b \neq 0$) ; on dit que cette expression est la fraction de numérateur a et de dénominateur b Il revient au même de dire que le groupe ordonné K^*/E est filtrant (§ 1, n°6, prop.4).

Lorsque x et y sont deux éléments de l'anneau A, la relation $x|y$ signifie que y appartient à l'idéal principal (x), ce qui s'écrit $y \equiv 0 \pmod{(x)}$; il revient au même de dire que l'on a la relation $(y) \subset (x)$ entre les idéaux principaux (x) et (y).

Etendant la notion d'idéal principal, nous dirons que, pour tout $x \in K$, l'ensemble des éléments zx, où z parcourt A (autrement dit, l'ensemble des multiples de x, ou encore le A-module A.x) est un idéal principal fractionnaire, que nous noterons (x) ; lorsque $x \in A$, on dit que l'idéal principal (x) est entier. Alors la relation $x|y$ est équivalente à $(y) \subset (x)$; pour que $(x)=(y)$ $(\neq(0))$, il faut et il suffit que x et y soient associés de K. L'application $x \longrightarrow (x)$ définiti donc, par passage au quotient, une application biunivoque du groupe ordonné K^*/E sur l'ensemble $\mathcal{P}^*$ des idéaux principaux $\neq 0$; en transportant par cette application la structure de groupe de K^*/E à $\mathcal{P}^*$, on définit donc le produit de deux idéaux principaux (x),(y) comme égal à l'idéal principal (xy) ; muni de cette loi de composition et de la relation d'ordre $(y) \subset (x)$, $\mathcal{P}^*$ est donc un groupe ordonné (multiplicatif) isomorphe à K^*/E.

2. Anneaux arithmétiques.

DÉFINITION 1.- On dit qu'un anneau d'intégrité A ayant un élément unité est un anneau arithmétique, si le groupe multiplicatif des idéaux principaux fractionnaires $\neq(0)$ du corps des fractions K de A (ou, ce qui revient au même, le groupe K^*/E quotient de K^* par le

le groupe des éléments inversibles de A) est un groupe ordonné décomposable (§ 1, n°11, déf. 10).

Nous verrons un peu plus loin que l'anneau $\mathbb{Z}$ des entiers rationnels est un anneau arithmétique, et que tout anneau de polynomes sur un anneau arithmétique est un anneau arithmétique.

Nous commencerons par traduire les principaux résultats du § 1 relatifs aux groupes décomposables, dans la terminologie propre à la théorie de la divisibilité.

Le lecteur verra de lui-même pour lesquelles de ces propriétés il suffirait de supposer que le groupe K^*/E est réticulé ; nous nous bornons ici à étudier le cas, de beaucoup le plus important d'après les exemples qui précèdent, où ce groupe est décomposable.

A la notion de borne inférieure (resp. supérieure) d'une partie d'un groupe ordonné additif correspond dans le groupe multiplicatif K^*/E ordonné (par la relation déduite de $x|y$ par passage au quotient) la notion de plus grand commun diviseur (resp. plus petit commun multiple): de façon précise, on dira qu'un élément $d \in K$ est plus grand commun diviseur (en abrégé p.g.c.d.) d'une partie H de K si d est diviseur de tous les éléments de H , et si tout élément qui est diviseur de tous les éléments de H est aussi diviseur de d : la classe de d dans K^*/E est donc borne inférieure des classes des éléments de H , et si d,d' sont tous deux p.g.c.d. d'un même ensemble H , ils sont associés. De même, on dira que $m \in K$ est plus petit commun multiple (en abrégé p.p.c.m.) de H si m est multiple de tous les éléments de H et si tout élément qui est multiple de tous les éléments de H est multiple de m . Si d est p.g.c.d. d'une partie H de K^* , d^{-1} est p.p.c.m. de l'ensemble H^{-1} des inverses des éléments de H (§ 1, prop. 5).

Comme K^*/E est un groupe réticulé par hypothèse, toute partie finie de K^* admet un p.g.c.d. et un p.p.c.m. En outre, on a les propositions suivantes :

PROPOSITION 2.- Si H et H' sont deux parties finies de K^*, d (resp. d') un p.g.c.d. de H (resp. H'), dd' est un p.g.c.d. de HH' .

C'est la traduction de la prop.7 du § 1 .

COROLLAIRE.- Le produit dd' est aussi p.g.c.d. du A-module engendré par HH' .

C'est une conséquence immédiate de la prop.1 .

PROPOSITION 3.- Si d est p.g.c.d. de deux éléments x,y de K , d^n est p.g.c.d. de x^n et y^n pour tout entier rationnel $n > 0$.

COROLLAIRE.- Si x est un élément de K tel que x^n soit entier pour un entier rationnel $n > 0$, x est entier.

Ce sont les traductions de la prop.9 du § 1 et de son cor. 2 .

PROPOSITION 4.- Si d est un p.g.c.d. de deux éléments x,y de K xy/d est p.p.c.m. de x et y.

Traduction du cor. de la prop.8 du § 1 .

Nous laissons au lecteur le soin de traduire de la même manière les propriétés d'associativité et de distributivité réciproque (§ 1, cor.2 de la prop.11) des opérations sup et inf dans un groupe réticulé.

3. Entiers relativement premiers dans un anneau arithmétique.

A la notion d'éléments positifs étrangers (§ 1, n°9) dans un groupe réticulé additif correspond, dans un anneau arithmétique celle d'entiers relativement premiers. Nous dirons que n entiers x_i $(1 \leqslant i \leqslant n)$ sont relativement premiers, ou premiers entre eux (ou encore premiers entre eux dans leur ensemble, pour éviter toute confusion) si 1 est un p.g.c.d. de ces n éléments. Si, pour tout i , y_i est un entier

divisant x_i , et si les x_i sont premiers entre eux, il en est de même des y_i .

Les propositions suivantes traduisent les propositions du § 1, n°9 relatives aux éléments étrangers :

PROPOSITION 5.- Si x,y,z sont trois entiers tels que x et y soient premiers avec z , xy est premier avec z .

COROLLAIRE.- Si x et y sont premiers entre eux, x^p et y^q sont premiers entre eux, quels que soient les entiers rationnels $p > 0$ et $q > 0$.

PROPOSITION 6.- Soient x,y,z trois entiers ; si x est premier avec y et s'il divise yz , il divise z .

PROPOSITION 7.- Soit d un p.g.c.d. de deux éléments x,y de K ; les entiers x/d et y/d sont premiers entre eux.

PROPOSITION 8.- Soit (a_i) une suite finie d'entiers, premiers entre eux deux à deux ; si x est multiple de chacun des a_i , il est multiple de leur produit.

Il suffit de raisonner par récurrence sur le nombre n de termes de la suite (a_i), la proposition étant triviale pour n=1 . Comme a_n est premier avec a_p pour $1 \leqslant p \leqslant n-1$, a_n est premier avec $a_1 a_2 \ldots a_{n-1}$ d'après la prop.5 ; par hypothèse x est multiple de a_n , et d'autre part x est multiple de $a_1 a_2 \ldots a_{n-1}$ d'après l'hypothèse de récurrence ; donc, comme le produit de deux entiers premiers entre eux est p.p.c.m. de ces entiers (§ 1, cor.1 de la prop.13), x est multiple de $a_1 a_2 \ldots a_{n-1} a_n$.

4. Fractions irréductibles.

A l'expression $x=x^+-x^-$ de tout élément d'un groupe additif réticulé correspond, dans un anneau arithmétique l'expression irréductible d'une fraction quelconque $x \in K^*$; si $x=a/b$, où a et b sont entiers $\neq 0$, soit d un p.g.c.d. de a et b ; on a $a=dp$, $b=dq$, et p et q sont

deux entiers premiers entre eux (prop.7 et tels que $x=p/q$; une telle expression de x comme quotient de deux entiers premiers entre eux est dite irréductible.

PROPOSITION 9.- Si p/q est une expression irréductible d'une fraction a/b , a est multiple de p et b multiple de q .

En effet, on a $aq=bp$, donc q divise bp , et comme il est premier avec p , il divise b (prop.6) ; si on pose $b=dq$ (d entier), on a $a=dp$.

Si p/q et p'/q' sont deux expressions irréductibles d'une même fraction, p est donc associé à p' et q associé à q' .

5. Entiers premiers dans un anneau arithmétique.

A la notion d'élément premier d'un groupe additif ordonné (§ 1, n°10) correspond, dans un anneau d'intégrité A ayant un élément unité, celle d'entier premier : un entier $p\neq 0$ non diviseur de 1 est dit premier si la relation $p|xy$ (x et y entiers) entraîne "$p|x$ ou $p|y$" . Comme la relation $p|x$ est équivalente à $x\in(p)$, on peut encore définir les entiers premiers $p\in A$ comme ceux qui possèdent la propriété que l'anneau quotient $A/(p)$ est un anneau d'intégrité.

De même, à la notion d'élément minimal d'un groupe ordonné additif (§ 1,n°10) correspond, dans A , celle d'entier indivisible : un entier $p\neq 0$ et non diviseur de 1 est dit indivisible si les seuls diviseurs de p sont les diviseurs de 1 et les entiers associés à p . Dans un anneau d'intégrité, tout entier premier est indivisible (§ 1,prop.19) ; la réciproque est inexacte en général (cf. exerc. 1).

Si A est un anneau arithmétique, les notions d'entier premier et d'entier indivisible sont identiques (§ 1,prop.18 et 19) ; si p et q sont deux entiers premiers, ou bien ils sont associés, ou bien ils sont relativement premiers. La définition des anneaux arithmétiques donne la proposition suivante :

PROPOSITION 10.- Soit (p_ι) une famille d'entiers premiers d'un anneau arithmétique A, telle que tout entier premier de A soit associé à un p_ι, et que deux entiers p_ι, p_κ d'indices distincts ne soient pas associés. Tout élément $x \neq 0$ du corps des quotients K de A peut alors s'écrire d'une manière et d'une seule sous la forme

$$x = \rho \prod_\iota p_\iota^{n_\iota} \tag{1}$$

où ρ est un diviseur de 1 dans A, et les n_ι des entiers rationnels, nuls sauf un nombre fini d'entre eux ; pour que x soit entier, il faut et il suffit que $n_\iota \geqslant 0$ pour tout ι.

Le second membre de (1) est appelé la décomposition de x en facteurs premiers. Lorsque x est entier, et qu'on connaît sa décomposition en facteurs premiers, il est facile de déterminer tous les entiers qui divisent x : ce sont les entiers de la forme $\lambda \prod_\iota p_\iota^{m_\iota}$, où $0 \leqslant m_\iota \leqslant n_\iota$ pour tout ι, et où λ est un diviseur de 1 quelconque. Le nombre des classes (mod.E) des diviseurs entiers de x est donc

$$\tau(x) = \prod_\iota (n_\iota + 1) \tag{2}$$

Etant donnés deux éléments $x = \alpha \prod_\iota p_\iota^{n_\iota}$, $y = \beta \prod_\iota p_\iota^{m_\iota}$ de K^*, décomposés en facteurs premiers, les p.g.c.d. de x et y sont les éléments $\gamma \prod_\iota p_\iota^{\inf(m_\iota, n_\iota)}$, les p.p.c.m. de x et y sont les éléments $\delta \prod_\iota p_\iota^{\sup(m_\iota, n_\iota)}$, α, β, γ et δ étant des diviseurs de 1 quelconques.

6. Anneaux principaux.

DEFINITION 2.- On dit qu'un anneau d'intégrité A, ayant un élément unité, est un anneau principal, lorsque tout idéal de A est un idéal principal.

Nous avons déjà vu (chap.I, § , n°5, et chap.IV, §) que l'anneau $\mathbb{Z}$ des entiers rationnels et l'anneau $K[X]$ des polynomes à une indéterminée sur un corps quelconque sont

des anneaux principaux ; nous reviendrons ci-dessous à l'étude de la théorie de la divisibilité dans ces deux anneaux.

THEOREME 1.- Tout anneau principal est un anneau arithmétique.

Nous allons montrer pour cela que le groupe ordonné $\mathscr{P}^*$ des idéaux principaux fractionnaires $\neq(0)$ du corps des quotients K de A est un groupe décomposable, en appliquant le th.1 du § 1. Prouvons en premier lieu que $\mathscr{P}^*$ est réticulé ; soient (a) et (b) deux éléments de $\mathscr{P}^*$; on peut écrire $a=p/r$, $b=q/r$, où p,q,r sont entiers, d'où $(a)=(p)(r)^{-1}$ et $(b)=(q)(r)^{-1}$, tout revient à prouver que les idéaux principaux entiers (p) et (q) admettent dans $\mathscr{P}^*$ une borne inférieure (pour la relation d'ordre opposée à la relation d'inclusion) : or (p)+(q) est un idéal de A , donc principal par hypothèse, soit (p)+(q)=(d) ; pour tout idéal principal (s) tel que $(p)\subset(s)$ et $(q)\subset(s)$, on a $(p)+(q)\subset(s)$, donc $(d)\subset(s)$, et inversement $(p)\subset(p)+(q)$ et $(q)\subset(p)+(q)$; l'idéal (d) est donc bien la borne inférieure de (p) et (q) .

En second lieu, montrons que le groupe ordonné $\mathscr{P}^*$ satisfait à la condition (T) du th.1 du § 1 : cela revient à voir ici qu'il ne peut exister une suite infinie $((a_n))$ d'idéaux fractionnaires principaux distincts et un idéal principal (b), tels que $(a_n)\subset(b)$ et $(a_{n+1})\supset(a_n)$ pour tout n . En effet, ces hypothèses entraînent que $c_n=a_n/b$ est entier et $c_{n+1}\mid c_n$ pour tout n ; considérons l'idéal de A engendré par l'ensemble des c_n ; par hypothèse, c'est un idéal principal (entier)(d), et la définition de cet idéal prouve qu'il existe un indice p tel que $d=\lambda_1 c_1+\ldots+\lambda_p c_p$, où les λ_i sont entiers d'où $c_p\mid d$ puisque c_p divise c_i pour $i<p$. Pour tout $n\geqslant p$, on a donc $c_n\mid d$; mais par définition $d\mid c_n$, donc $(d)=(c_n)$; par suite tous les

les idéaux (c_n) sont identiques pour $n \geqslant p$, et il en est de même de tous les idéaux (a_n).

Comme la relation $a|b$ équivaut à $(b) \subset (a)$, les idéaux maximaux (chap.I, §8, n°7) d'un anneau principal A sont identiques aux idéaux (p) engendrés par les éléments premiers de A ; pour tout élément premier p de A , l'anneau quotient $A/(p)$ est donc un corps (chap.I, § 9, th.2). Cela peut encore s'exprimer de la manière suivante :

PROPOSITION 11.- Dans un anneau principal A , soient p un entier premier, a et b deux entiers tels que $a \not\equiv 0 \pmod{p}$; la congruence

$$ax \equiv b \pmod{p}$$

a des solutions dans A ; si x_0 est une de ces solutions, toute autre solution est de la forme $x_0 + kp$, où k parcourt A .

Si $(\mathfrak{p}_i)$ désigne la famille des idéaux maximaux (principaux) de A, tout idéal fractionnaire (principal) $\mathfrak{a} \neq (0)$ de K peut s'écrire d'une seule manière sous la forme

$$\mathfrak{a} = \prod_i \mathfrak{p}_i^{n_i} \tag{3}$$

où les n_i sont des entiers rationnels positifs ou négatifs, nuls à l'exception d'un nombre fini d'entre eux.

PROPOSITION 12.- Soit A un anneau principal, K son corps des quotients ; si a et b sont deux éléments $\neq 0$ de K , d un p.g.c.d. de a et b , il existe deux entiers p,q de A tels que

$$d = pa + qb \tag{4}$$

En effet, (d) est la borne inférieure de (p) et (q) dans le groupe ordonné $\mathfrak{P}^*$, et on a vu dans la démonstration du th.1 que cette borne inférieure est identique à $(p) + (q)$.

COROLLAIRE 1.- Dans un anneau principal A , si a et b sont deux entiers relativement premiers, il existe deux entiers p,q tels que

$$1 = pa + qb . \tag{5}$$

COROLLAIRE 2.- Dans un anneau principal A , soient a,b,c trois entiers (tels que $ab \neq 0$), d un p.g.c.d. de a et b ; pour qu'il existe deux entiers x,y dans A tels que

(6) $$ax + by = c$$

il faut et il suffit que c soit multiple de d .

En effet, la relation (6) exprime que c appartient à l'idéal $(a)+(b) = (d)$.

On généralise aussitôt la prop.12 et ses corollaires à un nombre quelconque d'éléments de K^* .

7. Divisibilité dans l'anneau Z .

Nous avons déjà rappelé que l'anneau Z des entiers rationnels est un anneau principal (chap.I, § 8, n°5). Les seuls diviseurs de 1 dans Z sont +1 et -1 ; les nombres rationnels associés à un nombre r sont donc r et -r .

Lorsqu'on parle d'un diviseur (resp. multiple) d'un entier rationnel $n > 0$, on sous-entend d'ordinaire qu'il s'agit de diviseurs (resp. multiples) qui sont > 0 ; deux entiers > 0 ont un seul p.g.c.d. (resp. p.p.c.m.) qui soit > 0 ; c'est de ce nombre qu'il s'agit lorsqu'on parle du p.g.c.d. (resp. du p.p.c.m.) de deux entiers > 0

Les éléments premiers > 0 de Z sont appelés nombres premiers rationnels (ou simplement nombres premiers, cf.chap.I, § 8, n°7) ; tout élément premier de Z est donc de la forme p ou -p , où p est un nombre premier.

PROPOSITION 13.- L'ensemble des nombres premiers est infini.

Raisonnons par l'absurde, et supposons qu'il n'y ait que n nombres premiers p_i $(1 \leqslant i \leqslant n)$. Considérons le nombre $a=1+p_1p_2\cdots p_n$; comme il est >1 , il admet au moins un diviseur premier p , et l'hypothèse entraîne que $p=p_i$ pour un indice i mais comme p_i divise $p_1p_2\cdots p_n$; il diviserait $a-p_1p_2\cdots p_n=1$, ce qui est absurde.

8. Divisibilité dans les anneaux de polynomes.

Nous avons vu (chap.IV, §) que l'anneau $K[X]$ des polynomes à une indéterminée sur un corps quelconque (commutatif) K est un anneau principal. Le degré du produit de deux polynomes $\neq 0$ étant égal à la somme des degrés des facteurs, les diviseurs de 1 dans $K[X]$ sont les éléments $\neq 0$ de K (polynomes de degré 0). Les éléments premiers u de $K[X]$ sont les polynomes tels que l'idéal (u) soit maximal, donc les polynomes que nous avons appelés polynomes irréductibles (chap.IV, §). Tout polynome du premier degré est irréductible ; la réciproque n'est exacte que si K est algèbriquement fermé (chap.V , § 3).

PROPOSITION 14.- Si f et g sont deux polynomes de $K[X]$, de degrés respectifs m et n non tous deux nuls, et si h est un p.g.c.d. de f et g dans ~~kxxx~~ $K[X]$, il existe dans $K[X]$ un polynome u de degré $< n$ et un polynome v de degré $< m$ tels que

$$h = uf + vg \tag{7}$$

(identité de Bezout).

En effet, la prop.12 montre qu'il existe deux polynomes u_1, v_1 de $K[X]$ tels que $h=u_1 f + v_1 g$; si on divise u_1 par g , on peut écrire $u_1 = pg+u$, où deg.u $< n$; on a $h=uf+(pf+v_1)g$; si on pose $v=pf+v_1$, on a $vg=h-uf$, donc $\deg(vg) < m+n$ (le degré de h étant au plus égal au plus petit des degrés de f et g) ; d'où deg $v<m$, ce qui achève la démonstration.

COROLLAIRE 1.- Si f et g sont deux polynomes premiers entre eux dans $K[X]$, de degrés respectifs m et n non tous deux nuls, pour tout polynome h de $K[X]$, de degré $\leq m+n$, il existe dans $K[X]$ un polynome et un seul u de degré $< n$ et un polynome et un seul v de degré $< m$, tels que l'on ait identiquement (7) .

En effet, il existe deux polynomes u_1, v_1 tels que $1=u_1f+v_1g$, d'où $h=hu_1f+hv_1g$; divisant hu_1 par g, il vient $hu_1=pg+u$ où deg $u<n$, d'où $h=uf+(pf+hv_1)g$, et si $v=pf+hv_1$, on a $vg=h-uf$, d'où deg$(vg)<m+n$ et deg $v<m$. Si maintenant on a $h=u_2f+v_2g$ avec deg $u_2<n$ et deg $v_2<m$, on a $(u-u_2)f=(v_2-v)g$; comme g est premier avec f, il diviserait $u-u_2$ si ce dernier polynome était $\neq 0$; mais cela est impossible puisque deg$(u-u_2)<$deg g ; donc on a $u=u_2$ et $v=v_2$.

COROLLAIRE 2.- Soit K' un sur-corps de K ; si h est p.g.c.d. de f et g dans l'anneau $K[X]$, h est encore p.g.c.d. de f et g dans l'anneau $K'[X]$. ~~h est encore p.g.c.d. de f et g dans l'anneau K' X~~.

En effet (7) montre que h appartient à l'idéal $(f)+(g)$ dans $K'[X]$; comme f et g sont multiples de h dans $K'[X]$, on a $(h)=(f)+(g)$ dans $K'[X]$.

Soit maintenant A un anneau d'intégrité qui n'est pas un corps ; alors l'anneau $A[X]$ des polynomes à une indéterminée sur A n'est jamais un anneau principal ; en effet, si a est un élément de A, non diviseur de 1, l'idéal $(a)+(X)$ ne peut être un idéal principal dans $A[X]$, car si on avait $(a)+(X)=(f)$, f serait nécessairement un élément de A, et comme X est multiple de f, f devrait être diviseur de 1 dans A, ce qui est impossible, aucun multiple de a ne pouvant être diviseur de 1.

On remarquera en outre que les diviseurs de 1 dans $A[X]$ sont identiques aux diviseurs de 1 dans A.

THEOREME 2.- Soit A un anneau d'intégrité. Pour que l'anneau $A[X]$ des polynomes à une indéterminée sur A soit un anneau arithmétique, il faut et il suffit que A soit un anneau arithmétique.

Delsarte

La nécessité de cette condition est immédiate : en effet, si a et b sont deux éléments de A tels que a divise b dans l'anneau $A[X]$, a divise b dans l'anneau A et réciproquement ; comme deux éléments quelconques non nuls x,y de A ont par hypothèse un p.g.c.d. z dans $A[X]$, et que z ne peut être qu'un polynome de degré 0, c'est-à-dire un élément de A, z est aussi p.g.c.d. de x et y dans l'anneau A ; donc le groupe $\mathcal{P}^*$ des idéaux principaux fractionnaires $\neq(0)$ du corps des quotients K de A est réticulé ; en outre pour tout élément $a\neq 0$ de A il ne peut exister dans l'anneau $A[X]$ qu'un nombre fini d'idéaux principaux entiers contenant a ; un tel idéal étant engendré par un élément de A, on voit que dans le groupe $\mathcal{P}^*$, l'idéal principal (a) n'est contenu que dans un nombre fini d'idéaux entiers, donc (§ 1, th. 1), $\mathcal{P}^*$ est un groupe décomposable.

Montrons que la condition est suffisante. Etant donné un polynome $f(X) = \sum_{k=0}^{n} a_k X^k$ de $K[X]$, nous appellerons contenu de f un p.g.c.d. des coefficients non nuls de f ; un polynome ayant pour contenu 1 sera dit primitif ; si d est un contenu de f, on peut évidemment écrire $f(X)=dg(X)$, où $g(X) = \sum_{k=0}^{n} \frac{a_k}{d} X^k$ est un polynome primitif ; réciproquement, si g est primitif et $d\in K^*$, dg a pour contenu d. Cela étant, nous allons établir le lemme fondamental suivant :

Lemme (Gauss).- Soient f et g deux polynomes non nuls de $K[X]$, d et d' leurs contenus respectifs ; le produit dd' est un contenu du produit fg.

Il est clair que dd' divise tous les coefficients de fg ; si on pose $f=df_1$, $g=dg_1$, tout revient à montrer que f_1g_1 est un polynome primitif. Soit $f_1(X) = \sum_{k=0}^{m} a_k X^k$, $g_1(X) = \sum_{k=0}^{n} b_k X^k$; si f_1g_1 n'était pas primitif, ses coefficients $\neq 0$ auraient un diviseur premier commun p ; soient $\dot{a}_k$, $\dot{b}_k$ les classes (mod.p) de a_k et b_k dans l'anneau $A/(p)$

et posons $\dot{f}_1 = \sum_{k=0}^{m} \dot{a}_k X^k$, $\dot{g}_1 = \sum_{k=0}^{n} \dot{b}_k X^k$; par hypothèse les polynomes $\dot{f}_1, \dot{g}_1$ de $(A/(p))[X]$ sont $\neq 0$ et leur produit serait nul, ce qui est absurde, puisque $A/(p)$ est un anneau d'intégrité (chap.IV, §).

Il résulte de ce lemme que, si f et g sont deux polynomes primitifs de $A[X]$, tels que g divise f dans l'anneau $K[X]$, f/g est un polynome primitif, donc g divise f dans l'anneau $A[X]$; en particulier, les polynomes primitifs qui sont des éléments indivisibles de $A[X]$ sont identiques aux polynomes primitifs et irréductibles de $K[X]$; donc, les éléments indivisibles de $A[X]$ sont les éléments premiers de A et les polynomes primitifs et irréductibles. Or, un élément premier p de A ne peut diviser le produit fg de deux polynomes de $A[X]$ sans diviser l'un d'eux, puisqu'il divise le produit des contenus de f et g ; donc p est premier dans $A[X]$. De même, soit h un polynome primitif irréductible qui divise le produit de deux polynomes $f=df_1$, $g=dg_1$, où d et d' sont des contenus de f et g ; h divise $f_1 g_1$ dans l'anneau $K[X]$; étant irréductible, il divise aussi f_1 ou g_1 dans $K[X]$, et comme il est primitif il divise f_1 ou g_1 dans $A[X]$, ce qui montre que h est un élément premier de $A[X]$. Pour appliquer le th.1 du § 1, il reste à vérifier l'axiome (T) ; il est immédiat qu'on peut se limiter au cas d'une suite (f_n) de polynomes primitifs de $A[X]$, telle que $f_{n+1} \mid f_n$ quel que soit n ; si f_{n+1} n'est pas associé à f_n , son degré est strictement inférieur à celui de f_n ; donc il existe un n_0 tel que f_n soit associé à f_{n_0} pour $n \geqslant n_0$, sans quoi la suite des degrés des f_n serait décroissante et aurait une infinité de termes distincts. Le th.2 est donc complétement démontré.

Pour avoir une décomposition en facteurs premiers d'un polynome $d=df_1$ de $A[X]$, où d est un contenu de f , il suffira de décomposer d en facteurs premiers dans A et f_1 en facteurs irréductibles

(qu'on peut toujours prendre primitifs, puisque le produit de leurs contenus est diviseur de 1) dans $K[X]$.

Ce résultat peut s'interprèter de la manière suivante : appelons <u>fraction rationnelle primitive</u> dans K(X) une fraction qui est égale au quotient de deux polynomes primitifs ; il est clair que ces fractions forment un sous-groupe H du groupe multiplicatif R^* des fractions rationnelles $\neq 0$ sur K . Si E désigne toujours le groupe des diviseurs de 1 dans A , on voit donc que le groupe multiplicatif R^*/E est isomorphe au <u>produit</u> des groupes K^*/E et H/E .

PROPOSITION 15.- <u>Si</u> A <u>est un anneau arithmétique</u> (en particulier si A est un <u>corps</u>), <u>l'anneau</u> $A[X_1, X_2, .., X_n]$ <u>des polynomes à n indéterminées sur</u> A <u>est un anneau arithmétique</u>.

Il suffit d'appliquer le th.2 par récurrence sur n , en considérant $A[X_1, .., X_n]$ comme l'anneau des polynomes en X_n sur l'anneau $A[X_1, .., X_{n-1}]$.

<u>9. Applications : I. Ensemble de définition d'une fonction rationnelle</u>.

Soit K un corps commutatif ; comme $K[X_1, .., X_n]$ est un anneau arithmétique, toute fraction rationnelle $r \in K(X_1, .., X_n)$ peut s'écrire sous la forme <u>irréductible</u> ($n^o 4$) f_0/g_0 , où f_0 et g_0 sont deux polynomes de $K[X_1, .., X_n]$ premiers entre eux, déterminés à un facteur constant près ; en outre, si f et g sont deux autres polynomes tels que $r = f\,g$, il existe un polynome $h \neq 0$ tel que $f = hf_0$, $g = hg_0$ (prop.9). Cela étant, supposons que le corps K soit <u>infini</u> ; alors l'ensemble A_0 des points $(x_1, \ldots, x_n) \in K^n$ tels que $g_0(x_1, \ldots, x_n) \neq 0$ n'est pas vide (chap.IV, §), et si $f/g = r$, l'ensemble A des points où $g(x_1, \ldots, x_n) \neq 0$ contient A_0 . Donc, parmi toutes les <u>fonctions rationnelles</u> (chap.IV, §) qui correspondent à la <u>fraction rationnelle</u> r ,

la fonction $(x_1,..,x_n) \to f_0(x_1,..,x_n)/g_0(x_1,..,x_n)$ est celle dont l'ensemble de définition $\int A_0$ est le plus grand ; quand on parlera désormais de la fonction rationnelle correspondant à r , sans autre précision, il sera toujours sous-entendu que c'est de la fonction rationnelle précédente qu'il s'agira.

10. Applications : II. Décomposition canonique des fractions rationnelles à une indéterminée.

Soit K un corps commutatif, r une fraction rationnelle à une indéterminée sur K , f/g une expression irréductible ($n^o 4$) de r dans le corps K(X) ; on peut écrire $g = g_1^{\nu_1} g_2^{\nu_2} \cdots g_m^{\nu_m}$, où les g_i sont des polynomes irréductibles de $K[X]$, déterminés à un facteur constant près, les ν_i des entiers rationnels >0 bien déterminés. L'identité de Bezout (prop.14) appliquée aux polynomes premiers entre eux $g_1^{\nu_1} g_2^{\nu_2} \cdots g_{m-1}^{\nu_{m-1}}$ et $g_m^{\nu_m}$ montre qu'il existe deux polynomes u_m et h_m tels que

$$\frac{1}{g} = \frac{u_m}{g_1^{\nu_1} g_2^{\nu_2} \cdots g_{m-1}^{\nu_{m-1}}} + \frac{h_m}{g_m^{\nu_m}}$$

Par récurrence sur m , on voit donc qu'il existe m polynomes h_i $(1 \leqslant i \leqslant m)$ tels que

$$\frac{1}{g} = \frac{h_1}{g_1^{\nu_1}} + \frac{h_2}{g_2^{\nu_2}} + \ldots + \frac{h_m}{g_m^{\nu_m}}$$

d'où

$$\frac{f}{g} = \frac{fh_1}{g_1^{\nu_1}} + \ldots + \frac{fh_m}{g_m^{\nu_m}}$$

Cela étant, divisons fh_i par g_i ; on a $fh_i = q_{i1}g_i + r_{i1}$ avec $\deg(r_{i1}) < \deg(g_i)$; on a donc

$$\frac{fh_i}{g_i^{\nu_i}} = \frac{r_{i1}}{g_i^{\nu_i}} + \frac{q_{i1}}{g_i^{\nu_i - 1}}$$

On procède de même pour la fraction $\frac{q_{i1}}{g_i^{\nu_i - 1}}$, et par récurrence sur k $(1 \leqslant k \leqslant \nu_i)$, on voit qu'on peut écrire

$$\frac{fh_i}{g_i^{\nu_i}} = q_i + \frac{r_{i1}}{g_i^{\nu_i}} + \frac{r_{i2}}{g_i^{\nu_i - 1}} + \ldots + \frac{r_{i,\nu_i}}{g_i}$$

où $\deg(r_{ik}) < \deg(g_i)$ pour $1 \leqslant k \leqslant \nu_i$; d'où finalement

$$(8) \qquad \frac{f}{g} = q + \sum_{i=1}^{m} \left(\sum_{k=1}^{\nu_i} \frac{r_{ik}}{g_i^{\nu_i - k + 1}} \right)$$

Le second membre de (8) est appelé la décomposition canonique de la fraction rationnelle f/g . Il est aisé de voir que (les g_i étant déterminés par le choix du facteur diviseur de 1 dont chacun dépend) une telle décomposition est unique, c'est-à-dire que les polynomes q et r_{ik} qui figurent au second membre de (8) sont déterminés par la relation (8) et la condition $\deg(r_{ik}) < \deg(g_i)$ pour $1 \leqslant i \leqslant m$ et $1 \leqslant k \leqslant \nu_i$. En effet, on déduit en premier lieu de (8) que l'on a

$$(9) \qquad \frac{f}{g} = q + \sum_{i=1}^{m} \frac{h_i}{g_i^{\nu_i}}$$

où $\deg(h_i) < \deg(g_i^{\nu_i})$; par suite $\deg(f - qg) < \deg(g)$, ce qui prouve en premier lieu que q est le quotient euclidien de f par g . La relation (9) donne ensuite

$$f - qg = h_m g_1^{\nu_1} \cdots g_{m-1}^{\nu_{m-1}} + u_m g_m^{\nu_m}$$

où $\deg(u_m) < \deg(g_1^{\nu_1} \cdots g_{m-1}^{\nu_{m-1}})$; d'après le cor.1 de la prop.14 , h_m et u_m sont déterminés de façon unique par ces conditions ; comme on peut écrire

$$\frac{u_m}{g_1^{\nu_1} g_2^{\nu_2} \cdots g_{m-1}^{\nu_{m-1}}} = \sum_{i=1}^{m-1} \frac{h_i}{g_i^{\nu_i}}$$

on voit par récurrence sur m que les h_i sont bien déterminés pour $1 \leqslant i \leqslant m$; d'autre part, il est clair que r_{i1} est le reste de la division de h_i par g_i , r_{i2} le reste de la division de $(h_i - r_{i1})/g_i$ par g_i , et on voit ainsi par récurrence que les r_{ik} sont tous bien déterminés

Le cas le plus intéressant est celui où K est un corps algébriquement fermé ; alors chaque g_i peut être pris de la forme $X - a_i$ où $a_i \in K$, et les r_{ik} de la décomposition canonique sont des constantes ;

les constantes r_{i,ν_i} (numérateurs des fractions du second membre de (8) dont le dénominateur est du premier degré) sont appelés les résidus de la fraction f/g relatifs aux racines a_i de son dénominateur.

§ 4. Modules de type fini sur un anneau principal.

1. Modules de type fini et modules noethériens.

DEFINITION 1.- Etant donné un anneau A (commutatif ou non), on dit qu'un A-module à gauche (resp. à droite) est de type fini s'il possède un système fini de générateurs.

Un module monogène (chap.II, § 1, n°) est par définition un module de type fini. Si $(M_i)_{1 \leqslant i \leqslant n}$ est une famille finie de sous-modules de type fini d'un module E, la somme M de ces sous-modules est de type fini, puisqu'on obtient un système de générateurs de M en prenant la réunion de systèmes de générateurs de chacun des M_i. En particulier, le produit d'un nombre fini de modules de type fini est de type fini. Tout quotient E/H d'un module de type fini E est de type fini, car si φ est l'application canonique de E sur E/H, et S un système de générateurs de E, $\varphi(S)$ est un système de générateurs de $E/H = \varphi(E)$. On notera que d'après la prop. du chap.II, § 1, tout module unitaire de type fini est isomorphe à un module quotient de la forme A_g^n/H, où H est un sous-module quelconque de A_s^n.

Par contre, un sous-module d'un module de type fini n'est pas nécessairement un module de type fini.

Par exemple, soit A un anneau ayant un élément unité, $B = \prod_{n=1}^{\infty} A_n$ l'anneau produit d'une infinité dénombrable d'anneaux A_n tous identiques à A. Comme B admet un élément unité, le B-module à gauche B_g est monogène ; mais le sous-module C de B_g (idéal bilatère de B) formé des éléments n'ayant qu'un nombre fini de

coordonnées $\neq 0$ n'est pas de type fini, car si $(x_k)_{1 \leqslant k \leqslant p}$ est une partie finie quelconque de C , il existe une partie finie J de $\mathcal{N}$ telle que les coordonnées d'indice $i \notin J$ de chacun des x_k soient toutes nulles ; on en déduit aussitôt que tout élément du sous-module engendré par les x_k a aussi toutes ses coordonnées d'indice $i \notin J$ nulles, et par suite que ce sous-module ne peut être identique à C .

DÉFINITION 2.- On dit qu'un A-module à gauche M (resp. à droite) est noethérien si chacun de ses sous-modules est de type fini. On dit qu'un anneau A est un anneau noethérien à gauche (resp. à droite) si le A-module A_s (resp. A_d) est noethérien .

PROPOSITION 1.- Pour qu'un A-module E soit noethérien, il faut et il suffit qu'il satisfasse à l'axiome suivant :

(TK) Toute suite croissante (H_n) de sous-modules de E n'a qu'un nombre fini de termes distincts (autrement dit, on a $H_{n+1}=H_n$ à partir d'un certain rang).

Cet axiome n'est autre que l'axiome (T) du th.1 du § 1, formulé pour l'ensemble des sous-modules de E , et pour la relation d'ordre $\supset$ au lieu de $\leqslant$. On a vu au § 1, n°11 (remarque 1) qu'il est équivalent au suivant :

(TK') Tout ensemble non vide de sous-modules de E , ordonné par inclusion, a un élément maximal.

Aussi appelle-t-on l'axiome (TK') (ou l'axiome équivalent (TK)) condition maximale pour les sous-modules de E (cf. chap.I, § 6, exerc. 15).

La condition est nécessaire. En effet, supposons que tout sous-module de E soit de type fini, et soit (H_n) une suite croissante de sous-modules de E . La réunion H des H_n est un sous-module de E , donc est

engendrée par un nombre fini d'éléments a_i $(1 \leqslant i \leqslant p)$; chacun des a_i appartient à un H_n au moins, donc, comme la suite (H_n) est croissante, il existe un indice m tel que $a_i \in H_m$ pour $1 \leqslant i \leqslant p$, ce qui entraîne $H \subset H_m$, et par suite $H_n = H$ pour $n \geqslant m$.

La condition est <u>suffisante</u>. En effet, supposons que E satisfasse à (TK) , et soit H un sous-module quelconque de E . Si H n'était pas de type fini, on pourrait définir par récurrence (en utilisant l'axiome de choix) une suite (a_n) d'éléments de H telle que, si H_n est le sous-module engendré par $a_1, a_2, .., a_n$, on ait $a_{n+1} \notin H_n$. La suite (H_n) serait donc croissante et aurait tous ses termes distincts, contrairement à (TK), ce qui est absurde.

Tout <u>sous-module</u> d'un module noethérien est évidemment un module noethérien par définition. En outre, on a les propositions suivantes :

PROPOSITION 2.- <u>Tout module quotient d'un module noethérien est un module noethérien</u>.

En effet, tout sous-module de E/H est image canonique d'un sous-module $M \supset H$ de E , donc isomorphe à M/H , et on a vu que si M est de type fini, il en est de même de M/H .

PROPOSITION 3.- <u>Tout module produit d'un nombre fini de modules noethériens est un module noethérien</u>.

Il suffit évidemment de démontrer la proposition pour un produit $E \times F$ de deux modules noethériens, et de raisonner ensuite par récurrence sur le nombre des facteurs. Soit donc (H_n) une suite croissante de sous-modules de $E \times F$, et soit K_n la projection de H_n sur E ; on a $K_n \subset K_{n+1}$, donc il existe un entier m tel que $K_n = K_m$ pour $n \geqslant m$; par suite, pour $n \geqslant m$, pour tout $(x,y) \in H_n$, il existe un élément de H_m de la forme (x,z), et par suite $(x,y) = (x,z) + (0,y-z)$, autrement dit, on peut écrire $H_n = H_m + L_n$, où L_n est l'intersection de H_n et du module

composant $F'=\{0\}\times F$ de $E\times F$, isomorphe à F. Comme la suite (L_n) est croissante dans F', il existe un entier p tel que pour $n\geqslant p$ on ait $L_n=L_p$, d'où, pour $n\geqslant \mathrm{Max}(m,p)$, $H_n=H_m+L_p$.

COROLLAIRE 1.- Si $(M_i)_{1\leqslant i\leqslant n}$ est une suite finie de sous-modules noethériens d'un module E, la somme des M_i est un sous-module noethérien.

En effet, $M=\sum_{i=1}^{n} M_i$ est isomorphe à un module quotient de la somme directe des M_i, elle-même isomorphe à leur produit (chap.II, § 1,).

COROLLAIRE 2.- Tout module à gauche unitaire de type fini sur un anneau noethérien à gauche A est un module noethérien.

En effet, un tel module est isomorphe à un module quotient d'un module produit A_s^n.

2. Modules réguliers de type fini sur un anneau principal.

Nous allons étudier dans ce paragraphe les modules unitaires de type fini sur un anneau principal A ; un tel anneau étant évidemment noethérien, tout module de type fini sur A est noethérien (cor. 2 de la prop.3).

Nous utiliserons dans cette étude la définition générale suivante

DEFINITION 3.- On dit qu'un A-module à gauche unitair E est régulier si tout élément $\neq 0$ de E est libre (chap.II, § 1, n°).

Autrement dit, E est régulier si la relation $ax=0$ ($a\in A$, $x\in E$) est équivalente à "$x=0$ ou $a=0$".

Nous étudierons d'abord les modules réguliers et de type fini sur un anneau principal A. Si E est un tel module, on sait (chap.III, § 2) qu'on peut considérer E comme sous-module (par rapport à A) d'un espace vectoriel $\tilde{E}$ sur le corps des fractions K de A, dit associé à E, et bien déterminé à une isomorphie près. Quand on identifie ainsi canoniquement E à un sous-module de $\tilde{E}$, on sait qu'on a $\tilde{E}=KE$

(ensemble des λx , ou' λ parcourt K et x parcourt E) ; par suite, tout système de générateurs du A-module E est aussi un système de générateurs de l'espace vectoriel KE ; comme par hypothèse, E est de type fini, KE est de dimension finie ; cette dimension n , qui ne dépend donc que du A-module E , sera appelée le rang de E (c'est le rang de E au sens du chap.II, § 3, lorsque E est considéré comme partie de l'espace vectoriel KE) .

THÉORÈME 1.- Tout module régulier E de type fini et de rang n sur un anneau principal A est isomorphe à A^n (autrement dit, admet une base de n éléments).

La proposition étant évidente pour n=0 (cas ou' E est réduit à 0) nous raisonnerons par récurrence sur n . Soit x un élément $\neq 0$ de KE ; nous appellerons transporteur de x dans E l'ensemble $\mathfrak{a}$ des éléments $\lambda \in K$ tels que $\lambda x \in E$.

Lemme 1.- Le transporteur $\mathfrak{a}$ dans E d'un élément $x \neq 0$ de KE est un idéal fractionnaire (principal) dans K .

En effet, $\mathfrak{a}$ est évidemment un A-module, et comme l'application $\lambda \to \lambda x$ de K dans KE est biunivoque, $\mathfrak{a}$ est isomorphe au sous-module $\mathfrak{a} x$ de E , donc est de type fini ; soient (a_i) $(1 \leqslant i \leqslant p)$ un système de générateurs de $\mathfrak{a}$; il existe $\beta \in A$ tel que $\beta \neq 0$ et $\beta a_i \in A$ pour $1 \leqslant i \leqslant p$, donc $\beta \mathfrak{a}$ est un idéal de A , et par suite un idéal principal ; on a donc bien $\mathfrak{a} = (\gamma)$, ou' $\gamma \in K$. On en déduit que si on pose $y = \gamma x$, on a $y \in E$, et $\mathfrak{a} x = A.y$.

Ce lemme étant démontré, nous démontrerons le th.1 par récurrence sur n , le théorème étant évident pour n=0 (puisqualors E est réduit à 0). Soit $x \neq 0$ un élément de E , $\mathfrak{a} = (\gamma)$ le transporteur de x dans E ; le sous-module $M = \mathfrak{a} x$ de E admet une base formée du seul élément γx .

Considérons alors le A-module E/M ; il est de type fini et <u>régulier</u> ; en effet, si $z \in E$ et $\lambda \in A$ sont tels que $\lambda z \in M$, on a $\lambda z = \rho\gamma x$, où $\rho \in A$, d'où $z = \mu x$ avec $\mu \in K$, et comme $z \in E$, on a nécessairement $z \in M$ par définition de M. Dans l'espace vectoriel KE, on a $M = E \cap Kx$, donc $E/M = E/(E \cap Kx)$ est isomorphe au module quotient $(E+Kx)/Kx$ (chap.I, § 6, th.6) ; ce dernier est un sous-module de l'espace vectoriel KE/Kx, qui est de dimension n-1 ; donc E/M est de rang $\leqslant$ n-1, et comme $K((E+Kx)/Kx) = KE/Kx$, E/M est exactement de rang n-1 ; d'après l'hypothèse de récurrence il existe donc dans E/M une base de n-1 éléments, et par suite (chap.II, § 1, prop.4) M admet un supplémentaire dans E, qui a une base de n-1 éléments ; ce qui démontre le théorème.

COROLLAIRE 1.- <u>Pour que deux modules réguliers de type fini sur un anneau principal soient isomorphes, il faut et il suffit qu'ils aient même rang</u>.

COROLLAIRE 2.- <u>Soit E un module de type fini sur un anneau principal A ; si M est un sous-module de E tel que E/M soit régulier, M admet un supplémentaire dans E</u>.

En effet, E/M admet une base d'après le th.1, et le corollaire résulte donc de la prop.4 du chap.II, § 1.

Si E est régulier on notera que pour que E/M soit régulier, il faut et il suffit que, dans KE, on ait $M = E \cap (KM)$, car dire que E/M est régulier signifie que, si $z \in E$ est tel qu'il existe $\lambda \neq 0$ dans A tel que $\lambda z \in M$, on a $z \in M$; mais dire qu'il existe $\lambda \neq 0$ dans A tel que $\lambda z \in M$ signifie que $z \in KM$. En particulier, si $x \in E$, pour que E/Ax soit régulier, il faut et il suffit que le <u>transporteur</u> de x dans E soit égal à (1).

Remarque.- On notera qu'un A-module peut être régulier et de rang fini sans être de type fini : par exemple, si A n'est pas un corps, son corps des fractions K est un A-module régulier et de rang 1, mais ne peut admettre de base, car une telle base serait réduite à un élément α , et on aurait $K=A.\alpha$, d'où $A=K\alpha^{-1}=K$ contrairement à l'hypothèse.

3. Modules indécomposables de type fini sur un anneau principal.

Un module de type fini sur un anneau principal A n'est pas nécessairement régulier, comme le montre aussitôt l'exemple d'un module quotient A/(a) de A (considéré comme A-module à gauche) par un quelconque de ses idéaux (a) distinct de (0) et de A : un tel module a en effet pour annulateur l'idéal (a).

Nous allons voir que tout module de type fini sur A est isomorphe à la somme directe d'un module régulier et d'un nombre fini de modules de la forme A/(a). Pour démontrer ce résultat, nous établirons d'abord un certain nombre de propriétés de ces derniers modules.

PROPOSITION 4.- Dans l'anneau principal A , si $(a)=(p_1^{\nu_1})\ldots(p_n^{\nu_n})$ (p_i éléments premiers de A , distincts deux à deux), le module quotient A/(a) est isomorphe à la somme directe des n modules $A/(p_i^{\nu_i})$.

Comme $p_1^{\nu_1}$ et $p_2^{\nu_2}p_3^{\nu_3}\ldots p_n^{\nu_n}$ sont premiers entre eux, tout revient, par récurrence sur n , à montrer que si b et c sont premiers entre eux dans A , A/(bc) est isomorphe à la somme directe de A/(b) et A/(c). Or, on a par hypothèse (b)+(c)=A , et d'autre part bc est p.p.c.m. de b et c , donc (bc)=(b) $\cap$ (c) ; par suite A/(bc) est identique à ((b)+(c))/((b)$\cap$(c))=(b)/((b)$\cap$(c))+(c)/((b)$\cap$(c)), et comme l'intersection des sous-modules (b)/((b)$\cap$(c)) et (c)/((b)$\cap$(c)) est ((b)$\cap$(c))/((b)$\cap$(c))=(0) , leur somme est directe ;mais (b)/((b)$\cap$(c)) est isomorphe à ((b)+(c))/(c)=A/(c) (chap.I, §6,th.6) et on voit de même

que $(c)/((b)\cap(c))$ est isomorphe à $A/(b)$.

PROPOSITION 5.- Si a et b sont deux éléments quelconques $\neq 0$ de A, le sous-module $(a)/(ab)$ de $A/(ab)$ est isomorphe à $A/(b)$.

En effet, soit φ l'homomorphisme canonique de A sur $A/(ab)$; l'application $\lambda \longrightarrow \varphi(\lambda a)$ de A dans $A/(ab)$ est une représentation et l'image de A par cette représentation est l'image de (a) par φ, c'est-à-dire $(a)/(ab)$; d'autre part, pour que $\varphi(\lambda a)=0$ il faut et il suffit qu'il existe $\mu \in A$ tel que $\lambda a=\mu ab$, c'est-à-dire $\lambda=\mu b$, d'où la proposition.

La prop.4 nous montre que, dans certains cas, un module quotient $A/(a)$ peut se décomposer en somme directe de sous-modules $\neq(0)$; nous dirons que $A/(a)$ est indécomposable s'il n'est pas somme directe de sous-modules non réduits à 0.

PROPOSITION 6.- Pour qu'un module quotient $A/(a)$ soit indécomposable, il faut et il suffit que $(a)=(p^k)$, où p est un élément premier de A.

La condition est nécessaire, car si (a) n'est pas une puissance d'un idéal premier, la prop.4 montre que $A/(a)$ n'est pas indécomposable. Pour voir que la condition est suffisante, remarquons que tout sous-module de $A/(p^k)$ est de la forme $\mathfrak{a}/(p^k)$, où $\mathfrak{a}$ est un idéal de A tel que $(p^k)\subset \mathfrak{a}$; mais les seuls idéaux de A qui contiennent (p^k) sont les idéaux (p^h) où $0<h<k$ si $\mathfrak{a}\neq A$ et $\mathfrak{a}\neq(p^k)$; donc (prop.5), $\mathfrak{a}/(p^k)$ est isomorphe à $A/(p^{k-h})$, et admet donc (p^{k-h}) pour annulateur. Il s'ensuit que si $A/(p^k)$ était somme directe de deux de ces sous-modules, il aurait pour annulateur une puissance (p^r) avec $r<k$, ce qui est absurde.

PROPOSITION 7.- Soient G et G' deux modules sur un anneau principal A, tel que G (resp. G') soit somme directe d'un nombre fini sous-modules indécomposables G_i (resp. G'_j) (isomorphes à des modules quotients de A). Si G et G' sont isomorphes, il existe une application biunivoque φ de l'ensemble des indices i sur l'ensemble des indices j tels que $G'_{\varphi(i)}$ soit isomorphe à G_i pour tout i .

On peut évidemment se borner au cas où G'=G . Remarquons en premier lieu qu'un module indécomposable $A/(I^k)$ est entièrement déterminé à une isomorphie près par son annulateur (p^k). Pour démontrer la proposition, nous allons établir que pour tout élément premier $p \in A$, le nombre des groupes G_i qui admettent comme annulateur une puissance donnée (p^k) de p ne dépend que de G , et non de la décomposition (G_i) considérée.

Nous utiliserons le lemme suivant :

Lemme 2.- Si a et b sont deux éléments $\neq 0$ de A , d un p.g.c.d. de a et de b , le module $b(A/(a))$ est isomorphe à $(d)/(a)$.

En effet, si γ est l'homomorphisme canonique de A sur $A/(a)$, on a $\gamma(bx)=b\gamma(x)$ pour tout $x \in A$, donc $b(A/(a))$ est identique à $\gamma((b))$, et par suite (chap.I, §6,th.6) isomorphe à $((a)+(b))/(a) = (d)/(a)$.

On déduit de ce lemme et de la prop.5 que si p et q sont deux éléments premiers de A tels que $(p)\neq(q)$, $p^r(A/(q^s))$ est isomorphe à $A/(q^s)$, $p^r(A/(p^s))$ est isomorphe à $A/(p^{s-r})$ si $r < s$, et à (0) si $r \geqslant s$.

Considérons alors le module quotient $(p^{r-1}G)/(p^rG)$; comme p^rG (resp. $p^{r-1}G$) est isomorphe à la somme directe des p^rG_i (resp. $p^{r-1}G_i$). Par suite (chap.I, §6,prop.5), $(p^{r-1}G)/(p^rG)$ est isomorphe à la somme directe des $(p^{r-1}G_i)/(p^rG_i)$; mais ce dernier module, d'après ce qui précède, est isomorphe à (0) si p^r divise l'annulateur de G_i , à $A/(p)$

dans le cas contraire. Par suite, si $n(p^r)$ est le nombre des modules indécomposables G_i dont p^r divise l'annulateur, $(p^{r-1}G)/(p^rG)$ est isomorphe à la somme directe de $n(p^r)$ modules isomorphes à $A/(p)$; mais comme (p) est un idéal maximal, $A/(p)$ est un A-module simple, donc (chap.I, §6, prop.13), le nombre $n(p^r)$ ne dépend que de G (et de p^r), et non de la décomposition (G_i) considérée. Or, le nombre des G_i dont les annulateurs sont égaux à (p^k) est évidemment égal à $m(p^k)=n(p^k)-n(p^{k+1})$; il est donc lui aussi indépendant de (G_i), ce qui achève la démonstration.

Les idéaux (p^k) (ou les éléments p^k) tels que $m(p^k)\neq 0$) sont encore appelés les diviseurs élémentaires du module G , $m(p^k)$ étant appelé la multiplicité du diviseur élémentaire (p^k) dans G ; la prop.7 montre qu'un module G somme directe de modules indécomposables est entièrement déterminé à une isomorphie près par la donnée de ses diviseurs élémentaires et de la multiplicité de chacun d'eux (ces données étant d'ailleurs arbitraires). On dira pour abréger que deux tels modules G , G' ont même diviseurs élémentaires si, pour chaque idéal premier (p) de A et chaque entier $k > 0$, la multiplicité $m(p^k)$ est la même pour G et G' .

4. Facteurs invariants.

Tout module de type fini sur un anneau principal A est isomorphe à un module quotient A^n/M , où M est un sous-module de A^n ; A^n et M sont deux modules réguliers de type fini sur A ; nous sommes donc amenés à étudier la structure du quotient d'un module régulier de type fini par un de ses sous-modules.

Plus généralement, nous allons démontrer le théorème suivant :

THEOREME 2.- Soient M et N deux modules réguliers de type fini et de même rang n sur un anneau principal A , contenus dans un même espace vectoriel ~~xx~~ E=KM=KN (K corps des quotients de A). Il existe une base $(u_i)_{1 \leqslant i \leqslant n}$ de M et une base $(v_i)_{1 \leqslant i \leqslant n}$ de N telle que l'on ait $v_i = e_i u_i$ $(1 \leqslant i \leqslant n)$, où les e_i appartiennent à K et sont tels que e_i divise e_{i+1} pour $1 \leqslant i \leqslant n-1$; en outre, les idéaux fractionnaires (e_i) $(1 \leqslant i \leqslant n)$ sont déterminés de façon unique.

La dernière partie de l'énoncé signifie qu'il peut exister une autre base (u'_i) de M et une autre base (v'_i) de N telle que $v'_i = e'_i u'_i$ pour $1 \leqslant i \leqslant n$ et $(e'_i) \supset (e'_{i+1})$ pour $1 \leqslant i \leqslant n-1$, mais qu'alors $(e'_i) = (e_i)$ pour tout i .

L'ensemble des $\lambda \in K$ tels que $\lambda M \subset N$ est évidemment un A-module contenu dans K ; comme c'est l'intersection des transporteurs dans N des éléments d'une base (ou d'un système de générateurs) de M , c'est l'intersection d'un nombre fini d'idéaux fractionnaires, et par suite un idéal fractionnaire (a), que nous appellerons encore le transporteur de M dans N ; nous désignerons de même par (b) le transporteur de N dans M . On a évidemment $abM \subset bN \subset M$; cette relation donne en particulier abx M pour tout élément x d'une base de M , et montre donc que ab est un entier ; nous désignerons par p_i $(1 \leqslant i \leqslant m)$ ses facteurs premiers distincts.

Cela étant, (b) est par définition contenu dans le transporteur dans M de tout élément de N ; nous allons démontrer le lemme suivant :

Lemme 3.- Il existe un élément $x \in N$ dont le transporteur dans N est égal à (1) et dont le transporteur dans M est égal à (b) .

En effet, soit x un élément de N dont le transporteur dans N soit égal à (1) ; soit (d) son transporteur dans M ; comme $(d) \supset (b)$, on a $b=dh$, où h est entier. Le transporteur de dx M dans N est $(d^{-1})=(hb^{-1})$; par définition $(d^{-1}) \supset (a)$, donc d^{-1} divise a , et par suite h divise ab ; comme h et ab sont entiers, h est divisible par un au moins des p_i si $(h) \neq (1)$; alors b est divisible par dp_i , soit $b=cdp_i$, où c est entier ; on en déduit $x=(cp_ib^{-1})dx$, et comme $dx \in M$, $x \in p_ib^{-1}M$. Si donc nous déterminons x de sorte que $x \notin p_ib^{-1}M$ pour $1 \leqslant i \leqslant m$, on aura nécessairement $(h)=(1)$ et x satisfera aux conditions du lemme.

OR, d'après la définition de b , N n'est pas contenu dans $p_ib^{-1}M$. Soit x_i $(1 \leqslant i \leqslant m)$ un élément de N n'appartenant pas à $p_ib^{-1}M$. Déterminons d'autre part un élément $\lambda_i \in A$ tel que $\lambda_i \equiv 0 \pmod{p_j}$ pour $j \neq i$ et $\lambda_i \equiv 1 \pmod{p_i}$ (§3, prop.11) ; si on pose $y = \sum_{i=1}^{m} \lambda_i x_i$ chacun des termes de cette somme sauf $\lambda_i x_i$ appartient à $p_iN \subset p_ib^{-1}M$, et $\lambda_i x_i$ n'appartient pas à $p_ib^{-1}M$. Comme $y \in N$, le transporteur de y dans N est de la forme (r^{-1}) , où r est entier ; on a donc $x=r^{-1}y \in N$, le transporteur de x dans N est (1), et comme $y=rx$ n'appartient à aucun des $p_ib^{-1}M$, il en est de même de x a fortiori

Ce lemme étant établi, démontrons le théorème par récurrence sur n (le théorème est trivial pour n=0). Avec les mêmes notations que ci-dessus, soit x un élément satisfaisant aux conditions du lemme 3 ; posons $M_1=A.bx$, $N_1=A.x$; le transporteur de bx dans M étant (1) , M/M_1 est régulier, donc M_1 admet un supplémentaire M_1' de rang n-1 dans M ; $E=KM$ est somme directe de $KM_1=Kx$ et de KM_1' ; montrons que N est somme directe de N_1 et de $N_1'=N \cap KM_1'$. En effet, tout $z \in N$ peut s'écrire d'une seule manière sous la forme $z=\lambda x+y$, où $\lambda \in K$ et $y \in KM_1'$; d'après la définition de b , on a $bz \in M$, donc $b\lambda x \in M \cap Kx = M_1$, et par suite $\lambda x \in b^{-1}M_1 = N_1$, et $y \in N_1'$.

Cela étant, M'_1 et N'_1 sont des modules réguliers de type fini et de rang n-1, tels que $KM'_1 = KN'_1$; l'hypothèse de récurrence montre qu'il existe une base (u_i) $(2 \leqslant i \leqslant n)$ de M'_1 et une base (v_i) $(2 \leqslant i \leqslant n)$ de N'_1 telles que $v_i = e_i u_i$ $(2 \leqslant i \leqslant n)$, où e_i divise e_{i+1} pour $2 \leqslant i \leqslant n-1$; (e_2^{-1}) étant le transporteur de v_2 dans M, divise b^{-1} ; si on pose $u_1 = bx$, $v_1 = x$, $e_1 = b^{-1}$, on a $v_1 = e_1 u_1$, e_2 divise e_1, et l'existence des bases (u_i) et (v_i) est ainsi démontrée.

Reste à voir que les idéaux fractionnaires (e_i) sont déterminés de façon unique par les conditions du théorème. Il est clair tout d'abord que ces conditions entraînent que (e_1^{-1}) est le transporteur de N dans M. Posons en outre $e_i = c_i e_1$ pour $1 \leqslant i \leqslant n$; les c_i sont des entiers ; le module $N' = e_1^{-1} M$ est un sous-module de M, dont une base est formée des $e_1^{-1} v_i = c_i u_i$. Il en résulte que le module quotient M/N' est isomorphe à la somme directe des n-1 sous-modules $A/(c_i)$ $(2 \leqslant i \leqslant n)$, et par suite (prop 4) somme directe de modules indécomposables de la forme $A/(p^k)$, où p est premier. Chacun des (c_i) est donc produit d'un certain nombre de diviseurs élémentaires de M/N' (étant entendu que pour chaque élément premier p divisant c_i, le diviseur élémentaire correspondant est la plus haute puissance de p divisant c_i). Comme c_i divise c_{i+1}, on voit donc que pour tout élément premier p, la puissance de p qui figure dans la décomposition de c_i en facteurs premiers a pour exposant le plus petit entier k tel que $n-i+1 \leqslant \sum_{r=k}^{\infty} m(p^r)$ (ou à 0 s'il n'existe aucun entier ayant cette propriété), $m(p^r)$ désignant la multiplicité du diviseur élémentaire (p^r) dans M/N'. Les (c_i), et par suite aussi les (e_i) sont donc bien déterminés, ce qui achève la démonstration du th.2.

Les idéaux (e_i) (ou les éléments e_i, déterminés à des facteurs près diviseurs de 1) sont appelés les facteurs invariants de N par rapport à M.

Delsarte 60

Remarques.- 1) On peut facilement donner des exemples où il y a plusieurs bases (u_i) de M pour lesquelles il existe une base (v_i) de N satisfaisant aux conditions du th.2 .

2) Il est clair que si on pose $e'_i = e^{-1}_{n-i+1}$ $(1 \leqslant i \leqslant n)$, les e'_i sont les facteurs invariants de M par rapport à N ; en particulier, l'idéal (e_n) est le transporteur de M dans N .

Pour que N soit un sous-module de M , il faut et il suffit que e_1 (et par suite tous les e_i) soient entiers, puisqu'on doit avoir $v_1 = e_1 u_1 \in M$.

PROPOSITION 8.- Soit A un anneau principal, M un sous-module quelconque de A^n de rang $m \leqslant n$; il existe une base (u_i) $(1 \leqslant i \leqslant n)$ de A^n , et une base (v_i) $(1 \leqslant i \leqslant n)$ de M telles que $v_i = e_i u_i$ pour $1 \leqslant i \leqslant m$, les e_i étant des entiers $\neq 0$ tels que e_i divise e_{i+1} pour $1 \leqslant i \leqslant m-1$.

En effet, soit $P = A^n \cap KM$; P est un sous-module de rang m de A^n et il résulte de sa définition qu'on a $P = A^n \cap KP$, donc A^n/P est un module régulier, et par suite (cor.2 du th.1), P admet dans A^n un supplémentaire de rang n-m , isomorphe à A^{n-m}. D'autre part, M est un sous-module de P tel que $KM = KP$; en appliquant à M et P le th.2, on obtient la proposition.

Lorsqu'aucune confusion n'est possible, on dit que les e_i (déterminés à des facteurs près diviseurs de 1) sont les facteurs invariants du sous-module M de A^n .

COROLLAIRE.- Soient M et N deux sous-modules de A^n ; pour qu'il existe un automorphisme u de A^n tel que $u(M) = N$, il faut et il suffit que M et N aient mêmes facteurs invariants.

La condition est évidemment nécessaire ; elle est suffisante, car si $(a_i)_{1 \leqslant i \leqslant n}$ et $(b_i)_{1 \leqslant i \leqslant n}$ sont deux bases de A^n telles que

$(e_i a_i)_{1 \leqslant i \leqslant m}$ forme une base de M et $(e_i b_i)_{1 \leqslant i \leqslant m}$ une base de N , il suffit de définir u par les conditions $u(a_i)=b_i$ pour obtenir un automorphisme de A^n (chap.II, § 2, prop.) tel que $u(M)=N$.

Tout module quelconque de type fini sur A étant isomorphe à un module quotient A^n/M , les prop.8 et 4 donnent aussitôt la première partie du théorème suivant :

THEOREME 3.- Pour tout module E de type fini sur un anneau principal il existe un sous-module régulier H de E et une suite finie (G_i) de sous-modules indécomposables de E (isomorphes à des modules quotients de A) tels que E soit somme directe de H et des G_i . En outre, si H' est un second sous-module régulier de E , (G'_j) une seconde suite finie de sous-modules indécomposables de E tels que E soit somme directe de H' et des G'_j , H est isomorphe à H' , on a $\sum_i G_i = \sum_j G'_j$, et il existe une application biunivoque φ de l'ensemble des indices i sur l'ensemble des indices j telle que $G'_{\varphi(i)}$ soit isomorphe à G_i pour tout i .

La seconde partie du théorème résultera aussitôt de la prop.7 si on démontre que $\sum_i G_i = \sum_j G'_j$; pour cela nous allons voir que $S = \sum_i G_i$ est identique à l'ensemble des éléments liés du A-module E . En effet, si α est un p.p.c.m. des annulateurs des G_i , on a $\alpha x=0$ pour tout $x \in S$; réciproquement, si $\alpha \in A$ et $x \in E$ sont tels que $\alpha x=0$, on peut écrire $x=y+z$, où $y \in H$ et $z \in S$, donc $0=\alpha y+\alpha z$, et par suite $\alpha y=0$ et $\alpha z=0$; si $y \neq 0$ (c'est-à-dire $x \notin S$), on a $\alpha=0$ puisque H est régulier, donc si x est lié, on a $x \in S$.

On dit que les modules H et G_i (déterminés à un automorphisme près de E) forment une décomposition canonique de E . Les diviseurs élémentaires du module $S = \sum_i G_i$ sont encore appelés les diviseurs élémentaires du module E .

COROLLAIRE.- Pour que deux modules de type fini E,E' sur un anneau principal A , soient isomorphes, il faut et il suffit qu'ils aient mêmes diviseurs élémentaires, et que si S (resp. S') est le sous-module de E (resp. E') formé des éléments liés les modules réguliers E/S et E'/S' aient même rang.

5. Calcul des facteurs invariants.

Soit M un sous-module de rang m de A^n , $(e_i)_{1 \leqslant i \leqslant m}$ les facteurs invariants de M (e_i divisant e_{i+1} pour $1 \leqslant i \leqslant m-1$) ; nous allons donner une autre interprétation de ces éléments. Soit $(a_i)_{1 \leqslant i \leqslant n}$ une base de A^n , telle que les $b_i = e_i a_i$ $(1 \leqslant i \leqslant m)$ forment une base de M (prop.8) . Les n coordonnées (par rapport à la base canonique de A^n) d'un élément $x \in M$ sont évidemment multiples de e_1 . D'autre part, les n coordonnées de a_1 (par rapport à la base canonique) sont premières entre elles, car si elles admettaient un diviseur δ (non diviseur de 1), l'élément a_1/δ appartiendrait à A^n , contrairement au fait que (a_i) est une base de A^n . On en déduit que e_1 est un p.g.c.d. des n coordonnées de $e_1 a_1 = b_1$; par suite, e_1 est un p.g.c.d. de l'ensemble des coordonnées d'un système de générateurs de M .

Pour avoir une interprétation analogue des autres facteurs invariants de M , considérons le module $\bigwedge^p M$, puissance extérieure p-ème de M (chap.III, § 5, n°) ; comme M admet une base $(b_i)_{1 \leqslant i \leqslant m}$, $\bigwedge^p M$ admet, pour $p \leqslant m$, une base formée des éléments $b_{i_1} \wedge b_{i_2} \wedge \dots \wedge b_{i_p}$, pour toutes les suites croissantes de p indices $i_1, \dots, i_p$ de $[1,m]$; comme $\bigwedge^p A^n$ admet pour base des p-vecteurs $a_{j_1} \wedge a_{j_2} \wedge \dots \wedge a_{j_p}$ où (j_k) parcourt les suites croissantes de p indices appartenant à $[1,n]$, l'application canonique de $\bigwedge^p M$ dans $\bigwedge^p A^n$ est un isomorphisme de $\bigwedge^p M$ sur le sous-module de $\bigwedge^p A^n$ ayant pour base les éléments

$(e_{i_1}e_{i_2}\dots e_{i_p})a_{i_1}\wedge a_{i_2}\wedge\dots\wedge a_{i_p}$ $(1\leqslant i_1<i_2<\dots<i_p\leqslant m)$ sous-module qu'on identifie donc à $\bigwedge^p M$; le même raisonnement que ci-dessus montre alors que le produit $d_p=e_1e_2\dots e_p$ est un p.g.c.d. de l'ensemble des coordonnées (par rapport à la base canonique de $\bigwedge^p A^n$) d'un système de générateurs de $\bigwedge^p M$. Si on tient compte de l'expression de ces coordonnées au moyen de déterminants (chap.III, §6, n°), on obtient le résultat suivant :

PROPOSITION 9.- Soit A un anneau principal, M un sous-module de rang m de A^n, e_i $(1\leqslant i\leqslant m)$ ses facteurs invariants ; pour $1\leqslant p\leqslant m$ le produit $d_p=e_1\dots e_p$ est un p.g.c.d. de l'ensemble des mineurs d'ordre p de toute matrice dont les colonnes forment un système de générateurs de M.

Le produit d_p $(1\leqslant p\leqslant m)$ défini à un facteur près diviseur de 1, est appelé diviseur déterminantiel d'ordre p du module M.

COROLLAIRE.- Soit M' un sous-module de M, de rang $m'\leqslant m$; soient a_i $(1\leqslant i\leqslant m')$ les facteurs invariants de M' par rapport à M ; si d'_p $(1\leqslant p\leqslant m')$ est le diviseur déterminantiel d'ordre p de M', d'_p est multiple de $d_pa_1a_2\dots a_p$. En particulier, si $m'=m$ et si d'_m et d_m sont associés, on a $M'=M$.

En effet, d'après la prop.8, il existe une base $(b_i)_{1\leqslant i\leqslant m}$ de M et une base $(b'_i)_{1\leqslant i\leqslant m'}$ de M' telles que $b'_i=a_ib_i$ pour $1\leqslant i\leqslant m'$; la prop.9 montre alors que d'_p est multiple de $d_pa_1\dots a_p$. Si $m'=m$ et si d'_m et d_m sont associés, $a_1a_2\dots a_m$ est un diviseur de 1, donc il en est même de chacun des a_i, ce qui entraîne $M'=M$.

6. Structure des groupes abéliens de type fini.

Nous dirons qu'un groupe abélien G est de type fini s'il est engendré par un nombre fini d'éléments. Si on note G additivement, G est un $\mathbb{Z}$-module de type fini ; comme $\mathbb{Z}$ est un anneau principal,

le th.3 détermine complètement la structure de G :

PROPOSITION 10.- Tout groupe abélien G de type fini est produit direct d'un nombre fini de groupes monogènes d'ordre infini (isomorphes à Z), et d'un nombre fini de groupes monogènes d'ordres égaux à des puissances de nombres premiers. Le nombre des facteurs et leurs ordres sont les mêmes dans deux décompositions de G en produit direct de cette nature (dites décompositions canoniques de G).

Un groupe abélien de type fini est donc caractérisé, à une isomorphie près, par la donnée des groupes monogènes qui figurent dans une de ses décompositions canoniques ; on peut encore dire qu'un tel groupe est isomorphe à un groupe de la forme $\prod_{h=1}^{m} Z/(a_h)$ où a_h est égal à 0 ou à une puissance d'un nombre premier ; la donnée de la suite finie $(a_h)_{1 \leqslant h \leqslant m}$ détermine le groupe à une isomorphie près, et réciproquement deux groupes abéliens de type fini ne sont isomorphes que si les suites (a_h) qui leur correspondent ne diffèrent que par l'ordre des termes ; on dit qu'un groupe isomorphe à $\prod_{h=1}^{m} Z/(a_h)$ est de type $(a_h)_{1 \leqslant h \leqslant m}$. Par exemple, un groupe de type $(0, 0, 2, 4, 3)$ est isomorphe au produit de deux groupes isomorphes à Z, et de trois groupes cycliques d'ordres repsectifs 2, 4 et 3 .

§ 5. Applications de la théorie des diviseurs élémentaires.

1. Forme canonique d'une matrice sur un anneau principal.

Soit A un anneau principal ; étant donnée une application linéaire u de A^n dans A^m, on appelle facteurs invariants de u les facteurs invariants du sous-module $u(A^n)$ par rapport à A^m (§ 4, n°4) ; si φ est un automorphisme de A^n, ψ un automorphisme de A^m, il est clair que $\psi \circ u \circ \varphi$ a même facteurs invariants que u .

Une matrice X à m lignes et n colonnes, à éléments dans l'anneau A, est la matrice d'une application linéaire u de A^n dans A^m, par rapport aux bases canoniques de ces deux modules (chap.II, § 6, n°3) ; on appelle encore <u>facteurs invariants</u> de la matrice X ceux de l'application linéaire u. Si e_i $(1 \leqslant i \leqslant p)$ sont les facteurs invariants de X, la prop.9 du § 4 montre que $d_k = e_1 e_2 .. e_k$ est un p.g.c.d. des <u>mineurs d'ordre</u> k <u>de</u> X, ce qui permet de déterminer les e_i à des facteurs inversible près.

PROPOSITION 1.- <u>Pour que deux matrices à</u> m <u>lignes et</u> n <u>colonnes sur un anneau principal</u> A <u>soient équivalentes</u> (chap.II, § 6, n°10), <u>il faut et il suffit qu'elles aient mêmes facteurs invariants</u>.

La condition est évidemment <u>nécessaire</u>, d'après la définition de facteurs invariants d'une matrice. Pour voir qu'elle est <u>suffisante</u>, nous montrerons que toute matrice X sur A, à m lignes et n colonnes, ayant des facteurs invariants donnés e_i $(1 \leqslant i \leqslant p)$ est équivalente à la matrice

$$U = \begin{pmatrix} e_1 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & e_2 & \dots & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & e_p & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \end{pmatrix}$$

qui est dite <u>matrice canonique</u> à m lignes et n colonnes, ayant les facteurs invariants e_i $(1 \leqslant i \leqslant p)$.

Pour cela, nous allons voir qu'il existe deux bases $(a_i)_{1 \leqslant i \leqslant n}$ et $(b_j)_{1 \leqslant j \leqslant m}$ de A^n et A^m respectivement, telles que U soit la matrice de l'application linéaire u par rapport à ces bases. Nous prendrons

$(b_j)_{1 \leqslant j \leqslant m}$ de sorte que les $e_j b_j$ $(1 \leqslant j \leqslant p)$ forment une base de $u(A^n)$ (§ 4, prop.8). Comme $A^n / {}^{-1}u(0)$ est isomorphe à $u(A^n)$, donc régulier, A^n est somme directe de ${}^{-1}u(0)$ et d'un sous-module M (§ 4, cor.2 du th.1), et u est un isomorphisme de M sur $u(A^n)=u(M)$. Les éléments a_i $(1 \leqslant i \leqslant p)$ de M tels que $u(a_i)=e_i b_i$ forment donc une base de M ; en désignant par a_i, pour $p+1 \leqslant i \leqslant n$, n-p éléments formant une base de ${}^{-1}u(0)$ (§ 4, th.1), il est clair que U est la matrice de u, par rapport aux bases (a_i) et (b_j).

2. Réduction d'une matrice carrée sur un corps commutatif.

Soit E un espace vectoriel de dimension n sur un corps commutatif K. Si un endomorphisme u de E tel que, par rapport à une base $(a_i)_{1 \leqslant i \leqslant n}$ de E, sa matrice soit une matrice diagonale, E est somme directe des n sous-espaces Ka_i, dont chacun est tel que $u(Ka_i) \subset Ka_i$; réciproquement, si E est somme directe de n sous-espaces de cette nature de la matrice de u par rapport à la base (a_i) est diagonale.

Nous allons chercher si, pour un endomorphisme quelconque u de E, il n'existe pas une propriété analogue ; de façon précise, peut-on décomposer E en somme directe de sous-espaces M_k $(1 \leqslant k \leqslant r)$ tels que $u(M_k) \subset M_k$ pour tout k, et dont les dimensions soient les plus petites possibles ?

Soit A la matrice de u par rapport à une base quelconque de E ; le problème précédent est équivalent au suivant : existe-t-il une matrice $A' = PAP^{-1}$ semblable à A (P matrice inversible d'ordre n sur K) qui se mette sous la forme d'un "tableau diagonal de matrices"

$$(1) \qquad A' = \begin{pmatrix} A'_1 & 0 & 0 & \dots & 0 \\ 0 & A'_2 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & A'_r \end{pmatrix}$$

dans lequel l'ordre des sous-matrices A'_k $(1 \leqslant k \leqslant r)$ soit le plus petit possible ?

Nous allons ramener ce problème à l'étude d'un module de type fini sur un anneau principal. Nous poserons $u^k = u^{k-1} \circ u = u \circ u^{k-1}$ pour tout entier $k > 0$ (puissance k-ème dans l'anneau $\mathscr{L}(E)$) ; par abus de langage, nous dirons qu'un sous-espace vectoriel G de E est <u>invariant</u> par u si $u(G) \subset G$.

Il est clair que l'ensemble des endomorphismes $v \in \mathscr{L}(E)$ tels que G soit invariant par v est un <u>sous-anneau</u> de $\mathscr{L}(E)$ contenant l'élément unité ; en particulier, si G est invariant par un endomorphisme u , il est aussi invariant par le sous-anneau J de $\mathscr{L}(E)$ <u>engendré</u> par u et l'élément unité de $\mathscr{L}(E)$ (qu'on peut noter u^0) ; comme K est commutatif J est identique à l'ensemble des endomorphismes f(u) , où f parcourt l'anneau $K[X]$ des polynomes à une indéterminée sur K (chap. IV, § 2, prop.1).

Définissons alors sur E une loi de composition externe ayant $K[X]$ comme ensemble d'opérateurs, en posant, pour tout polynome $f = \sum_{k=0}^{m} a_k X^k$ de $K[X]$ et tout élément $x \in E$, $f.x = \sum_{k=0}^{m} a_k u^k(x)$; on vérifie aussitôt que cette loi et l'addition dans E définissent sur E une structure de $K[X]$-<u>module</u>, telle que par restriction à K de la loi externe de ce module, on obtienne sur E la structure d'espace vectoriel donnée initialement. Nous désignerons par E_u le $K[X]$-module ainsi défini ; il est clair alors que si G est un sous-espace vectoriel de E invariant par u , G est un <u>sous-module</u> de E_u , et réciproquement.

Nous sommes donc ramenés à <u>décomposer</u> E_u <u>en somme directe de sous-modules</u>. Or, $K[X]$ est un anneau principal (chap.IV, § 1) ;

une base de l'espace vectoriel E est évidemment un système de générateurs du module E_u, donc E_u est de type fini ; enfin, aucun élément de E_u n'est libre, car pour tout $x \in E$, les $n+1$ éléments $x, u(x), \ldots, u^n(x)$ de E forment un système lié, ce qui signifie qu'il existe un polynome $f = \sum_{k=0}^{n} a_k X^k \neq 0$ dans $K[X]$ tel que $f.x = 0$ dans E_u. Nous savons donc décomposer E_u en somme directe de sous-modules indécomposables, déterminés à une isomorphie près (§ 4, th.3); et par suite résoudre complètement le problème posé.

De façon précise, le module E_u sur $K[X]$ est caractérisé (à une isomorphie près) par ses facteurs invariants, qui sont r idéaux principaux (f_i) de $K[X]$ $(1 \leqslant i \leqslant r \leqslant n)$, où f_i est un polynome qui divise f_{i+1} pour $1 \leqslant i \leqslant r-1$; les polynomes f_i ne sont déterminés qu'à un facteur près appartenant à K ; on convient de choisir ce facteur de sorte que les f_i soient unitaires (chap.IV, § 1) ; les r polynomes f_i ainsi déterminés sont encore appelés les facteurs invariants de l'endomorphisme u (ou de toute matrice A de u par rapport à une base quelconque de E) . Les diviseurs élémentaires de E_u, qui sont les puissances des polynomes irréductibles (supposés unitaires) de $K[X]$ figurant dans la décomposition des f_i en facteurs premiers, sont encore appelés les diviseurs élémentaires de l'endomorphisme u (ou de la matrice A) ; pour tout polynome irréductible $p \in K[X]$ divisant f_r, et tout entier $k > 0$, la multiplicité $m(p^k)$ du diviseur élémentaire p^k de u est le nombre des entiers $i \leqslant r$ tels que p^k soit la puissance de p qui figure dans la décomposition de f_i en facteurs premiers. A chacun des diviseurs élémentaires p^k de u correspondent $m(p^k)$ sous-modules $G_{\alpha,k,p}$ $(1 \leqslant \alpha \leqslant m(p^k))$ de E_u, qui sont indécomposables, et tels que E_u soit somme directe des $G_{\alpha,k,p}$. Cette décomposition résout donc le problème initial, et montre en outre (§ 4, th.3)

que ce dernier n'admet qu'une solution, à une isomorphie près du module E_u .

On peut en outre déterminer explicitement une matrice $\underline{A}'$ de la forme (1), semblable à $\underline{A}$, et dans laquelle les $\underline{A}'_k$ ne dépendent que des diviseurs élémentaires de $\underline{A}$. En effet soit $G_{\alpha,h,p}$ un sous-module de E_u correspondant au diviseur élémentaire $p^h(X)=X^m+\rho_1 X^{m-1}+\ldots+\rho_{m-1}X+\rho_m$; par définition, p^h est l'annulateur de $G_{\alpha,h,p}$, et ce module est monogène : soit e_o un élément qui l'engendre ; si on pose $e_j=X^j.e_o=u^j(e_o)$ pour $1\leqslant j\leqslant m-1$, il résulte de la définition de e_o que les éléments e_j $(0\leqslant j\leqslant m-1)$ sont linéairement indépendants sur K . donc forment une base de l'espace vectoriel $G_{\alpha,h,p}$. On a en outre $u(e_j)=e_{j+1}$ pour $0\leqslant j\leqslant m-2$, et $u(e_{m-1})=X^m.e_o=-\rho_m e_o-\rho_{m-1}e_1-\ldots-\rho_1 e_{m-1}$; la restriction de u à $G_{\alpha,h,p}$ a donc pour matrice, quand on la rapporte à la base précédente

$$\underline{A}'_{\alpha;h,p}=\begin{pmatrix} 0 & 0 & \ldots & 0 & -\rho_m \\ 1 & 0 & \ldots & 0 & -\rho_{m-1} \\ 0 & 1 & \ldots & 0 & -\rho_{m-2} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 1 & -\rho_1 \end{pmatrix}$$

Si on opère de même pour chacun des sous-modules $G_{\alpha,h,p}$ dont E est somme directe, on voit donc que la matrice de u , par rapport à la base de E ainsi déterminée, est identique au tableau diagonal des matrices $\underline{A}'_{\alpha,h,p}$, ce qui établit notre assertion.

Ces résultats permettent de donner une condition nécessaire et suffisante pour que deux matrices carrées de même ordre sur K soient semblables. Il revient au même (chap. II, § 6, n° 11) de résoudre le problème suivant : étant donnés deux endomorphismes u,v de E , à quelle condition existe-t-il un automorphisme φ de E tel que $v=\varphi u\varphi^{-1}$,

ou encore $v\varphi=\varphi u$. Or, cela signifie que pour tout $x\in E$, on a $\varphi(u(x))=v(\varphi(x))$, et par récurrence sur k, on en déduit $\varphi(u^k(x))=v^k(\varphi(x))$ pour tout entier $k>0$; autrement dit, si E_u et E_v sont les $K[X]$-modules correspondant à u et à v , φ est une application biunivoque de E_u sur E_v telle que $\varphi(x+y)=\varphi(x)+\varphi(y)$ et $\varphi(X^k.x)=X^k.\varphi(x)$ pour tout $k>0$, et par suite $\varphi(f.x)=f.\varphi(x)$ pour tout opérateur $f\in K[X]$; en d'autres termes, φ est un <u>isomorphisme</u> du $K[X]$-module E_u sur le $K[X]$-module E_v . Inversement, si φ est un tel isomorphisme, il est clair que φ est un automorphisme de l'<u>espace vectoriel</u> E et qu'on a $v\varphi=\varphi u$. Donc, d'après le cor. du th.3 du § 4 :

PROPOSITION 2.- <u>Etant donnés deux endomorphismes</u> u,v <u>d'un espace vectoriel</u> E <u>de dimension finie sur un corps commutatif</u> K , <u>pour qu'il existe un automorphisme</u> φ <u>de</u> E <u>tel que</u> $v=\varphi u\varphi^{-1}$, <u>il faut et il suffit que</u> u <u>et</u> v <u>aient mêmes facteurs invariants</u> (ou <u>mêmes diviseurs élémentaires</u>).

COROLLAIRE.- <u>Pour que deux matrices carrées d'ordre n sur un corps commutatif</u> K <u>soient semblables, il faut et il suffit qu'elles aient mêmes facteurs invariants</u> (ou <u>mêmes diviseurs élémentaires</u>).

<u>3. Polynome caractéristique d'une matrice carrée sur un corps commutatif</u>

Soit E un espace vectoriel de dimension finie n sur un corps commutatif K , u un endomorphisme de E , E_u le $K[X]$-module associé à l'endomorphisme u obtenu en munissant E de la loi de composition externe ayant $K[X]$ pour ensemble d'opérateurs, définie par la relation $X.x=u(x)$ pour tout $x\in E$ ($n^o 2$). Considérons d'autre part le $K[X]$-module $F=E_{(K[X])}$ obtenu par <u>extension</u> à $K[X]$ du corps d'opérateurs K de l'espace vectoriel E (chap.III, § 2) ; toute base de l'espace vectoriel E est une base du $K[X]$-module F , qui est donc isomorphe à $(K[X])^n$; E peut être considéré comme sous-ensemble de F , et tout

élément de F est de la forme $\sum_i f_i(X)x_i$, où $x_i \in E$, $f_i \in K[X]$.

Cela étant, il existe une application linéaire ψ bien déterminée du $K[X]$-module F dans le $K[X]$-module E_u , telle que l'on ait $\psi(f(X)x)=f(X).x$ pour tout $f \in K[X]$ et tout $x \in E$: en effet, l'application $(f,x) \to f.x$ est une application bilinéaire de $K[X] \times E$ dans E ($K[X]$ et E étant considérés comme espaces vectoriels sur K) , donc il existe une application linéaire ψ de l'espace vectoriel $K[X] \otimes E$ dans E telle que $\psi(f(X) \otimes x)=f(X).x$, et cette relation montre aussitôt que ψ est une application linéaire du $K[X]$-module $F=E_{(K[X])}$ dans le $K[X]$-module E_u ; en outre comme $\psi(x)=x$ pour tout $x \in E \subset F$, ψ est une application de F sur E_u . Si on pose $H = \psi^{-1}(0)$, E_u est donc isomorphe au $K[X]$-module F/H . Nous allons montrer que H est le sous-module engendré par les éléments $Xz-u(z)$, où z parcourt E ; en effet, si H' est le sous-module de F engendré par ces éléments, on a $H' \subset H$, car $\psi(Xz-u(z))= \psi(Xz)- \psi(u(z))=X.z-u(z)=0$ par définition ; d'autre part la relation $Xz \equiv u(z)$ (mod.H') pour tout $z \in E$ montre que tout élément de F est congru modulo H' à un élément de E ; par suite, si $y \in H$, il existe $z \in E$ tel que $y-z \in H'$; on a donc $0= \psi(y-z)= \psi(z) =z$, autrement dit $y \in H'$, et par suite $H'=H$.

Cela étant, on sait (chap.III, § 2) que l'endomorphisme u de E se prolonge d'une seule manière en un endomorphisme $\bar{u}$ du $K[X]$-module $F = E_{(K[X])}$. Comme $y \to Xy$ est un endomorphisme de F , on peut encore dire que H est l'image de F par l'endomorphisme $y \to Xy-\bar{u}(y)$; cet endomorphisme peut s'écrire $Xe-\bar{u}$, si e désigne l'application identique de F sur lui-même. Les considérations qui précèdent montrent donc que les facteurs invariants de l'endomorphisme u de l'espace vectoriel E sont identiques aux facteurs invariants distincts de 1 de l'endomorphisme $Xe-\bar{u}$ du $K[X]$-module F (n^o 1).

Soit $\underline{A}$ la matrice de u par rapport à une base $(a_i)_{1 \leqslant i \leqslant n}$ de E ; comme (a_i) est aussi une base de F , $\underline{A}$ est la matrice de $\overline{u}$ par rapport à cette base, et $X\underline{I}-\underline{A}$ la matrice de $Xe-\overline{u}$ par rapport à la même base ($\underline{I}$ matrice unité d'ordre n) ; on voit donc que :

PROPOSITION 3.- Les facteurs invariants d'une matrice carrée A d'ordre n sur un corps commutatif K sont identiques aux facteurs invariants distincts de 1 de la matrice $X\underline{I}-\underline{A}$ sur l'anneau principal $K[X]$ (n^o 1).

Ceci démontre à nouveau une partie du cor. de la prop.2, car on peut écrire, pour toute matrice carrée inversible $\underline{P}$,

$$X\underline{I}-\underline{PAP}^{-1} = \underline{P}(X\underline{I}-\underline{A})\underline{P}^{-1}$$

donc les facteurs invariants de $\underline{PAP}^{-1}$ sont les mêmes que ceux de $\underline{A}$

DEFINITION 1.- On appelle polynome caractéristique d'une matrice carrée $\underline{A}$ d'ordre n sur un corps commutatif K , le déterminant $\chi(X)$ de la matrice carrée $X\underline{I}-\underline{A}$ sur l'anneau principal $K[X]$.

Autrement dit, si $\underline{A}=(a_{ij})$, on a

$$\chi(X)=\det(X\underline{I}-\underline{A})=\begin{vmatrix} X-a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & X-a_{22} & \cdots & -a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ -a_{n1} & -a_{n2} & \cdots & X-a_{nn} \end{vmatrix}$$

Il est clair que $\chi(X)$ est un polynome unitaire de degré n ; le coefficient de X^{n-1} dans ce polynome n'est autre que $-Tr(\underline{A})$, et le terme constant $(-1)^n \det \underline{A}$.

PROPOSITION 4.- Soient $f_i(X)$ $(1 \leqslant i \leqslant r)$ les facteurs invariants d'une matrice carrée A d'ordre n sur un corps commutatif K . On $r \leqslant n$, et pour tout k tel que $n-r<k \leqslant n$, le produit $g_k(X)=f_1(X)f_2(X)\ldots f_{k-n+r}(X)$ est un p.g.c.d. des mineurs d'ordre k de la matrice $X\underline{I}-\underline{A}$ sur $K[X]$; en particulier, on a

(2) $$\chi(X)=\det(X\underline{I}-\underline{A}) = f_1(X)f_2(X)\ldots f_r(X) .$$

Cette proposition est une conséquence immédiate de la prop.3 &x ci-dessus, et de la prop.9 du § 4 ; on voit en outre que, pour $k \leqslant n-r$, le p.g.c.d. des mineurs d'ordre k de $X\underline{I}-\underline{A}$ est égal à 1 .

On sait que le dernier facteur invariant (f_r) du module E_u est l'annulateur de ce module : autrement dit, pour qu'un polynome $g \in K[X]$ soit tel que g(u) soit l'endomorphisme identiquement nul, il faut et il suffit que g soit multiple de f_r ; il revient au même de dire que f_r est le polynome unitaire de plus petit degré tel que g(u)=0 (ou $g(\underline{A})=0$ pour toute matrice $\underline{A}$ correspondant à u) ; aussi di-t-on que f_r est le polynome minimal de l'endomorphisme u (ou de la matrice $\underline{A}$) ; la prop.4 montre que f_r est le quotient du polynome caractéristique $\chi(X)$ par le p.g.c.d. des mineurs d'ordre n-1 de la matrice $X\underline{I}-\underline{A}$. En particulier :

PROPOSITION 5 ("théorème de Hamilton-Cayley").- Si χ est le polynome caractéristique d'unematrice carrée $\underline{A}$ sur un corps commutatif K , on a $\chi(\underline{A})=0$.

La prop. 4 prouve aussi que :

PROPOSITION 6.- Soit K_o un sous-corps d'un corps commutatif K , $\underline{A}$ une matrice d'ordre n à éléments dans K_o . Les facteurs invariants de $\underline{A}$ sont les mêmes, que l'on considère $\underline{A}$ comme matrice sur le corps K_o ou sur le corps K .

On notera par contre que les diviseurs élémentaires de $\underline{A}$ considérée comme matrice sur K ne sont pas en général les mêmes que lorsque $\underline{A}$ est considérée comme matrice sur K_o , car un polynome irréductible dans $K_o[X]$ peut être réductible dans $K[X]$.

COROLLAIRE.- Si A et B sont deux matrices sur K_0, semblables quand on les considère comme matrices sur K, elles sont aussi semblables quand on les considère comme matrices sur K_0.

Autrement dit, s'il existe une matrice inversible P à éléments dans K telle que $B=PAP^{-1}$, il existe aussi une matrice inversible P_0 à éléments dans K_0, telle que $B=P_0AP_0^{-1}$.

4. Réduction d'une matrice carrée sur un corps algèbriquement fermé.

Un cas particulièrement important est celui où les diviseurs élémentaires d'une matrice carrée A sont des puissances depolynomes du premier degré c'est-à-dire si le polynome caractéristique de A a toutes ses racines dans K ; ce cas se présente toujours lorsque le corps K est algèbriquement fermé. Les racines du polynome caractéristique de A sont alors appelées racines caractéristiques ou valeurs propres de la matrice A (ou de l'endomorphisme u) ; leur ensemble est appelé le spectre de A (ou de u). Ces racines sont les éléments $\lambda \in K$ tels que l'endomorphisme $x \longrightarrow \lambda x - u(x)$ ait un déterminant nul, ou encore soit de rang $< n$; il revient au même de dire que ce sont les valeurs de λ telles que l'équation

$$u(x) = \lambda x \tag{2}$$

admette au moins une solution $x \neq 0$. Pour une valeur propre λ de u, les éléments $x \in E$ satisfaisant à (2) sont appelés vecteurs propres correspondant à la valeur propre λ ; si $\lambda I - A$ est de rang $n-p$, les vecteurs propres correspondant à λ forment un espace vectoriel de dimension p.

D'après l'expression du rang d'une matrice carrée à l'aide de ses mineurs (chap.III, §7, prop.) et la prop.4, le nombre p est identique au nombre des facteurs invariants f_i de A qui sont divisibles par $X-\lambda$.

Lorsqu'un diviseur élémentaire de A est de la forme $(X-\lambda)^m$, on peut choisir une base dans chacun des sous-espaces $G_{\alpha,h,p}$ correspondant à ce diviseur, de sorte que la matrice de u (restreint à ce sous-espace) par rapport à cette base soit particulièrement simple. En effet, par hypothèse $G_{\alpha,h,p}$ est un sous-module monogène de E_u, dont $(X-\lambda)^m$ est l'annulateur ; soit a un élément engendrant ce sous-module ; si on pose $b_i=(X-\lambda)^{m-i}.a$ pour $1\leqslant i\leqslant m$ (c'est-à-dire $b_i=\sum_{k=0}^{m}(-1)^k\binom{m-i}{k}\lambda^k u^{m-i-k}(a)$) les b_i forment un système libre de m éléments de $G_{\alpha,h,p}$, puisqu'aucun polynome non nul de degré $<m$ ne peut annuler a ; les b_i forment donc une base de $G_{\alpha,h,p}$, et on a

$$u(b_1)=X.b_1=(X-\lambda).b_1+\lambda b_1=(X-\lambda)^m.a+\lambda b_1=\lambda b_1$$

$$u(b_i)=X.b_i=(X-\lambda).b_i+\lambda b_i=b_{i-1}+\lambda b_i \quad \text{pour} \quad 2\leqslant i\leqslant m$$

Autrement dit, la matrice de la restriction de u à $G_{\alpha,h,p}$, rapportée à la base (b_i), est la matrice d'ordre m

$$(3)\qquad J=\begin{pmatrix} \lambda & 1 & 0 & \dots & 0 & 0 \\ 0 & \lambda & 1 & \dots & 0 & 0 \\ & & \dots\dots\dots\dots & & & \\ 0 & 0 & 0 & \dots & \lambda & 1 \\ 0 & 0 & 0 & \dots & 0 & \lambda \end{pmatrix}.$$

Une matrice de cette forme est dite matrice de Jordan ; si donc le polynome caractéristique de A a toutes ses racines dans K, la matrice A est semblable à un "tableau diagonal de matrices" composé de matrices de Jordan, dont chacune correspond à un diviseur élémentaire de A ; une telle matrice est appelée forme canonique de Jordan de A.

Le cas le plus intéressant est celui où toutes les matrices de Jordan correspondant aux diviseurs élémentaires de A sont d'ordre 1, c'est-à-dire où A est semblable à la matrice diagonale

$$\begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \lambda_n \end{pmatrix}$$

où λ_i $(1 \leqslant i \leqslant n)$ sont les n racines caractéristiques de A (distinctes ou non). C'est le cas d'où nous sommes partis au début dun n° 2 ; chacun des modules monogènes en lesquels se décompose E_u est alors simple, autrement dit, E_u est un module semi-simple (chap.I, § 6, n°) ; on dit alors que l'endomorphisme u (ou la matrice A) est complètement réductible. Pour qu'il en soit ainsi, il faut et il suffit que tous les diviseurs élémentaires de A soient du premier degré, ou, ce qui revient au même, que le polynome minimal de A n'ait pas de racine multiple (en admettant toujours que toutes ses racines appartiennent à K) . Il en est ainsi, évidemment dans le cas plus particulier où le polynome caractéristique de A n'a que des racines simples, appartenant toutes à K.

Etant donné une extension algèbriquement fermée Ω du corps K , on appelle encore racines caractéristiques de A les racines dans Ω de son polynome caractéristique (même si elles n'appartiennent pas à K) ; on peut dire que ce sont les racines caractéristiques de A considérée comme matrice à éléments dans Ω . Si λ_i $(1 \leqslant i \leqslant n)$ sont ces racines (distinctes ou non), on a les relations

$$(4) \qquad \operatorname{Tr} A = \sum_{i=1}^{n} \lambda_i$$

$$\det A = \prod_{i=1}^{n} \lambda_i .$$

Remarque.- Le calcul des racines caractéristiques d'une matrice $A=(a_{ij})$ est particulièrement simple lorsque A est une matrice triangulaire (chap.II, § 6, n°5) ; le polynome caractéristique est en effet alors $\prod_{i=1}^{n} (X-a_{ii})$; on voit que dans ce cas les racines caractéristiques appartiennent à K .

PROPOSITION 7.- Toute matrice carrée sur un corps commutatif K est semblable à sa transposée.

D'après le cor. de la prop.6, il suffit de démontrer qu'une matrice carrée A sur K et sa transposée ${}^tA$ sont semblables quand on les considère comme matrices sur une extension algébriquement fermée Ω de K. Comme A est alors semblable à une matrice B mise sous la forme canonique de Jordan, et par suite ${}^tA$ semblable à ${}^tB$, on peut se borner à faire la démonstration pour une matrice de Jordan J de la forme (3). Or, une telle matrice est la matrice, par rapport à une base $(b_i)_{1\leqslant i\leqslant m}$ d'un espace G, de l'endomorphisme u de G tel que $u(b_1)=\lambda b_1$, $u(b_i)=b_{i-1}+\lambda b_i$ pour $2\leqslant i\leqslant m$; si on pose $c_i=b_{m-i}$, on a $u(c_i)=\lambda c_i+c_{i+1}$ pour $0\leqslant i\leqslant m-2$ et $u(c_{m-1})=\lambda c_{m-1}$, donc la matrice de u par rapport à la base (c_i) n'est autre que ${}^tJ$, ce qui démontre la proposition.

PROPOSITION 8.- Soit A une matrice carrée d'ordre n sur un corps algébriquement fermé K, et soient λ_i $(1\leqslant i\leqslant n)$ les racines caractéristiques (distinctes ou confondues) de A ; si g est une fraction rationnelle quelconque de $K(X)$, pour que A soit substituable dans g, il faut et il suffit que chacun des λ_i le soit, et les racines caractéristiques de la matrice $g(A)$ sont alors $g(\lambda_i)$ $(1\leqslant i\leqslant n)$.

Démontrons d'abord la proposition lorsque g est un polynome : elle se réduit alors à prouver que les racines caractéristiques de la matrice $g(A)$ sont les $g(\lambda_i)$. Il suffit évidemment de faire la démonstration pour une matrice de Jordan J de la forme (3) ; or, on vérifie aussitôt par récurrence que dans la matrice J^k, les termes diagonaux sont tous égaux à λ^k, et les termes au-dessous de la diagonale sont nuls ; par suite, dans la matrice $f(J)$, les termes diagonaux sont tous égaux

à $f(\lambda)$, et les termes au-dessous de la diagonale sont nuls ce qui signifie que $f(\lambda)$ est racine multiple d'ordre m du polynome caractéristique de $f(\underline{J})$.

La proposition étant ainsi démontrée pour les polynomes, on en déduit d'abord que si $g=\frac{u}{v}$, où u et v sont des polynomes premiers entre eux de $K[X]$, les racines caractéristiques de $\underline{B}=v(\underline{A})$ sont les $v(\lambda_i)$; pour que $\underline{A}$ soit substituable dans g, c'est-à-dire que $\underline{B}$ soit inversible, il faut et il suffit que les racines caractéristiques $v(\lambda_i)$ de $\underline{B}$ soient toutes $\neq 0$, c'est-à-dire que chacun des λ_i soit substituable dans g. En supposant cette condition réalisée, nous allons voir qu'il existe un polynome $w \in K[X]$ tel que l'on ait $\underline{B}^{-1}=w(\underline{B})$ et, en posant $\mu_i=v(\lambda_i)$, $\mu_i^{-1}=w(\mu_i)$ $(1 \leqslant i \leqslant n)$; on en déduira bien que $g(\underline{A})=u(\underline{A})\underline{B}^{-1}=u(\underline{A})w(v(A))$ a pour racines caractéristiques $u(\lambda_i)w(v(\lambda_i))=u(\lambda_i)w(\mu_i)=u(\lambda_i)(v(\lambda_i))^{-1}=g(\lambda_i)$. Or, pour former le polynome w, considérons le polynome minimal $h(X)=\sum_{k=0}^{p} a_k X^k$ de la matrice $\underline{B}$; on a $h(\underline{B})=0$, c'est-à-dire $\sum_{k=0}^{p} a_k \underline{B}^k = 0$; cela entraîne d'abord $a_0 \neq 0$, sans quoi, en multipliant par $\underline{B}^{-1}$, on voit que $\underline{B}$ annulerait un polynome de degré $< p$, et par suite que h ne serait pas le polynome minimal de $\underline{B}$. On peut donc écrire $\underline{B}^{-1}=w(\underline{B})$, en posant $w(X) = -\sum_{k=1}^{p} \frac{a_k}{a_0} X^{k-1}$; d'autre part, on a $h(\mu_i)=0$ pour $1 \leqslant i \leqslant n$, d'où on tire $\mu_i^{-1} = w(\mu_i)$ par le même raisonnement. La proposition est ainsi complètement démontrée.

5. Application aux équations linéaires sur un corps algèbriquement fermé.

Soit E un espace vectoriel de dimension n sur un corps commutatif algèbriquement fermé K ; si u est un endomorphisme de l'espace E, la connaissance des diviseurs élémentaires de u permet d'étudier aisément l'équation linéaire en x

(6) $\lambda x - u(x) = y$ (où $y \in E$)

suivant les diverses valeurs du paramètre $\lambda \in K$. Pour que (6) ait une solution quel que soit $y \in E$, il faut et il suffit que l'équation $u(x) - \lambda x = 0$ n'ait d'autre solution que 0 (chap.II, § 3, cor. de la prop.11); autrement dit, que λ soit distinct des valeurs propres de u.

Pour obtenir dans ce cas l'expression de x en fonction de y et de λ, rapportons u à une base telle que la matrice correspondante $\underline{A}$ soit sous la forme canonique de Jordan

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

où les $\underline{J}_i$ sont des matrices de Jordan. L'équation (6) équivaut à l'équation

(7) $$(\lambda \underline{I} - \underline{A})x = y$$

(en identifiant comme d'ordinaire x et y avec les matrices à une colonne correspondantes) ; si on pose $\underline{R}_\lambda = (\lambda \underline{I} - \underline{A})^{-1}$, on en tire $x = \underline{R}_\lambda y$; il suffit donc de calculer la matrice $\underline{R}_\lambda$, qu'on appelle la résolvante de l'équation (7), ou de la matrice $\underline{A}$. Il est immédiat que $\underline{R}_\lambda$ est un "tableau diagonal" formé des résolvantes des matrices de Jordan $\underline{J}_i$; tout revient donc au cas où la matrice de u est une matrice de Jordan

$$\underline{J} = \begin{pmatrix} \lambda_0 & 1 & \dots & 0 \\ 0 & \lambda_0 & \dots & 0 \\ & \dots\dots\dots & & \\ 0 & 0 & \dots & \lambda_0 \end{pmatrix}$$

Soit alors $(b_i)_{1\leqslant i\leqslant n}$ la base à laquelle on a rapporté u ; si $x=\sum_{i=1}^{n} b_i \xi_i$, $y=\sum_{i=1}^{n} b_i \eta_i$, l'équation $(\lambda \underline{I}-\underline{J})x=y$ est équivalente au système linéaire

$$(\lambda-\lambda_0)\xi_i-\xi_{i+1}=\eta_i \qquad (1\leqslant i\leqslant n-1)$$
$$(\lambda-\lambda_0)\xi_n=\eta_n$$

qui se résout aussitôt par récurrence et donne

$$\xi_i=\sum_{h=0}^{n-i}\frac{\eta_{i+h}}{(\lambda-\lambda_0)^{h+1}} \qquad (1\leqslant i\leqslant n)$$

d'où la résolvante de $\underline{J}$

$$(\lambda \underline{I}-\underline{J})^{-1}=\begin{pmatrix} \frac{1}{\lambda-\lambda_0} & \frac{1}{(\lambda-\lambda_0)^2} & \cdots & \frac{1}{(\lambda-\lambda_0)^n} \\ 0 & \frac{1}{\lambda-\lambda_0} & \cdots & \frac{1}{(\lambda-\lambda_0)^{n-1}} \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & & \frac{1}{\lambda-\lambda_0} \end{pmatrix}$$

En revenant au cas général, soient λ_i $(1\leqslant i\leqslant p)$ les racines caractéristiques distinctes de la matrice $\underline{A}$; pour chaque indice i , soient $(X-\lambda_i)^{m_{ij}}$ les diviseurs élémentaires de $\underline{A}$ (distincts ou non) correspondant à la racine λ_i $(1\leqslant j\leqslant q_i)$; on a $\sum_{i=1}^{p}\left(\sum_{j=1}^{q_i} m_{ij}\right)=n$. Si pour chaque i , on désigne par m_i le plus grand des entiers m_{ij} $(1\leqslant j\leqslant q_i)$, on voit, d'après ce qui précède, que la résolvante de $\underline{A}$ peut s'écrire

$$\underline{R}_\lambda=\sum_{i=1}^{p}\sum_{k=1}^{m_i}\frac{1}{(\lambda-\lambda_i)^k}\underline{R}_{ik}$$

où les $\underline{R}_{ik}$ sont des matrices $\neq 0$, ne dépendant pas de λ .

On remarquera que, si λ et μ sont deux éléments de K distincts des valeurs propres de $\underline{A}$, on a l'identité

$$(8) \qquad \underline{R}_\lambda-\underline{R}_\mu=(\lambda-\mu)\underline{R}_\lambda\underline{R}_\mu \ .$$

En effet, il suffit de multiplier par $\underline{R}_\lambda\underline{R}_\mu$ les deux membres de l'identité $(\lambda \underline{I}-\underline{A})-(\mu \underline{I}-\underline{A})=(\lambda-\mu)I$, en remarquant que $\underline{R}_\lambda$ et $\underline{R}_\mu$ sont permutables, puisque leurs inverses le sont.

Delsarte 10-1

Supposons maintenant que λ soit une valeur propre de l'endomorphisme u ; il résulte alors de la théorie générale des équations linéaires (chap.II, § 4, th.3) que la condition de possibilité de l'équation (6) est que y soit orthogonal au sous-espace vectoriel G du dual E^* de E, formé des solutions de l'équation

$$\lambda x' - {}^t u(x') = 0 . \qquad (9)$$

Autrement dit, G est l'ensemble des vecteurs propres $x' \in E^*$ correspondant à la valeur propre λ de ${}^t u$, c'est-à-dire le nombre ρ des diviseurs élémentaires de ${}^t u$ qui sont des puissances de $X-\lambda$; comme ${}^t u$ a les mêmes diviseurs élémentaires que u (prop.7), ρ est aussi le nombre des vecteurs propres de u correspondant à la valeur propre λ. Si on désigne par v l'endomorphisme $x \longrightarrow \lambda x - u(x)$, ${}^{-1}v(0)$ est donc de dimension ρ, $v(E)$ de dimension $n-\rho$ (autrement dit, v est de rang $n-\rho$). Mais il faut noter qu'en général, $v(E)$ n'est pas supplémentaire de ${}^{-1}v(0)$. Cherchons en effet les éléments y de l'intersection ${}^{-1}v(0) \cap v(E)$; pour un tel y, il existe $x \in E$ tel que $y = \lambda x - u(x) = (\lambda - X).x$, et d'autre part on doit avoir $\lambda y - u(y) = 0$, c'est-à-dire $(\lambda - X).y = 0$, d'où $(\lambda - X)^2.x = 0$; la réciproque est immédiate. Or, soit $\sigma \leqslant \rho$ le nombre des diviseurs élémentaires de u qui sont divisibles par $(X-\lambda)^2$; le raisonnement qui conduit à la forme canonique de Jordan (n° 4) montre que ${}^{-1}v(0) \cap v(E)$ a une dimension égale à σ. On a donc la proposition suivante :

PROPOSITION 9.- Soit u un endomorphisme d'un espace vectoriel E de dimension n sur un corps commutatif K ; soit λ une valeur propre de u, v l'endomorphisme $x \longrightarrow \lambda x - u(x)$; pour que E soit somme directe des sous-espaces ${}^{-1}v(0)$ et $v(E)$, il faut et il suffit que λ soit racine simple du polynome minimal de u.

On notera que cette condition sera remplie en particulier lorsque u est complètement réductible.

Remarque.- Lorsqu'on cherche à généraliser la notion de valeur propre à un endomorphisme u d'un espace vectoriel E de dimension infinie sur un corps commutatif K , l'idée la plus naturelle consiste à donner ce nom aux éléments $\lambda \in K$ tels que l'équation (6) ait des solutions $\neq 0$. Mais alors la plupart des résultats ci-dessus ne sont plus valables : par exemple, en désignant par v l'endomorphisme $x \longrightarrow \lambda x - u(x)$, on peut avoir $v^{-1}(0) = \{0\}$, mais $v(E) \neq E$; dans ce cas, λ n'est pas valeur propre au sens précédent, mais l'équation $\lambda x - u(x) = y$ n'a pas de solution pour certaines valeurs de y ; on notera que dans ce cas, λ est valeur propre (au sens ci-dessus) de la transposée ${}^t u$ de u . Inversement, il peut se faire qu'on ait $v^{-1}(0) \neq 0$, mais $v(E) = E$: λ est alors valeur propre de u , mais non de ${}^t u$. Comme nous le verrons ultérieurement, il convient d'élargir la notion de "valeur propre" , en désignant ainsi les valeurs λ pour lesquelles $x \longrightarrow \lambda x - u(x)$ cesse d'être un automorphisme de E , ou cesse de satisfaire à certaines conditions en relation avec une topologie donnée sur E .

6. Base normale d'une extension cyclique.

Au chap.V (§ 6), nous avons démontré que toute extension galoisienne N d'un corps K infini, de degré fini sur K , admet une base normale. Nous allons maintenant démontrer, à l'aide de la théorie des diviseurs élémentaires, le même théorème dans le cas où K est un corps fini ; on sait alors que N est une extension cyclique de K (chap.V, § 7, prop.6). La démonstration que nous allons donner (due à Artin) suppose seulement que N est une extension cyclique de K , K étant fini ou non.

Soit Γ le groupe (cyclique) de N sur K , n son ordre, σ un générateur de Γ ; lorsqu'on considère N comme un espace vectoriel de dimension n sur K , σ est un endomorphisme de N ; il lui correspond donc (n°2) un $K[X]$-module N_σ , le produit $f.x$, où $f = \sum_{k=0}^{m} a_k X^k$ appartient à $K[X]$, étant égal à $\sum_{k=0}^{m} a_k \sigma^k(x)$. Par hypothèse, on a $\sigma^n = 1$, donc $(X^n-1).x=0$ pour tout $x \in N$, X^n-1 est un multiple de l'annulateur $g = \sum_{k=0}^{m} \beta_k X^k$ du module N_σ ; mais d'autre part le degré m de cet annulateur est nécessairement $\geqslant n$, sans quoi on aurait identiquement $\sum_{k=0}^{m} \beta_k \sigma^k(x)=0$ pour tout $x \in N$, les β_k n'étant pas tous nuls, et on sait (chap.V, § 4, th.1) que les n automorphismes distincts σ^k $(0 \leqslant k \leqslant n-1)$ sont linéairement indépendants. On voit ainsi que X^n-1 est l'annulateur de N_σ , et comme il est de degré n , N_σ est un $K[X]$-module monogène (n°2) ; si $a \in N$ est un élément engendrant N_σ , les n éléments $\sigma^k(a)$ sont par définition linéairement indépendants par rapport à K $(0 \leqslant k \leqslant n-1)$, et forment donc bien une base normale de N par rapport à K .

§ 6. Anneaux noetheriens.

(théorie élémentaire)

Il ne sera question dans ce paragraphe que d'anneaux commutatifs ayant un élément unité.

1. Le théorème de Hilbert.

Nous avons défini au § 4 (n°1) les anneaux noetheriens (commutatifs , et ayant un élément unité). Tout anneau principal (et en particulier tout corps commutatif) est un anneau noetherien.

PROPOSITION 1.- Tout anneau quotient d'un anneau noetherien est un anneau noetherien.

En effet, soit A un anneau noetherien, $\mathfrak{a}$ un idéal dans A , φ l'homomorphisme canonique de A sur $A/\mathfrak{a}$; tout idéal dans $A/\mathfrak{a}$ est de la forme $\varphi(\mathfrak{b})$, où $\mathfrak{b}$ est un idéal de A contenant $\mathfrak{a}$; comme $\mathfrak{b}$ admet par hypothèse un système de générateurs fini S (en tant que A-module), $\varphi(\mathfrak{b})$ admet (en tant que $A/\mathfrak{a}$ -module) le système de générateurs fini $\varphi(S)$.

PROPOSITION 2.- Tout anneau produit d'un nombre fini d'anneaux noetheriens est un anneau noetherien.

En effet, si $A=\prod_{i=1}^{n} A_i$ est un produit d'anneaux noetheriens, tout idéal dans A est produit de ses projections $\mathfrak{a}_i$ dans A_i ; si S_i est un système fini de générateurs de $\mathfrak{a}_i$ $(1\leqslant i\leqslant n)$, il est immédiat que $\prod_{i=1}^{n} S_i$ est un système fini de générateurs de $\mathfrak{a}$.

On notera par contre qu'un sous-anneau d'un anneau noetherien n'est pas nécessairement noetherien : par exemple, si A est un anneau d'intégrité qui n'est pas noetherien, son corps des quotients $K \supset A$ est un anneau noetherien.

THÉORÈME 1 (Hilbert).- Si A est un anneau noetherien (commutatif et ayant un élément unité), l'anneau ~~des polynomes~~ $A[X]$ des polynomes à une indéterminée sur A est un anneau noetherien.

Soit $\mathfrak{a}$ un idéal quelconque dans $A[X]$, et pour tout entier $n \geqslant 0$, soit H_n l'ensemble des polynomes $u \in \mathfrak{a}$ de degré $\leqslant n$; $H_0 = \mathfrak{a} \cap A$ est un idéal dans A , et par suite un A-module de type fini ; nous allons voir d'abord par récurrence sur n que H_n est un A-module de type fini pour tout $n > 0$. En effet, considérons l'ensemble $\mathfrak{a}_n$ des coefficients de X^n dans tous les éléments de H_n ; il est immédiat que $\mathfrak{a}_n$ est un idéal dans A , et par suite admet un système fini de générateurs $a_1, a_2, \ldots, a_p$. Pour chaque indice k $(1\leqslant k\leqslant p)$ soit u_k un polynome appartenant à H_n et ayant a_k comme coefficient de X^n ;

soit $u(X)=\lambda_0 X^n+\lambda_1 X^{n-1}+\ldots+\lambda_n$ un élément quelconque de H_n ; par hypothèse, il existe des éléments $\mu_k \in A$ $(1\leqslant k\leqslant p)$ tels que $\lambda_0=\sum_{k=1}^{p}\mu_k a_k$; donc $u-\sum_{k=1}^{p}\mu_k u_k$ a un degré $\leqslant n-1$, autrement dit appartient à H_{n-1} ; si S est un système de générateurs fini du A-module H_{n-1}, on voit donc que les u_k $(1\leqslant k\leqslant p)$ et les éléments de S forment un système de générateurs de H_n ; ce dernier est donc un A-module de type fini, et a fortiori un $A[X]$-module de type fini.

Soit maintenant $\mathfrak{b}$ l'ensemble formé de 0 et des coefficients des termes dominants des polynomes $u \in \mathfrak{a}$ non nuls, et montrons que $\mathfrak{b}$ est un <u>idéal</u> dans A. Il est évident que si α est coefficient du terme dominant de u, $\lambda\alpha$ est coefficient du terme dominant de λu si $\lambda \neq 0$, et nul dans le contraire, donc appartient à $\mathfrak{b}$; d'autre part, si $u=\lambda_0 X^m+\ldots+\lambda_m$ et $v=\mu_0 X^n+\ldots+\mu_n$ sont deux polynomes appartenant à $\mathfrak{a}$, de degrés respectifs m et n, et si par exemple $m\leqslant n$, le polynome $X^{n-m}u+v$ appartient à $\mathfrak{a}$, et si $\lambda_0+\mu_0\neq 0$, c'est le coefficient du terme dominant de ce polynome, donc $\lambda_0+\mu_0$ appartient à $\mathfrak{b}$. Soit alors $(\beta_i)_{1\leqslant i\leqslant q}$ un système de générateurs fini de cet idéal, et pour chaque indice i $(1\leqslant i\leqslant q)$, soit v_i un polynome de dont β_i est le coefficient du terme dominant ; soit n le plus grand des degrés n_i des v_i ; nous allons voir que les v_i et un système de générateurs de H_n forment un système de générateurs de $\mathfrak{a}$, ce qui établira le théorème.

Soit donc $u=\lambda_0 X^m+\ldots+\lambda_m$ un polynome quelconque de degré m appartenant à $\mathfrak{a}$, et prouvons que u est combinaison linéaire (à coefficients dans $A[X]$) des v_i et d'éléments de H_n. Si $m\leqslant n$, la proposition est évidente, puisque $u\in H_n$; raisonnons donc par récurrence sur m. On a par hypothèse $\lambda_0 \in \mathfrak{b}_q$, donc il existe q éléments $\mu_i \in A$ $(1\leqslant i\leqslant q)$ tels que $\lambda_0=\sum_{i=1}^{q}\mu_i\beta_i$; par suite le polynome

$u - \sum_{i=1}^{q} \mu_i X^{m-n_i} v_i$, qui appartient à $\mathfrak{a}$, a un degré $\leqslant n-1$, et par suite est combinaison linéaire (à coefficients dans $A[X]$) des v_i et d'éléments de H_n . C.Q.F.D.

COROLLAIRE.- Si A est un anneau noetherien, tout anneau de polynomes $A[X_1, X_2, \ldots, X_n]$ à un nombre fini d'indéterminées est un anneau noetherien.

Il suffit d'appliquer le th.1 par récurrence sur n .

En particulier, pour tout corps K , l'anneau de polynomes $K[X_1, X_2, \ldots, X_n]$ est noetherien ; de même, si A est un anneau principal, $A[X_1, X_2, \ldots, X_n]$ est noetherien.

Un exemple d'anneau non noetherien est donné par un anneau de polynomes $K[X_n]_{n \in \mathbb{N}}$ à une infinité dénombrable d'indéterminées. Désignons en effet par $\mathfrak{a}_n$ l'idéal de cet anneau engendré par les X_p d'indice $p \leqslant n$; on a $\mathfrak{a}_n \subset \mathfrak{a}_{n+1}$ et X_{n+1} , qui appartient à $\mathfrak{a}_{n+1}$, ne peut appartenir à $\mathfrak{a}_n$, car tout polynome appartenant à $\mathfrak{a}_n$ et $\neq 0$ a toujours un degré non nul par rapport à l'un des X_p d'indice $\leqslant n$.

2. Produit d'idéaux.

Dans ce n^{o} et les trois suivants, les anneaux que nous considérerons sont commutatifs et ont un élément unité, mais ne sont pas nécessairement noetheriens.

DÉFINITION 1.- Etant donnés deux idéaux $\mathfrak{a}$, $\mathfrak{b}$ dans un anneau A , on appelle produit de $\mathfrak{a}$ par $\mathfrak{b}$ l'idéal engendré par les éléments xy, ou x parcourt $\mathfrak{a}$ et y parcourt $\mathfrak{b}$.

Autrement dit, ce produit est l'ensemble des sommes $\sum_{i=1}^{n} x_i y_i$, où (x_i) et (y_i) $(1 \leqslant i \leqslant n)$ sont deux suites finies quelconques d'éléments appartenant respectivement à $\mathfrak{a}$ et $\mathfrak{b}$.

Par abus de langage, nous désignerons le produit de $\mathfrak{a}$ par $\mathfrak{b}$ par la notation $\mathfrak{a}\mathfrak{b}$ ou $\mathfrak{a}.\mathfrak{b}$, bien que cette notation ait désigné jusqu'ici l'ensemble des produits xy, où $x \in \mathfrak{a}$ et $y \in \mathfrak{b}$, ensemble qui n'est pas un idéal en général (cf. exerc.) ; mais comme cet ensemble n'interviendra pas dans les questions où intervient le produit d'idéaux, il ne saurait y avoir de confusion. On notera que si $\mathfrak{a}$ est un idéal principal (a) de A, $(a).\mathfrak{b}$ est l'ensemble des éléments ay, où $y \in \mathfrak{b}$; on le note encore $a\mathfrak{b}$. Si $\mathfrak{b} = (b)$ est aussi un idéal principal, on a $\mathfrak{a}\mathfrak{b} = (ab)$ (autrement dit le produit de deux idéaux principaux est le produit défini dans ce cas au § 3, n°1).

Il est immédiat que le produit ainsi défini dans l'ensemble $\mathfrak{J}$ des idéaux de A est commutatif et associatif, car les idéaux $\mathfrak{a}(\mathfrak{b}\mathfrak{c})$ et $(\mathfrak{a}\mathfrak{b})\mathfrak{c}$ sont tous deux identiques à l'idéal engendré par les produits xyz, où $x \in \mathfrak{a}$, $y \in \mathfrak{b}$ et $z \in \mathfrak{c}$. L'idéal principal (1)=A est élément neutre de cette loi de composition.

La relation $\mathfrak{a} \subset \mathfrak{b}$ entraîne évidemment $\mathfrak{a}\mathfrak{c} \subset \mathfrak{b}\mathfrak{c}$ quel que soit l'idéal $\mathfrak{c}$; en outre, on a la propriété de distributivité

$$\mathfrak{a}(\mathfrak{b} + \mathfrak{c}) = \mathfrak{a}\mathfrak{b} + \mathfrak{a}\mathfrak{c} \tag{1}$$

car chacun des deux membres est engendré par l'ensemble formé des produits xy et des produits $x'z$ (où x et x' parcourent $\mathfrak{a}$, y parcourt $\mathfrak{b}$ et z parcourt $\mathfrak{c}$).

On peut donc dire que, muni de la loi de composition interne $(\mathfrak{a}, \mathfrak{b}) \to \mathfrak{a}\mathfrak{b}$ et de la relation d'inclusion, $\mathfrak{J}$ est un monoïde semi-réticulé supérieurement (§ 1, n°7) ; toutes les propriétés de ces monoïdes démontrées au § 1 sont donc applicables à $\mathfrak{J}$; nous laissons au lecteur le soin de les énoncer avec les notations correspondantes.

On remarquera qu'en général, $\mathcal{J}$ n'est pas semi-réticulé inférieurement, c'est-à-dire qu'on a en général, $\mathfrak{a}(\mathfrak{b}\cap\mathfrak{c})\neq(\mathfrak{a}\mathfrak{b})\cap(\mathfrak{a}\mathfrak{c})$ (on peut seulement dire que le premier membre est contenu dans le second). Par exemple, considérons dans l'anneau $Q[X,Y]$ les idéaux $\mathfrak{b}=(X)$, $\mathfrak{c}=(Y)$ et $\mathfrak{a}=(X)+(Y)$; il est immédiat que $\mathfrak{b}\cap\mathfrak{c}=(XY)$; donc les polynomes appartenant à $\mathfrak{a}(\mathfrak{b}\cap\mathfrak{c})$ ont tous leurs termes $\neq 0$ de degré $\geqslant 3$, alors que le polynome XY appartient à la fois à $\mathfrak{a}\mathfrak{b}$ et à $\mathfrak{a}\mathfrak{c}$.

On notera enfin qu'on a $\mathfrak{a}\mathfrak{b}\subset\mathfrak{a}\cap\mathfrak{b}$, les deux membres étant en général distincts ; en particulier $\mathfrak{a}^{n+1}\subset\mathfrak{a}^n$ pour tout entier $n>0$.

Remarque.- La déf.1 peut s'étendre au cas où $\mathfrak{a}$ et $\mathfrak{b}$ sont deux A-modules dans une algèbre commutative E sur l'anneau A ; toutes les propriétés énoncées ci-dessus pour le produit d'idéaux sont encore valables dans ce cas.

3. Transporteurs d'idéaux.

Soient $\mathfrak{a}$ et $\mathfrak{b}$ deux idéaux dans un anneau A ; l'ensemble des éléments $x\in A$ tels que $x\mathfrak{b}\subset\mathfrak{a}$ est un idéal, puisque $x\mathfrak{b}+y\mathfrak{b}=(x+y)\mathfrak{b}$, et $zx\mathfrak{b}\subset x\mathfrak{b}$ pour tout $z\in A$. Cet idéal est dit transporteur de $\mathfrak{b}$ dans $\mathfrak{a}$, et noté $\mathfrak{a}:\mathfrak{b}$; on a évidemment $\mathfrak{a}\subset\mathfrak{a}:\mathfrak{b}$.

Exemple.- Si A est un anneau principal (§ 3, n°6), $(\mathfrak{p}_\iota)$ la famille des idéaux maximaux de A, et si $\mathfrak{a}=\prod_\iota \mathfrak{p}_\iota^{n_\iota}$ $\mathfrak{b}=\prod_\iota \mathfrak{p}_\iota^{m_\iota}$, pour que $x\in\mathfrak{a}:\mathfrak{b}$, il faut et il suffit évidemment, si $(x)=\prod_\iota \mathfrak{p}_\iota^{q_\iota}$, que l'on ait $q_\iota+m_\iota\geqslant n_\iota$ pour tout ι, d'où l'on déduit aussitôt que

$$\mathfrak{a}:\mathfrak{b}=\prod_\iota \mathfrak{p}_\iota^{(n_\iota-m_\iota)+}$$

Si $\mathfrak{b}\subset\mathfrak{a}$, on a $\mathfrak{a}:\mathfrak{b}=A=(1)$; onversement, si $\mathfrak{a}:\mathfrak{b}=(1)$, on a par définition $1.\mathfrak{b}=\mathfrak{b}\subset\mathfrak{a}$

D'après la définition de $\mathfrak{a} : \mathfrak{b}$ on a $\mathfrak{b} . (\mathfrak{a} : \mathfrak{b}) \subset \mathfrak{a}$, mais en général cet idéal produit est distinct de , comme le montre l'exemple considéré ci-dessus.

La proposition suivante est évidente à partir des définitions ;:

PROPOSITION 3.- Quels que soient la famille $(\mathfrak{a}_\nu)$ d'idéaux de A , on a, pour tout idéal $\mathfrak{b}$ de A

(1) $$(\bigcap_\nu \mathfrak{a}_\nu) : \mathfrak{b} = \bigcap_\nu (\mathfrak{a}_\nu : \mathfrak{b}) .$$

4. Idéaux premiers ; radical d'un idéal.

DÉFINITION 2.- Dans un anneau commutatif A ayant un élément unité, on dit qu'un idéal $\mathfrak{p} \neq A$ est premier si l'anneau quotient $A/\mathfrak{p}$ est un anneau d'intégrité.

Il revient au même de dire que les relations $x \notin \mathfrak{p}$, $y \notin \mathfrak{p}$ entraînent $xy \notin \mathfrak{p}$, puisque la relation $x \notin \mathfrak{p}$ signifie que, dans $A/\mathfrak{p}$, la classe de x est $\neq 0$. La déf.2 peut donc encore s'exprimer en disant que le complémentaire $\complement \mathfrak{p}$ est une partie de A stable pour la multiplication.

Exemples.- 1) Tout idéal maximal $\mathfrak{p}$ dans A est premier, puisque $A/\mathfrak{p}$ est alors un corps. Dans un anneau principal, tout idéal premier est maximal, car si (a) n'est pas maximal (c'est-à-dire (§ 3, n°6) si a n'est pas un élément premier dans A), on peut écrire $a = bc$, où b et c ne sont pas divisibles par a . Mais on peut donner des exemples d'anneaux dans lesquels il existe des idéaux premiers non maximaux : c'est le cas d'un anneau de polynomes $K[X,Y]$ sur un corps K , où l'idéal (X) est premier mais non maximal, l'anneau quotient $K[X,Y]/(X)$ étant isomorphe à l'anneau d'intégrité $K[Y]$, qui n'est pas un corps.

2) Soit $\mathfrak{a}$ un idéal de A , $\mathfrak{p}$ un idéal premier de A , contenant $\mathfrak{a}$; dans l'anneau quotient $A/\mathfrak{a}$, l'idéal $\mathfrak{p}/\mathfrak{a}$ est premier, puisque l'anneau quotient $(A/\mathfrak{a})/(\mathfrak{p}/\mathfrak{a})$ est isomorphe à $A/\mathfrak{p}$.

Il résulte aussitôt de la déf.2, par récurrence sur n, que les relations $a_i \notin \mathfrak{p}$ $(1 \leqslant i \leqslant n)$ entraînent $a_1 a_2 \dots a_n \notin \mathfrak{p}$; en particulier, la relation $a \notin \mathfrak{p}$ entraîne $a^n \notin \mathfrak{p}$ pour tout entier $n > 0$.

PROPOSITION 4.- Soient $\mathfrak{p}$ un idéal premier, $\mathfrak{a}$ et $\mathfrak{b}$ deux idéaux dans A ; les relations $\mathfrak{a} \not\subset \mathfrak{p}$ et $\mathfrak{b} \not\subset \mathfrak{p}$ entraînent $\mathfrak{a}\mathfrak{b} \not\subset \mathfrak{p}$.

En effet, il existe $a \in \mathfrak{a}$ et $b \in \mathfrak{b}$ tels que $a \notin \mathfrak{p}$ et $b \in \mathfrak{p}$; on a donc $ab \notin \mathfrak{p}$, et par suite $\mathfrak{a}\mathfrak{b} \not\subset \mathfrak{p}$.

Ceci montre que dans le monoïde semi-réticulé supérieurement $\mathfrak{J}$ des idéaux de A , les idéaux premiers sont les éléments premiers au sens du § 1, n° 10, déf.8 .

PROPOSITION 5.- Soit $\mathfrak{a}$ un idéal quelconque dans un anneau commutatif A ; l'ensemble des éléments $x \in A$ tels que, pour un entier $n > 0$ (dépendant de x) on ait $x^n \in \mathfrak{a}$, est un idéal $\mathfrak{b}$.

En effet si $x^m \in \mathfrak{a}$ et $y^n \in \mathfrak{a}$, on a $(x-y)^{m+n-1} \in \mathfrak{a}$, car dans un terme $x^p y^{m+n-p-1}$, on a nécessairement $p \geqslant m$ ou $m+n-p-1 \geqslant n$; d'autre part, il est évident que si $x^m \in \mathfrak{a}$ on a aussi $(zx)^m \in \mathfrak{a}$ pour tout $z \in A$, d'où la proposition.

L'idéal $\mathfrak{b}$ est appelé le radical de $\mathfrak{a}$ et noté Rad $\mathfrak{a}$. On a évidemment $\mathfrak{a} \subset$ Rad $\mathfrak{a}$, et Rad(Rad $\mathfrak{a}$)=Rad $\mathfrak{a}$; la relation $\mathfrak{a} \subset \mathfrak{b}$ entraîne Rad $\mathfrak{a} \subset$ Rad $\mathfrak{b}$. D'après ce qui a été vu plus haut, pour tout idéal premier $\mathfrak{p}$, on a Rad $\mathfrak{p} = \mathfrak{p}$.

PROPOSITION 6.- Quels que soient les idéaux $\mathfrak{a}$, $\mathfrak{b}$ dans A , on a

(2) $$\text{Rad}(\mathfrak{a}\mathfrak{b}) = \text{Rad}(\mathfrak{a} \cap \mathfrak{b}) = (\text{Rad}\ \mathfrak{a}) \cap (\text{Rad}\ \mathfrak{b}).$$

On a évidemment $\mathrm{Rad}(\mathfrak{a}\mathfrak{b}) \subset \mathrm{Rad}(\mathfrak{a} \cap \mathfrak{b})$, et d'autre part la définition du radical prouve que $\mathrm{Rad}(\mathfrak{a} \cap \mathfrak{b}) \subset (\mathrm{Rad}\ \mathfrak{a}) \cap (\mathrm{Rad}\ \mathfrak{b})$. D'autre part, si $x^m \in \mathfrak{a}$ et $x^n \in \mathfrak{b}$, on a $x^{m+n} \in \mathfrak{a}\mathfrak{b}$, donc $(\mathrm{Rad}\ \mathfrak{a}) \cap (\mathrm{Rad}\ \mathfrak{b}) \subset \mathrm{Rad}(\mathfrak{a}\mathfrak{b})$, ce qui achève la démonstration.

COROLLAIRE.- Pour tout idéal premier $\mathfrak{p}$, on a $\mathrm{Rad}(\mathfrak{p}^n) = \mathfrak{p}$.

Exemple.- Dans un anneau principal, le radical de tout idéal $\mathfrak{a} = \prod_\nu \mathfrak{p}_\nu^{n_\nu}$ est égal d'après la prop.6 au produit des idéaux premiers $\mathfrak{p}_\nu$ pour lesquels $n_\nu > 0$.

PROPOSITION 7.- Soit A un anneau noethérien. Pour tout idéal $\mathfrak{a}$ de A, il existe un entier $n > 0$ tel que $(\mathrm{Rad}\ \mathfrak{a})^n \subset \mathfrak{a}$.

En effet, soit $(a_i)_{1 \leqslant i \leqslant p}$ un système de générateurs de $\mathrm{Rad}\ \mathfrak{a}$; pour tout indice i $(1 \leqslant i \leqslant p)$ il existe un entier $n_i > 0$ tel que $a_i^{n_i} \in \mathfrak{a}$. Soit $n = \sum_{i=1}^{p} n_i$; pour tout $x \in \mathrm{Rad}\ \mathfrak{a}$, il existe p éléments $b_i \in A$ tels que $x = \sum_{i=1}^{p} b_i a_i$. Soient alors $x_j = \sum_{i=1}^{p} b_{ij} a_i$ n éléments quelconques de $\mathrm{Rad}\ \mathfrak{a}$; le produit $x_1 x_2 \ldots x_n$ est somme de termes de la forme $c \prod_{i=1}^{p} a_i^{\nu_i}$, où $c \in A$ et $\sum_{i=1}^{p} \nu_i = n = \sum_{i=1}^{p} n_i$; il existe donc pour chacun de ces termes un indice i tel que $\nu_i \geqslant n_i$, ce qui montre que $x_1 x_2 \ldots x_n$ appartient à $\mathfrak{a}$, et par suite que $(\mathrm{Rad}\ \mathfrak{a})^n \subset \mathfrak{a}$.

On notera que cette proposition n'est plus exacte si on ne suppose plus que A soit noethérien. Prenons par exemple pour A l'anneau $K[X_n]_{n \in \mathbb{N}}$ des polynomes à une infinité dénombrable d'indéterminées sur un corps K, pour $\mathfrak{a}$ l'idéal engendré par les éléments X_n^n $(n \in \mathbb{N})$. Il est immédiat que $\mathrm{Rad}\ \mathfrak{a}$ est l'idéal engendré par les X_n (idéal des polynomes sans terme constant), comme on le voit par un raisonnement analogue à celui de la prop.7 ; mais pour tout entier n, on a $(\mathrm{Rad}\ \mathfrak{a})^n \not\subset \mathfrak{a}$, car le polynome X_{n+1}^n n'appartient pas à l'idéal $\mathfrak{a}$.

5. Idéaux primaires.

DÉFINITION 3.- Dans un anneau commutatif A ayant un élément unité on dit qu'un idéal $\mathfrak{q}$ est primaire si, dans l'anneau quotient $A/\mathfrak{q}$, tout diviseur de 0 est nilpotent (c'est-à-dire a une de ses puissances nulles)

En d'autres termes, les relations $xy \in \mathfrak{q}$, $y \notin \mathfrak{q}$ entraînent qu'il existe un entier $n > 0$ tel que $x^n \in \mathfrak{q}$; on peut aussi dire que les relations $xy \in \mathfrak{q}$, $y \notin \mathfrak{q}$ entraînent $x \in \mathrm{Rad}\,\mathfrak{q}$. Tout idéal premier est évidemment primaire.

Exemple.- Dans un anneau principal A, pour que la relation $xy \in (q)$ entraîne $y \in (q)$ ou $x^n \in (q)$ pour un entier n au moins il faut et il suffit que q ne soit divisible que par un seul élément premier, autrement dit que $q = p^r$ (p premier, r entier > 0) ; en effet, si on avait $q = p_1^h p_2^k$, on aurait $xy \in (q)$ en prenant $x = p_1^h$, $y = p_2^k$, mais x^n ni y^n n'appartiennent à (q) pour aucun entier n. En d'autres termes, les idéaux primaires sont dans ce cas les puissances d'idéaux premiers.

PROPOSITION 8.- Le radical d'un idéal primaire est premier.

Soit $\mathfrak{q}$ un idéal primaire, $\mathfrak{P} = \mathrm{Rad}\,\mathfrak{q}$. Si $xy \in \mathfrak{P}$, il existe un entier $n > 0$ tel que $x^n y^n \in \mathfrak{q}$; si $x^n \in \mathfrak{q}$, on a $x \in \mathfrak{P}$ par définition ; si au contraire $x^n \notin \mathfrak{q}$, il existe un entier $m > 0$ tel que $y^{mn} \in \mathfrak{q}$ et par suite $y \in \mathfrak{P}$, ce qui achève la démonstration.

Remarques.- 1) La réciproque de la prop.8 est inexacte : un idéal peut avoir un radical premier sans être primaire. Prenons par exemple pour A le sous-anneau de l'anneau $\mathbb{Z}[X]$ des polynomes à une indéterminée à coefficients entiers, formé des polynomes $\sum a_n X^n$ tels que $a_1 \equiv 0 \pmod 3$. Dans cet anneau, l'idéal $\mathfrak{P} = (3X) + (X^2)$ est formé de tous les polynomes sans terme constant ; donc $A/\mathfrak{P}$ est isomorphe à $\mathbb{Z}$ et par suite $\mathfrak{P}$ est premier.

Considérons alors l'idéal $\mathfrak{a} = \mathfrak{P}^2 = (9X^2)+(3X^3)+(X^4)$; son radical est $\mathfrak{P}$ (cor. de la prop.6), mais il n'est pas primaire, car on a $9X^2 \in \mathfrak{a}$ et $9 \notin \mathfrak{P}$, $X^2 \notin \mathfrak{a}$. (et exemple prouve en même temps qu'une puissance d'un idéal premier n'est pas nécessairement primaire.

2) D'autre part, un idéal primaire n'est pas nécessairement une puissance d'un idéal prmier. Par exemple, dans l'anneau $\mathbb{Z}[X]$, l'idéal $\mathfrak{q} = (4)+(X)$ est primaire, car $\mathbb{Z}[X]/\mathfrak{q}$ est isomorphe à $\mathbb{Z}/(4)$, où la classe du nombre 2 est le seul diviseur de 0 et est nilpotente ; le seul idéal distinct de $\mathbb{Z}/(4)$, le seul idéal distinct de $\mathbb{Z}[X]$ et de $\mathfrak{q}$ et contenant $\mathfrak{q}$ dans l'anneau $\mathbb{Z}[X]$ est l'idéal maximal $\mathfrak{P} = (2)+(X)$, qui est évidemment le radical de $\mathfrak{q}$; mais X n'appartient à aucune puissance $\mathfrak{P}^k$, où $k > 1$, et par suite $\mathfrak{q}$ n'est égal à aucune de ces puissances.

PROPOSITION 9.- Soient $\mathfrak{q}$ un idéal primaire, $\mathfrak{a}$ et $\mathfrak{b}$ deux idéaux dans A ; les relations $\mathfrak{a}\mathfrak{b} \subset \mathfrak{q}$ et $\mathfrak{a} \not\subset \mathfrak{q}$ entraînent $\mathfrak{b} \subset \mathrm{Rad}\,\mathfrak{q} = \mathfrak{P}$.

En effet, si on avait $\mathfrak{b} \not\subset \mathfrak{P}$, il existerait $y \in \mathfrak{b}$ tel que $y \notin \mathfrak{P}$.

Comme d'autre part il existe $x \in \mathfrak{a}$ tel que $x \notin \mathfrak{q}$, on aurait $xy \in \mathfrak{a}\mathfrak{b} \subset \mathfrak{q}$, contrairement à l'hypothèse que $\mathfrak{q}$ est primaire.

COROLLAIRE 1.- Si $\mathfrak{q}$ est primaire, la relation $\mathfrak{a}^n \subset \mathfrak{q}$ entraîne $\mathfrak{a} \subset \mathrm{Rad}\,\mathfrak{q}$.

C'est une conséquence de la prop.9 , par récurrence sur n .

COROLLAIRE 2.- Si $\mathfrak{q}$ est primaire, et $\mathfrak{b} \not\subset \mathrm{Rad}\,\mathfrak{q}$, on a $\mathfrak{q} : \mathfrak{b} = \mathfrak{q}$.

En effet, on a $\mathfrak{b}.(\mathfrak{q} : \mathfrak{b}) \subset \mathfrak{q}$; comme $\mathfrak{b} \not\subset \mathrm{Rad}\,\mathfrak{q}$, la prop.9 montre que $\mathfrak{q} : \mathfrak{b} \subset \mathfrak{q}$; mais on a l'autre part $\mathfrak{q} : \mathfrak{b} \supset \mathfrak{q}$, d'où le corollaire.

6. Intersections d'idéaux primaires.

PROPOSITION 10.- *Si* $(\mathfrak{q}_i)_{1\leqslant i\leqslant n}$ *est une famille finie d'idéaux primaires ayant tous même radical* $\mathfrak{P}$, *l'intersection* $\mathfrak{q} = \bigcap_{i=1}^{n} \mathfrak{q}_i$ *est un idéal primaire ayant pour radical* $\mathfrak{P}$.

En effet, $\mathfrak{P}$ est le radical de $\mathfrak{q}$ (prop.6) ; si $xy \in \mathfrak{q}$, et $x \notin \mathfrak{q}$ il existe un indice i tel que $x \notin \mathfrak{q}_i$; alors comme $xy \in \mathfrak{q}_i$, on a $y \in \mathfrak{P}$, d'où la proposition.

Il suit de la prop.10 que si $(\mathfrak{q}_i)_{1\leqslant i\leqslant n}$ est une famille finie quelconque d'idéaux primaires, il existe une famille finie $(\mathfrak{q}'_j)$ d'idéaux primaires dont les radicaux sont *deux à deux distincts*, tels que $\bigcap_i \mathfrak{q}_i = \bigcap_j \mathfrak{q}'_j$; en effet, soient $\mathfrak{P}_j$ $(1\leqslant j\leqslant p)$ les radicaux distincts des $\mathfrak{q}_i$, et soit H_j l'ensemble des indices i tels que $\operatorname{Rad}\mathfrak{q}_i = \mathfrak{P}_j$; il suffit de prendre $\mathfrak{q}'_j = \bigcap_{i\in H_j} \mathfrak{q}_i$, d'après la prop.1.

Nous dirons qu'une famille finie $(\mathfrak{q}_i)_{1\leqslant i\leqslant n}$ d'idéaux primaires est *réduite* si les radicaux des $\mathfrak{q}_i$ sont deux à deux distincts, et si l'intersection de n-1 quelconques des $\mathfrak{q}_i$ est distincte de $\bigcap_{i=1}^{n} \mathfrak{q}_i$. Ce qui précède prouve que toute intersection d'une famille finie quelconque d'idéaux primaires est aussi l'intersection d'une famille *réduite* d'idéaux primaires.

PROPOSITION 11.- *Si* $(\mathfrak{q}_i)_{1\leqslant i\leqslant n}$ *est une famille réduite d'idéaux primaires telle que* $n > 1$, *l'idéal* $\mathfrak{q} = \bigcap_{i=1}^{n} \mathfrak{q}_i$ *n'est pas primaire.*

En effet, soient $\mathfrak{P}_i = \operatorname{Rad}\mathfrak{q}_i$ les radicaux des $\mathfrak{q}_i$ $(1\leqslant i\leqslant n)$; soit k tel que $\mathfrak{P}_k$ soit minimal dans l'ensemble des $\mathfrak{P}_i$. Pour $i\neq k$, on a donc $\mathfrak{P}_i \not\subset \mathfrak{P}_k$, et par suite il existe $a_i \in \mathfrak{P}_i$ tel que $a_i \notin \mathfrak{P}_k$. Par définition, il existe un entier r_i tel que $a_i^{r_i} \in \mathfrak{q}_i$; si r est le plus grand des r_i , on a donc $a_i^r \in \mathfrak{q}_i$ pour $i\neq k$. D'autre part, comme la famille $(\mathfrak{q}_i)$ est réduite, on a $\mathfrak{q} \neq \mathfrak{q}_k$, donc il existe un élément $b_k \in \mathfrak{q}_k$ tel que $b_k \notin \mathfrak{q}$. L'élément $x = b_k(\prod_{i\neq k} a_i)^r$

appartient à $\mathfrak{q}_k$ et à chacun des $\mathfrak{q}_i$ d'indice $i=k$, donc à par définition ; si était primaire, comme on a $b_k \notin \mathfrak{q}$ il existerait un entier s tel que $(\prod_{i\neq k} a_i)^{rs} \in \mathfrak{q} \subset \mathfrak{q}_k$, et par suite $\prod_{i\neq k} a_i \in \mathfrak{P}_k$; mais comme $\mathfrak{P}_k$ est premier, cela entraînerait $a_i \in \mathfrak{P}_k$ pour au moins un indice $i\neq k$, ce qui est absurde.

THÉORÈME 2.- *Si $(\mathfrak{q}_i)_{1\leqslant i\leqslant m}$ et $(\mathfrak{q}'_j)_{1\leqslant j\leqslant n}$ sont deux familles réduites d'idéaux primaires telles que $\bigcap_i \mathfrak{q}_i = \bigcap_j \mathfrak{q}'_j$, on a $m=n$, et il existe une permutation σ de $[1,n]$ telle que* $\operatorname{Rad} \mathfrak{q}_i = \operatorname{Rad} \mathfrak{q}'_{\sigma(i)}$ *pour* $1\leqslant i\leqslant n$.

Posons $\mathfrak{a} = \bigcap_i \mathfrak{q}_i = \bigcap_j \mathfrak{q}'_j$, $\mathfrak{P}_i = \operatorname{Rad} \mathfrak{q}_i$, $\mathfrak{P}'_j = \operatorname{Rad} \mathfrak{q}'_j$. Considérons parmi les $m+n$ idéaux premiers $\mathfrak{P}_i$, $\mathfrak{P}'_j$, un élément maximal (pour la relation d'inclusion) ; nous pouvons supposer par exemple que $\mathfrak{P}_1$ est un tel idéal (en faisant au besoin une permutation sur l'ensemble des indices). Montrons d'abord qu'il existe alors un indice j tel que $\mathfrak{P}'_j = \mathfrak{P}_1$. Raisonnons par l'absurde ; on peut écrire, d'après la prop.3

$$\bigcap_{i=1}^{m} (\mathfrak{q}_i : \mathfrak{q}_1) = \bigcap_{j=1}^{n} (\mathfrak{q}'_j : \mathfrak{q}_1) = \mathfrak{a} : \mathfrak{q}_1 \tag{3}$$

Mais par hypothèse, on aurait $\mathfrak{q}_1 \not\subset \operatorname{Rad} \mathfrak{q}'_j = \mathfrak{P}'_j$ pour $1\leqslant j\leqslant n$, car de la relation $\mathfrak{q}_1 \subset \operatorname{Rad} \mathfrak{q}'_j$ on tire $\mathfrak{P}_1 = \operatorname{Rad} \mathfrak{q}_1 \subset \operatorname{Rad} \mathfrak{q}'_j = \mathfrak{P}'_j$, et d'après le choix de $\mathfrak{P}_1$, cela ne serait possible que si $\mathfrak{P}'_j = \mathfrak{P}_1$, contrairement à l'hypothèse. Le cor.2 de la prop.9 montre donc qu'on aurait $\mathfrak{q}'_j : \mathfrak{q}_1 = \mathfrak{q}'_j$, et par suite $\mathfrak{a} : \mathfrak{q}_1 = \mathfrak{a}$. Mais de la même manière on voit que $\mathfrak{q}_i : \mathfrak{q}_1 = \mathfrak{q}_i$ pour $i \geqslant 2$, et comme $\mathfrak{q}_1 : \mathfrak{q}_1 = A$, on aurait, d'après (3), $\mathfrak{a} = \bigcap_{i=2}^{m} \mathfrak{q}_i$, contrairement au fait que $(\mathfrak{q}_i)_{1\leqslant i\leqslant m}$ est supposée réduite.

On peut donc supposer, en faisant au besoin une permutation sur l'ensemble des indices j, que l'on a $\mathfrak{P}'_1 = \mathfrak{P}_1$. Alors, posons $\mathfrak{b} = \mathfrak{q}_1 \cap \mathfrak{q}'_1$; on a

(4) $\bigcap_{i=1}^{m} (\mathfrak{q}_i : \mathfrak{b}) = \bigcap_{j=1}^{n} (\mathfrak{q}'_j : \mathfrak{b})$

Comme $\mathfrak{b} \subset \mathfrak{q}_1$, on a $\mathfrak{q}_1 : \mathfrak{b} = A$, et de même $\mathfrak{q}'_1 : \mathfrak{b} = A$; d'autre part, le même raisonnement que ci-dessus prouve que $\mathfrak{q}_i : \mathfrak{b} = \mathfrak{q}_i$ et $\mathfrak{q}'_j : \mathfrak{b} = \mathfrak{q}'_j$ pour $i \geqslant 2$ et $j \geqslant 2$, car $\mathfrak{b}$ est primaire et a pour radical $\mathfrak{p}_1$ (prop.10). La relation (4) s'écrit donc

(5) $\bigcap_{i=2}^{m} \mathfrak{q}_i = \bigcap_{j=2}^{n} \mathfrak{q}'_j$

Pour achever la démonstration, il suffit de raisonner par récurrence sur m. Le théorème est vrai pour m=1 d'après la prop.11. D'autre part, l'hypothèse de récurrence, appliquée à la relation (5), montre (puisque toute sous-famille d'une famille réduite d'idéaux primaires est réduite) qu'on a $m-1=n-1$, donc $m=n$, et qu'il existe une permutation ρ de $[2,n]$ telle que $\mathfrak{p}'_{\rho(i)} = \mathfrak{p}_i$ pour $2 \leqslant i \leqslant n$.

On notera que les deux familles $(\mathfrak{q}_i)$ et $(\mathfrak{q}'_j)$ peuvent être formées d'idéaux primaires différents. Par exemple, dans l'anneau $K[X,Y]$ (K corps), soit $\mathfrak{a} = (X^2) \cap (XY)$; si on pose $\mathfrak{q}_1 = (X)$, $\mathfrak{q}_2 = (X^2) + (XY) + (Y^2)$, $\mathfrak{q}_3 = (X^2) + (1)$, $\mathfrak{q}_1$ est premier, on voit aussitôt que $\mathfrak{q}_2$ et $\mathfrak{q}_3$ sont primaires et ont pour radical l'idéal maximal $(X)+(Y)$; or, on a à la fois $\mathfrak{a} = \mathfrak{q}_1 \cap \mathfrak{q}_2 = \mathfrak{q}_1 \cap \mathfrak{q}_3$.

7. Le théorème de Lasker-E.Noether.

THÉORÈME 3. (Lasker-Noether).- Dans un anneau noetherien (ayant un élément unité) tout idéal est intersection d'un nombre fini d'idéaux primaires.

Nous dirons qu'un idéal $\mathfrak{a}$ est irréductible si la relation $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$ entraîne $\mathfrak{a} = \mathfrak{b}$ ou $\mathfrak{a} = \mathfrak{c}$, réductible dans le cas contraire.

1° Dans un anneau noethérien, tout idéal est intersection d'un nombre fini d'idéaux irréductibles.

Raisonnons par l'absurde et supposons que l'ensemble $\mathfrak{M}$ des idéaux pour lesquels la proposition est fausse ne soit pas vide ; il existe alors dans $\mathfrak{M}$ un élément maximal $\mathfrak{a}$. Par hypothèse, $\mathfrak{a}$ ne peut être irréductible ; on a donc $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$, où $\mathfrak{a} \neq \mathfrak{b}$ et $\mathfrak{a} = \mathfrak{c}$; il s'ensuit que $\mathfrak{b}$ ni $\mathfrak{c}$ ne peuvent appartenir à $\mathfrak{M}$, et par suite que chacun d'eux est intersection d'un nombre fini d'idéaux irréductibles. Mais alors il en est de même de $\mathfrak{a}$, ce qui est absurde.

2° Dans un anneau noetherien, tout idéal irréductible est primaire.

Nous démontrerons cette proposition en prouvant qu'un idéal non primaire $\mathfrak{a}$ est réductible. Par hypothèse il existe deux éléments a,b tels que $ab \in \mathfrak{a}$, $a \notin \mathfrak{a}$ et $b^r \notin \mathfrak{a}$ pour tout entier $r > 0$. La suite des idéaux $\mathfrak{a} : (b^k)$ est croissante, donc il existe un indice n tel que $\mathfrak{a} : (b^n) = \mathfrak{a} : (b^{n+1})$. Posons $\mathfrak{b} = \mathfrak{a} + (a)$, $\mathfrak{c} = \mathfrak{a} + (b^n)$; on a évidemment $\mathfrak{a} \subset \mathfrak{b}$, $\mathfrak{a} \subset \mathfrak{c}$ et $\mathfrak{a} \neq \mathfrak{b}$, $\mathfrak{a} \neq \mathfrak{c}$; nous allons prouver que $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$, ce qui montrera que $\mathfrak{a}$ est réductible. En effet, soit c un élément de $\mathfrak{b} \cap \mathfrak{c}$; on peut écrire, puisque $c \in \mathfrak{a} + (b^n)$, $c = x + yb^n$, avec $x \in \mathfrak{a}$, $y \in A$. Comme $c \in \mathfrak{a} + (a)$, on a d'autre part $bc \in \mathfrak{a} + (ab) \subset \mathfrak{a}$ ce qui s'écrit $bx + yb^{n+1} \in \mathfrak{a}$, et entraîne donc $yb^{n+1} \in \mathfrak{a}$. Mais comme $\mathfrak{a} : (b^{n+1}) = \mathfrak{a} : (b^n)$, on a aussi $yb^n \in \mathfrak{a}$, donc $c \in \mathfrak{a}$. C.Q.F.D.

Pour tout idéal $\mathfrak{a}$ d'un anneau noethérien A, il existe donc une famille <u>réduite</u> $(\mathfrak{q}_i)_{1 \leqslant i \leqslant n}$ d'idéaux primaires telles que $\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i$; le th.2 montre que le nombre n d'idéaux de cette famille, et les radicaux des $\mathfrak{q}_i$ sont déterminés de façon <u>unique</u> par l'idéal $\mathfrak{a}$. On dit que les $\mathfrak{q}_i$ forment une famille de <u>composantes primaires</u> de $\mathfrak{a}$, et que leurs radicaux $\mathfrak{p}_i$ sont les idéaux premiers <u>associés à</u> $\mathfrak{a}$.

COROLLAIRE.- <u>Dans un anneau noetherien, pour tout idéal</u> $\mathfrak{a}$, Rad $\mathfrak{a}$ <u>peut s'écrire d'une manière et d'une seule comme intersection d'un nombre fini d'idéaux premiers</u>.

En effet, si $\mathfrak{P}_i$ $(1 \leqslant i \leqslant n)$ sont les idéaux premiers associés à $\mathfrak{a}$, on a Rad $\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{P}_i$ d'après le th.3 et la prop.6 ; l'unicité de l'expression de Rad $\mathfrak{a}$ comme l'intersection d'idéaux premiers résulte du th.2.

8. Le théorème de Krull.

PROPOSITION 12.- Soient $\mathfrak{a}$ et $\mathfrak{b}$ deux idéaux dans un anneau noethérien A. Il existe un idéal $\mathfrak{a}'$ et un entier $r > 0$ tels que $\mathfrak{a}\mathfrak{b} = \mathfrak{a}' \cap \mathfrak{b}$ et $\mathfrak{a}' \supset \mathfrak{a}^r$.

Considérons une famille de composantes primaires de $\mathfrak{a}\mathfrak{b}$; désignons par $\mathfrak{q}_i$ $(1 \leqslant i \leqslant m)$ celles de ces composantes telles que $\mathfrak{a} \subset \mathrm{Rad}\ \mathfrak{q}_i$, par $\mathfrak{q}'_j$ $(1 \leqslant j \leqslant n)$ les autres. On a donc $\mathfrak{a}\mathfrak{b} = \mathfrak{a}' \cap \mathfrak{b}_1$ avec $\mathfrak{a}' = \bigcap_i \mathfrak{q}_i$ et $\mathfrak{b}_1 = \bigcap_j \mathfrak{q}'_j$. Il existe (prop.7) un entier $r > 0$ tel que $(\mathrm{Rad}\ \mathfrak{q}_i)^r \subset \mathfrak{q}_i$ pour $1 \leqslant i \leqslant m$, et par suite $\mathfrak{a}^r \subset \mathfrak{a}'$. D'autre part, comme $\mathfrak{a} \not\subset \mathrm{Rad}\ \mathfrak{q}'_j$, il existe $x \in \mathfrak{a}$ tel que $x \notin \mathrm{Rad}\ \mathfrak{q}'_j$; comme $x\mathfrak{b} \subset \mathfrak{a}\mathfrak{b} \subset \mathfrak{q}'_j$, on a nécessairement $\mathfrak{b} \subset \mathfrak{q}'_j$ $(1 \leqslant j \leqslant n)$, et par suite $\mathfrak{b} \subset \mathfrak{b}_1$. Cela étant, on peut écrire $\mathfrak{a}\mathfrak{b} = (\mathfrak{a}\mathfrak{b}) \cap \mathfrak{b} = (\mathfrak{a}' \cap \mathfrak{b}_1) \cap \mathfrak{b} = \mathfrak{a}' \cap \mathfrak{b}$, ce qui établit la proposition.

THÉORÈME 4 (Krull).- Soit $\mathfrak{a}$ un idéal d'un anneau noetherien A, distinct de A ; pour que $\bigcap_{n \in N} \mathfrak{a}^n = (0)$, il faut et il suffit qu'il n'existe dans A aucun diviseur de zéro congru à 1 modulo $\mathfrak{a}$.

La condition est nécessaire ; en effet, supposons qu'il existe deux éléments b,c de A tels que $b \neq 0$, $c \neq 0$, $bc = 0$ et $a = 1 - b \in \mathfrak{a}$. On a donc $ac = c - bc = 0$, d'où par récurrence sur n, $a^n c = c \neq 0$. Comme $a^n \in \mathfrak{a}^n$, on a donc $c \in \mathfrak{a}^n$ quel que soit n, ou encore $c \in \bigcap_n \mathfrak{a}^n$.

La condition est suffisante. Soit en effet $\mathfrak{b} = \bigcap_{n \in N} \mathfrak{a}^n$; on a évidemment $\mathfrak{b} = \mathfrak{a}^n \cap \mathfrak{b}$ pour tout entier n. D'après la prop.12, il existe un idéal $\mathfrak{a}'$ et un entier $r > 0$ tels que $\mathfrak{a}' \supset \mathfrak{a}^r$,

et $\mathfrak{a}\mathfrak{b} = \mathfrak{a}' \cap \mathfrak{b}$, d'où $\mathfrak{a}\mathfrak{b} \supset \mathfrak{a}^2 \cap \mathfrak{b}$. Autrement dit, on a $\mathfrak{b} \subset \mathfrak{a}\mathfrak{b}$. Nous allons en déduire que, s'il n'existe aucun diviseur de 0 congru à 1 modulo $\mathfrak{a}$, on a $\mathfrak{b} = 0$. En effet, soit $(b_i)_{1 \leqslant i \leqslant n}$ un système de générateurs de l'idéal $\mathfrak{b}$; de la relation $\mathfrak{b} \subset \mathfrak{a}\mathfrak{b}$, on déduit que, pour $1 \leqslant i \leqslant n$, on a

$$(6) \qquad b_i = \sum_{j=1}^{n} a_{ij} b_j$$

où $a_{ij} \in \mathfrak{a}$ pour $1 \leqslant i \leqslant n$, $1 \leqslant j \leqslant n$. Les relations (6) peuvent encore s'écrire (7) $\sum_{j=1}^{n} (\delta_{ij} - a_{ij}) b_j = 0$ $(1 \leqslant i \leqslant n)$, où δ_{ij} est l'indice de Kronecker. Soit $\Delta = \det(\delta_{ij} - a_{ij})$, et soit Δ_{ij} le cofacteur de $\delta_{ij} - a_{ij}$ dans Δ ; multipliant chacune des relations (7) par Δ_{ih} et ajoutant membre à membre les n relations obtenues, il vient $\Delta . b_h = 0$ $(1 \leqslant h \leqslant n)$. Or, on a évidemment $\Delta \equiv 1 \pmod{\mathfrak{a}}$; on a donc $\Delta \neq 0$, sans quoi on aurait $1 \in \mathfrak{a}$, ou $\mathfrak{a} = A$, contrairement à l'hypothèse ; d'autre part, si $\mathfrak{b} \neq (0)$ les b_h ne sont pas tous nuls, donc Δ serait un diviseur de 0 , ce qui est contraire à l'hypothèse. Le théorème est ainsi démontré.

COROLLAIRE.- Dans un anneau d'intégrité noethérien A , pour tout idéal $\mathfrak{a} \neq A$, on a $\bigcap_{n \in \mathbb{N}} \mathfrak{a}^n = (0)$.
