MÉMOIRES DE LA S. M. F.

M.-P. MALLIAVIN-BRAMERET

Largeurs d'anneaux et de modules

Mémoires de la S. M. F., tome 8 (1966)

<http://www.numdam.org/item?id=MSMF_1966__8__3_0>

Bull. Soc. math. France,
Mémoire 8, 1966, 76 p.

LARGEURS D'ANNEAUX ET DE MODULES

par Marie-Paule MALLIAVIN-BRAMERET (*)

-:-:-

TABLE DES MATIERES

(*) Thèse Sciences math., Paris 1965

CHAPITRE IV

Groupes p-réduits

-:-:-:-

INTRODUCTION

Dans la conférence qu'il a donnée au Colloque de Bruxelles, en 1956, M. Paul DUBREIL a caractérisé les anneaux, commutatifs, unitaires, dont le treillis des idéaux est totalement ordonné, comme étant les anneaux dans lesquels tout idéal du demi-groupe multiplicatif est un idéal de l'anneau : nous généralisons ce résultat dans le Chapitre I de ce travail. Nous introduisons d'abord la notion de largeur d'un module à gauche M sur un anneau A, non nécessairement commutatif : la largeur de M, lorsqu'elle est finie, est le plus petit entier n tel que tout sous-module de M, engendré par une famille finie d'éléments, puisse être engendré par n éléments de cette famille. Nous définissons, d'autre part, pour chaque entier $n > 0$ une application $\int_n$ de l'ensemble ordonné des parties de M qui sont multiplicativement stables par A, dans lui-même, en associant à toute partie I de M, multiplicativement stable par A, l'ensemble des sommes de n éléments de I. Alors la largeur de M est égale à n si et seulement si l'image de $\int_n$ est le treillis des sous-A-modules de M.

La largeur gauche (resp. droite) d'un anneau A est définie comme étant la largeur du module à gauche (resp. à droite) A_s (resp. A_d).

La notion de largeur peut être définie dans un treillis T : la largeur de T, lorsque celle-ci est finie, est le plus petit entier n tel que, dans tout système de $n+1$ éléments de T, l'un d'entre eux est inférieur à la borne supérieure des n autres. Alors la largeur d'un module à gauche M sur un anneau A est la largeur du treillis des sous-modules de M. La largeur (bilatère) d'un anneau A, non nécessairement unitaire, est définie comme la largeur du treillis de ses idéaux bilatères. Si, pour tout idéal bilatère I du demi-groupe multiplicatif d'un anneau unitaire A, l'ensemble des sommes de n éléments de I est un idéal de A, alors la largeur de A est inférieure à n. Mais, dans le cas "bilatère", on ne peut établir la réciproque de ce résultat qu'en imposant à A des hypothèses supplémentaires.

La majeure partie du Chapitre I est consacrée à l'étude de la notion de largeur dans la catégorie des anneaux commutatifs et, plus particulièrement, dans la catégorie $\mathcal{L}$ des anneaux locaux noethériens.

La largeur d'un anneau A, commutatif, intègre et intégralement clos, est égale à n si et seulement si A est l'intersection de n anneaux de valuation de son corps des quotients. Soit A un anneau commutatif, intègre, de largeur n ; alors, quel que soit l'élément x du corps des quotients de A, entier sur A, x est racine d'un polynôme unitaire à coefficients dans A <u>de degré inférieur à</u> n .

Un anneau A de la catégorie $\mathcal{L}$ est de largeur finie si et seulement si son rang est fini ; alors la largeur et le rang de A coïncident. La notion de rang d'un anneau commutatif est celle de I. S. COHEN : un anneau commutatif A est de rang inférieur à k , si tout idéal de A possède un système de générateurs de k éléments. I. S. COHEN a remarqué qu'un anneau de rang fini est de dimension au plus égale à 1 , la dimension étant prise au sens de KRULL. Nous démontrons ici la réciproque de cette proposition, ce qui permet d'associer <u>à tout anneau local commutatif noethérien, de dimension</u> $\leqslant 1$, <u>un entier strictement positif, à savoir sa largeur</u>. Pour démontrer ce résultat, nous utilisons essentiellement le fait que la largeur d'un anneau A de la catégorie $\mathcal{L}$ est égale à la largeur du complété de A pour la topologie m(A)-adique, où m(A) désigne l'idéal maximal de A . L'étude d'un anneau complet de dimension au plus 1 est décomposée ensuite selon les trois cas suivants : celui d'un anneau d'égales caractéristiques ; celui d'un anneau d'inégales caractéristiques dont aucun idéal premier minimal ne contient p.1 (p étant la caractéristique du corps résiduel de l'anneau et 1 l'élément unité de l'anneau) ; enfin, celui d'un anneau dont la caractéristique est une puissance d'un nombre premier.

La multiplicité d'un anneau de la catégorie $\mathcal{L}$, de dimension 1 , est inférieure à sa largeur. Moyennant des hypothèses assez fortes sur l'anneau, on prouve l'égalité de ces deux quantités. Ces hypothèses reposent sur l'existence d'éléments superficiels d'ordre 1 pour l'idéal maximal de l'anneau et sur le fait que l'idéal maximal n'est pas un idéal premier de (0). Il existe des cas où la multiplicité de l'anneau est strictement inférieure à sa largeur.

Nous étudions, au Chapitre II, quelques propriétés des anneaux unitaires dont la largeur gauche est égale à 1. Un tel anneau A , s'il est complètement premier, possède un corps des quotients à gauche. Contrairement à ce qui se passe pour les anneaux commutatifs, la largeur gauche du A-module K n'est pas toujours égale à 1. Lorsque la largeur gauche du A-module K est égale à 1, alors K est aussi corps des quotients à droite de A et la largeur droite de l'anneau A est égale à 1. Plus précisément, les conditions suivantes sont équivalentes : d'une part K est un A-module à gauche de largeur 1, d'autre part A est régulier à droite (i.e. A possède un corps des quotients à droite), enfin la largeur droite de A est égale à 1. Tout sur-anneau d'un anneau de valuation V , au sens de O. SCHILLING, d'un corps gauche K vérifie ces conditions. Nous terminons le Chapitre II en donnant des exemples, tirés de la théorie des groupes finis, d'anneaux noethériens à droite et à gauche sur lesquels tout module de type fini indécomposable est de largeur 1.

Si un corps K est le corps des quotients d'un anneau A complètement premier dont les largeurs, droite et gauche, sont égales à 1 et si K est algébrique sur son centre F, en particulier si K est de rang fini sur F, alors K est égale à $A \otimes_V F$, où V est le centre de l'anneau A. Pour l'étude de tels anneaux, nous introduisons, au Chapitre III, la notion de quasi-valuation d'un module simple fidèle M sur un anneau B. A une quasi-valuation de M est associé un sous-anneau A de B, appelé l'anneau de la quasi-valuation ; en particulier si B est l'anneau des endomorphismes du F-espace vectoriel M, où F est le corps commutant de M sur B, tout sous-A-module de M induit une nouvelle quasi-valuation de M. On définit une quasi-valuation d'un corps K comme une quasi-valuation de K si et seulement si la largeur gauche de A est égale à 1 et si K coïncide avec $A \otimes_V F$, où V est le centre de A et F le corps des quotients de V. La notion de quasi-valuation permet de caractériser les C-groupes p-réduits. Nous appelons C-groupe, un groupe commutatif dont le treillis des sous-groupes complètement invariants est totalement ordonné, i.e. un groupe qui, en tant que module sur son anneau d'endomorphismes, est de largeur 1. Les groupes p-réduits, dont nous donnons quelques propriétés au Chapitre IV, sont des Q_p-modules sans torsion et séparés pour la topologie p-adique, où Q_p désigne le sous-anneau du corps des nombres rationnels formé des fractions r/s, où s est premier à p. L'étude des C-groupes ne permet pas une détermination complète. Nous terminons le Chapitre III en étudiant la structure des anneaux nilpotents de largeur 1, à l'aide de la structure de leur groupe additif. L'étude des groupes p-réduits, faite au Chapitre IV, permet de donner la forme des sous-groupes ouverts, pour la topologie p-adique des groupes p-réduits.

Il m'est agréable d'exprimer à M. Paul Dubreil et à Mme Dubreil-Jacotin mon affectueuse gratitude pour l'aide constante que j'ai trouvée près d'eux.

Je suis heureuse de pouvoir exprimer ma reconnaissance à M. Michel Lazard pour les conseils qu'il n'a cessé de me prodiguer pendant la rédaction de ce travail et pour les améliorations qu'il m'a ainsi permis d'y apporter.

Ma reconnaissance va également à M. Pierre Samuel sans les encouragements de qui ce travail n'eût pas été entrepris, à M. Gabriel Thierrin qui a suivi avec beaucoup de sympathie mes recherches.

Mes remerciements vont aussi à M. Jacques Dixmier qui a bien voulu me donner un second sujet de thèse.

REMARQUES LIMINAIRES

Sauf mention du contraire, tous les anneaux considérés sont supposés posséder un élément unité ; tous les modules (à droite, à gauche) sont unitaires. Un homomorphisme d'anneaux implique l'élément unité sur l'élément unité. Tout sous-anneau a pour élément unité celui de l'anneau dans lequel il est contenu.

Par "idéal" d'un anneau, on entendra toujours "idéal bilatère".

Un idéal I d'un anneau A est dit propre si I est différent de A .

Par radical d'un anneau, on entendra toujours radical de Jacobson.

Un anneau A sera dit local s'il ne possède qu'un idéal à gauche maximal ; cet idéal coïncide avec le radical de A et tout élément de A n'appartenant pas au radical est inversible.

Un anneau commutatif A sera dit semi-local s'il possède un nombre fini d'idéaux maximaux.

Nous appellerons anneau d'intégrité tout anneau commutatif sans diviseurs de zéro propres.

CHAPITRE I

Largeurs d'anneaux

§ 1.- Largeur d'un treillis.

1.1.1. - Proposition. - Soient T un treillis, dont les opérations sont notées $\vee$ et $\wedge$, et m un nombre entier, $m \geqslant 1$. Les conditions suivantes sont équivalentes :

1º) Dans chaque système $a_1,\dots,a_m,a_{m+1}$ d'éléments de T, l'un des a_i est inférieur à la borne supérieure des autres éléments ;

2º) La borne supérieure d'une famille finie d'éléments de T est la borne supérieure de m éléments, au plus, de cette famille ;

3º) Dans chaque système $a_1,\dots,a_m,a_{m+1}$ d'éléments de T, l'un des a_i est supérieur à la borne inférieure des autres éléments ;

4º) La borne inférieure d'une famille finie d'éléments de T est la borne inférieure de m éléments, au plus, de cette famille.

Démonstration. Il est évident que les conditions 1º) et 2º) (resp. 3º) et 4º)) sont équivalentes. La condition 1º) (resp. 3º)) étant supposée vérifiée, on prouve la condition 3º) (resp. 1º)), en considérant les éléments $b_i = \bigwedge_{j\neq i} a_j$ (resp. $c_i = \bigvee_{j\neq i} a_j$), pour $i = 1,2,\dots,m+1$.

1.1.2. - Définition. - Nous appellerons largeur d'un treillis T, le plus petit entier m, $m \geqslant 1$, pour lequel les conditions équivalentes de 1.1.1. sont vérifiées; si un tel entier n'existe pas, nous dirons que la largeur de T est infinie.

1.1.3. - Proposition. - Le produit cartésien de deux treillis X et Y, de largeur respective n et m, est un treillis de largeur $n+m$.

Démonstration. La largeur de $X\times Y$ est, au moins, égale à $n+m$; en effet il suffit de considérer un système d'éléments $a_1,\dots,a_n$ (resp. $b_1,\dots,b_n$) de X (resp. Y) tel qu'aucun des a_i (resp. b_i) n'est inférieur, dans X (resp. Y), à la borne supérieure des autres éléments et de poser $a_o = \bigwedge_{i=1}^{n} a_i$ (resp. $b_o = \bigwedge_{i=1}^{m} b_i$) ; alors, aucun des éléments $(a_o,b_1),\dots,(a_o,b_m),(a_1,b_o),\dots,(a_n,b_o)$ n'est inférieur à la borne supérieure des autres, dans $X\times Y$. La largeur de $X\times Y$ est, au plus, égale à n+m ; en effet soit $(a_i = (x_i, y_i))_{i\in I}$ une famille finie d'éléments de $X\times Y$; il existe deux sous-familles J et L de I, de cardinal inférieur à n et m respectivement, telles que, si $x = \bigvee_{i\in J} x_i$ et $y = \bigvee_{i\in L} y_i$, on ait $x \vee x_j = x$ et $y \vee y_j = y$, pour tout $j \in I$. On a, alors, $a \vee a_i = a$, pour tout $i \in I$, où $a = \bigvee_{i\in J\cup L} (x_i, y_i)$ et le cardinal de $J\cup L$ est, au plus, $n+m$.

1.1.4. - Proposition. - Si la longueur d'un treillis T est finie, sa largeur est finie et est inférieure à la longueur de T.

Démonstration. Soit s la longueur de T et soient $x_1,\dots,x_s,x_{s+1}$ des éléments de T, deux à deux incomparables pour la relation d'ordre de T. Posons $y = \bigwedge_{i=1}^{s+1} x_i$. La chaîne $y \leqslant x_1 \leqslant x_1 \vee x_2 \leqslant \dots \leqslant \bigvee_{i=1}^{s+1} x_i$ possédant $s+1$ éléments, il existe un indice i pour lequel on a : $\bigvee_{j=1}^{i+1} x_j = \bigvee_{k=1}^{i} x_k$; donc x_{i+1} est inférieur à $\bigvee_{j\neq i+1} x_j$.

Si a est un élément d'un ensemble ordonné E, on notera $\overset{\leqslant}{a}$ [resp. $\overset{\geqslant}{a}$] la section commençante (resp. finissante) de a, c'est-à-dire l'ensemble des éléments x de E tels que $x \leqslant a$ [resp. $x \geqslant a$]. Si E est un treillis, $\overset{\leqslant}{a}$ et $\overset{\geqslant}{a}$ sont des sous-treillis de E.

1.1.5. - Proposition. - Si T est un treillis de largeur n et si T' est un sous-treillis de T, la largeur de T' est, au plus, n. Si a est un élément de T, la largeur des treillis $\overset{\leqslant}{a}$ et $\overset{\geqslant}{a}$ est, au plus n.

Un treillis T est dit modulaire, s'il satisfait à l'axiome suivant :

$x \leqslant z$ implique $x \vee (y \wedge z) = (x \vee y) \wedge z$ quel que soit $y \in T$.

1.1.6. - THEOREME. - Soient T un treillis modulaire et a un élément de T ; si les largeurs des treillis $\overset{\leqslant}{a}$ et $\overset{\geqslant}{a}$ sont respectivement égales à n et m, la largeur de T est inférieure à $n+m$.

Démonstration. Soit $(x_\lambda)_{\lambda\in\Lambda}$ une famille finie d'éléments de T ; on suppose que le cardinal de Λ est supérieur à $n+m$. Puisque la largeur du treillis $\overset{\geqslant}{a}$ est m, il existe d'après 1.1.1., des éléments $x_1,\dots,x_m$ de la famille $(x_\lambda)_{\lambda\in\Lambda}$ tels que, en posant $y = \bigvee_{i=1}^{m} x_i$ on ait :

(1.1.6.1) $x_\lambda \leqslant y \vee a$ quel que soit $\lambda \in \Lambda$.

En raison de la modularité de T, on a :

(1.1.6.2) $y \vee ((x_\lambda \vee y) \wedge a) = (y \vee a) \wedge (x_\lambda \vee y)$.

D'après 1.1.6.1., l'égalité (1.1.6.2) s'écrit :

(1.1.6.3) $x_\lambda \vee y = y \vee ((x_\lambda \vee y) \wedge a)$ quel que soit $\lambda \in \Lambda$.

Posons $x'_\lambda = (x_\lambda \vee y) \wedge a$ pour tout $\lambda \in \Lambda$. Puisque la largeur de $\overset{<}{a}$ est égale à n, il existe n éléments $x'_{m+1},\dots,x'_{m+n}$ de la famille $(x'_\lambda)_{\lambda\in\Lambda}$ tels que :

(1.1.6.4) $x'_\lambda \leqslant \bigvee_{i=1}^{n} x'_{m+i}$ quel que soit $\lambda \in \Lambda$.

D'où d'après (1.1.6.3),

$$x_\lambda \leqslant (\bigvee_{i=1}^{n} x'_{m+i}) \vee y \quad \text{quel que soit } \lambda \in \Lambda,$$

c'est-à-dire que $\bigvee_{j=1}^{m+n} x_j = \bigvee_{\lambda\in\Lambda} x_\lambda$.

§ 2.- Largeurs d'anneaux et de modules.

1.2.1. - Définition. - Nous appellerons largeur d'un anneau A (resp. d'un A-module M) la largeur du treillis des idéaux de A (resp. des sous-modules de M). Nous appellerons largeur gauche (resp. droite) d'un anneau A, la largeur du A-module A_s (resp. A_d).

1.2.2. - Proposition. - Soient A un anneau et M un A-module ; les conditions suivantes sont équivalentes :

1º) La largeur de A (resp. M) est inférieure à n ;

2º) Dans chaque système $x_1,\dots,x_n,x_{n+1}$ de $n+1$ éléments de A (resp. M), il existe un élément x_i qui appartient à l'idéal de A (resp. au sous-module de M) engendré par les n autres.

Démonstration. Il est évident que 1º) implique 2º). Démontrons, pour l'anneau A, que 2º) entraine 1º). Soient $I_1,\dots,I_{n+1}$, $n+1$ idéaux de A, tels que, pour $i = 1,\dots,n$, I_i ne soit pas contenu dans l'idéal engendré par les x_i, $i = 1,\dots,n$, où $x_i \in I_i$ et $x_i \notin \sum_{j\neq i} I_j$; d'où I_{n+1} est contenu dans $\sum_{i=1}^{n} I_i$.

1.2.3. - Corollaire. - Soit A un anneau noethérien à gauche dont la largeur est égale à n. Alors chaque idéal à gauche de A peut être engendré par moins de n éléments.

1.2.4. - Définition. - Soit A un anneau (resp. M un A-module) ; nous dirons que n éléments de A (resp. M), $x_1,\dots,x_n$ sont incomparables dans leur ensemble si aucun des x_i n'est contenu dans l'idéal (resp. le sous-module) engendré par les x_j, $j \neq i$. Nous dirons que n idéaux (resp. sous-modules) de A (resp. M) $I_1,\dots,I_n$ sont incomparables dans leur ensemble, si aucun des I_i n'est contenu dans l'idéal (resp. le sous-module) engendré par les I_j, $j \neq i$.

Puisque le produit de deux idéaux d'un anneau est contenu dans leur intersection, on a :

1.2.5. - Proposition. - Un anneau A de largeur n possède, au plus, n idéaux maximaux. Si A est commutatif, il est semi-local.

Il résulte de 1.1.5., la proposition suivante :

1.2.6. - Proposition. - La largeur d'un anneau (resp. d'un module) holomorphe à un anneau (resp. un module) de largeur n est inférieure à n. La largeur d'un sous-module d'un module de largeur n est inférieure à n.

1.2.7. - Proposition. - Soient A un anneau commutatif de largeur n et S une partie multiplicative de A ; la largeur du A-module $S^{-1}A$ est, au plus, n.

Démonstration. La proposition résulte de ce que deux éléments de $S^{-1}A$ peuvent toujours s'écrire sous la forme a/s et a'/s, a et $a' \in A$, $s \in S$.

1.2.8. - Corollaire. - Soient A un anneau d'intégrité, K son corps des quotients. La largeur de A est égale à n si et seulement si K est un A-module de largeur n.

Démonstration. La condition est nécessaire d'après 1.2.7.. Elle est suffisante puisque A est un sous-A-module de K.

1.2.9. - Proposition. - Soient A un anneau d'intégrité de largeur n, K le corps des quotients de A, H un sous-corps de K. La largeur de l'anneau $B = A \cap H$ est, au plus, n.

Démonstration. Soient $x_1, \dots, x_{n+1}$ des éléments non nuls de B. On a, par exemple, $x_1A \cap \dots \cap x_nA \subseteq x_{n+1}A$. Pour tout $y \in H$, $y \neq 0$, on a : $yH = H$ et $y(H \cap A) = yH \cap yA$. Donc : $x_1B \cap \dots \cap x_nB \subseteq x_{n+1}B$.

1.2.10.- Proposition. - Soient K un corps, A et B deux sous-anneaux de K de largeur finie. Alors la largeur de l'anneau $A \cap B$ est, au plus, égale à la somme des largeurs des anneaux A et B.

Démonstration. D'après 1.2.9., on peut supposer que K est le corps des quotients de l'anneau $A \cap B$. Soient n et m les largeurs respectives de A et de B. Soit $(x_i)_{i \in I}$ une famille finie d'éléments de K. On a : $\bigcap_{i \in I} x_i(A \cap B) = \bigcap_{i \in I} (x_iA \cap x_iB) = (\bigcap_{i \in I} x_iA) \cap (\bigcap_{i \in I} x_iB)$. Il existe une sous-famille J de I de cardinal au plus n et une sous-famille L de I de cardinal au plus m telles que : $\bigcap_{i \in I} x_iA = \bigcap_{i \in J} x_iA$ et $\bigcap_{i \in I} x_iB = \bigcap_{i \in L} x_iB$. D'où $\bigcap_{i \in I} x_i(A \cap B) = \bigcap_{i \in J \cup L} x_i(A \cap B)$ et le cardinal de la famille $J \cup L$ est au plus $n+m$. Donc la largeur de l'anneau

$A \cap B$ est au plus $n+m$.

Il résulte de 1.1.6., la proposition suivante :

1.2.11.- Proposition. - Soient A un anneau, M un A-module et N un sous-module de M. Si les largeurs des modules M/N et N sont finies, la largeur de M est finie et est, au plus égale à la somme des largeurs de M/N et de N.

1.2.12.- Proposition. - Soient A un anneau, R un sous-anneau de A. On suppose que A est un R-module à gauche de largeur n. Si M est un A-module à gauche libre de dimension m, la largeur du R-module M est égale à nm. Si N est un A-module à gauche de type fini et si m est le nombre minimum de générateurs de N, la largeur du R-module M est, au plus, nm.

Démonstration. La seconde partie de la proposition résulte de la première et du fait que N est un quotient d'un A-module libre de dimension m. D'autre part, le R-module M est somme directe de m sous-modules isomorphes au R-module à gauche A. Donc, d'après 1.2.11., la largeur de M, en tant que R-module, est au plus nm. Mais il existe n éléments $a_1,\dots,a_n$ du R-module à gauche A qui sont incomparables dans leur ensemble. Donc, si $x_1,\dots, x_m$ est une base de M sur A, les nm éléments $a_i x_j$, $i = 1,\dots,n$, $j = 1,\dots,m$, du R-module M sont incomparables dans leur ensemble. Par suite, la largeur du R-module M est égale à nm.

1.2.13.- Corollaire. - Si la largeur gauche d'un anneau A est égale à n et si M est un A-module à gauche libre de dimension m, la largeur de M est égale à nm. Si N est un A-module à gauche de type fini et si m est le nombre minimal de générateurs de N, la largeur du module N est, au plus, nm.

Démonstration. Il suffit de faire $R = A$ dans 1.2.12..

1.2.14.- THEOREME. - Soient A un anneau, M un A-module et $P_1 \supsetneq P_2 \supsetneq \dots \supsetneq P_n \supsetneq \dots$, une chaîne d'idéaux de A [resp. de sous-modules de M]. On suppose que les conditions suivantes sont réalisées :

1º) Pour chaque idéal [resp. sous-module] P de type fini de A [resp. M] on a : $\bigcap_{i=1}^{\infty} (P + P_i) = P$;

2º) L'ensemble des largeurs des anneaux A/P_i [resp. des modules M/P_i] est borné. Alors, la largeur de l'anneau A (resp. du module M) est égale à la borne supérieure des largeurs des anneaux A/P_i (resp. des modules M/P_i).

Démonstration. Nous ne ferons la démonstration que pour le module M et nous supposerons que $P_m \neq (0)$, pour tous les indices m. Soit n la borne supérieure des largeurs des modules M/P_i . Puisque, d'après 1.2.6., la largeur de M/P_i est inférieure à la largeur de M , il suffit de prouver que la largeur de M est inférieure à n . Soient $x_1,\ldots,x_{n+1} \in M$; quel que soit le nombre entier positif m , il existe un indice $i(m)$, compris entre 1 et $n+1$, tel que $x_{i(m)} \in P_m + \sum_{j\neq i(m)} Ax_j$; on a, alors, $x_{i(m)} \in P_s + \sum_{j\neq i(m)} Ax_j$, si $s \leqslant m$. Par suite, il existe un indice i tel que, quel que soit k , on a : $x_i \in P_k + \sum_{j\neq i} Ax_j$. D'après la condition 1º), on a : $x_i \in \sum_{j\neq i} Ax_j$; d'après 1.2.2., la largeur de M est, au plus n .

1.2.15.- <u>Corollaire</u>. - <u>Soient</u> A <u>un anneau commutatif noethérien et</u> N <u>le radical de</u> A . <u>Si l'ensemble des largeurs des anneaux</u> A/N^s <u>est borné, la largeur de l'anneau</u> A <u>est égale à la borne supérieure des largeurs des anneaux</u> A/N^s .

<u>Démonstration</u>. L'anneau A étant commutatif et noethérien, chaque idéal de A est fermé pour la topologie N-adique (cf. [19] , Théorème 9 ; p. 262). Il suffit donc d'appliquer 1.2.14. au module A_s et à la chaîne des sous-modules $N \supseteq N^2 \supseteq \ldots \supseteq N^s \supseteq \ldots$ de A_s .

1.2.16.- <u>Proposition</u>. - <u>Soient</u> A <u>un anneau et</u> $I_1, I_2,\ldots, I_k$ <u>des idéaux bilatères de</u> A . <u>On suppose que</u> :

(i) $\bigcap_{j=1}^{k} I_k = (0)$;

(ii) <u>La largeur gauche de l'anneau</u> A/I_j , $j = 1,\ldots,k$ <u>est finie</u>.

<u>Alors la largeur gauche de l'anneau</u> A <u>est finie et est au plus égale à la somme des largeurs gauches des anneaux</u> A/I_j .

<u>Démonstration</u>. Il suffit de faire la démonstration pour $k=2$. Les A-modules à gauche A/I_i , $i = 1,2$, sont de largeur finie. Puisque $I_1 = I_1/(I_1 \cap I_2)$ est isomorphe, en tant que A-module à gauche, à $(I_1 + I_2)/I_2$, il est de largeur finie. Par suite, le A-module à gauche A_s est de largeur finie, d'après 1.2.11..

§ 3.- <u>Modules de largeur finie et Anneaux artiniens</u>.

1.3.1. - <u>Définition</u>. - Soient A un anneau, I un idéal de A et M un A-module à gauche ; nous dirons que I <u>est nilpotent relativement à</u> M , s'il existe un nombre entier m , $m \geqslant 1$, tel que :

(1.3.1.1) $I^m.M = (0)$.

Nous appellerons ordre de nilpotence de I relativement à M , le plus petit des nombres entiers m, $m \geqslant 1$, pour lesquels l'égalité (1.3.1.1) est vérifiée.

1.3.2. - THEOREME. - <u>Soient</u> A <u>un anneau</u>, N <u>son radical et</u> M <u>un</u> A-<u>module à gauche</u>.

(i) <u>Si la longueur de</u> M <u>est finie, sa largeur est finie et est inférieure à la longueur de</u> M ;

(ii) <u>Si l'anneau</u> A/N <u>est semi-simple, si la largeur de</u> M <u>est finie et si</u> N <u>est nilpotent relativement à</u> M , <u>alors la longueur de</u> M <u>est finie</u>.

<u>Démonstration</u>. (i) résulte de 1.1.4. .

(ii) Supposons que $N.M = (0)$. Alors, M est un A/N-module. Puisque A/N est semi-simple, M est un A/N-module semi-simple ; par conséquent, M est un A-module semi-simple. Soit $M = \bigoplus_{i\in I} M_i$ une décomposition de M en somme directe de sous-modules simples. L'ensemble d'indices I contient, au plus, n éléments ; en effet, soient $i_1,\dots,i_{n+1}$ des éléments deux à deux distincts de I . D'après 1.1.3., la largeur du module $\bigoplus_{k=1}^{n+1} M_{i_k}$ est $n+1$ ce qui est impossible. Supposons à présent que l'ordre de nilpotence h de N , relativement à M , soit différent de 1 ; on a une chaîne $M \supset NM \supset \dots \supset N^{h-1}M$ et les A/N-modules $N^iM/N^{i+1}M$ sont de largeur finie. Il résulte de la première partie de la démonstration, que les A-modules $N^iM/N^{i+1}M$ sont de longueur finie. La longueur du A-module M est donc finie.

1.3.3. - <u>Corollaire</u>. - <u>Si la largeur d'un anneau commutatif est finie et si son radical est nilpotent, l'anneau</u> A <u>est artinien</u>.

<u>Démonstration</u>. Soit N le radical de A . Puisque d'après 1.2.4. l'anneau A possède un nombre fini d'idéaux maximaux, l'anneau A/N est semi-simple. Il suffit donc d'appliquer 1.3.2. au module A_s .

1.3.4. - <u>Proposition</u>. - <u>Soient</u> A <u>un anneau commutatif, local, noethérien et</u> N <u>l'idéal maximal de</u> A . <u>La largeur du complété</u> $\hat{A}$ <u>de</u> A , <u>pour la topologie</u> N-<u>adique est finie si et seulement si celle de</u> A <u>est finie et elles sont égales</u>.

<u>Démonstration</u>. L'anneau $\hat{A}$ est un anneau local d'idéal maximal $\hat{N} = N\hat{A}$. Soit s un nombre entier, $s \geqslant 1$; l'anneau A/N^s est artinien ; il coïncide donc avec $\hat{A}/\hat{N}^s$ (cf. [19], Ch. VIII ; Cor. 2 du th. 6 ; p. 258). Il suffit donc d'appliquer 1.2.14., pour prouver que les largeurs de A et de $\hat{A}$ sont finies en même temps et qu'elles sont égales. En effet, la largeur de $\hat{A}$ est la borne supérieure des largeurs des anneaux A/N^s , lorsque s parcourt l'ensemble des entiers naturels.

1.3.5. - <u>Proposition</u>. - <u>Soient</u> A <u>un anneau et</u> $J_1 \supseteq J_2 \supseteq \dots \supseteq J_s \supseteq \dots$, <u>une chaîne d'idéaux de</u> A . <u>Supposons que les deux conditions suivantes soient réalisées</u> :

1º) <u>L'anneau</u> A/J_s <u>est noethérien à gauche, pour tout</u> s ;

2º) <u>Pour chaque idéal à gauche</u> I <u>de</u> A , <u>il existe un entier</u> s , $s > 0$, <u>tel que, si</u> $I = K + (I \cap J_s)$, <u>où</u> K <u>est un idéal à gauche de type fini de</u> A , <u>on a</u>

$I = K$.

Alors, l'anneau A est noethérien à gauche.

Démonstration. Soient I un idéal à gauche de A et s un entier positif associé à I , par la condition 2º). L'anneau A/J_s étant noethérien à gauche, il existe un idéal à gauche de type fini, $k = \sum_{i=1}^{m} Ax_i$, $x_i \in I$, tel que $I + J_s = K + J_s$. Puisque K est contenu dans I , on a : $I = K + (I \cap J_s)$; par suite, $I = \sum_{i=1}^{m} Ax_i$.

1.3.6. - Corollaire. - Soient A un anneau et N le radical de A . Supposons que les conditions suivantes soient réalisées :

1º) L'anneau A/N est semi-simple ;

2º) La largeur gauche de A est finie ;

3º) Pour chaque idéal à gauche I de A , il existe un nombre entier s, $s > 0$, tel que si $I = J + (I \cap N^s)$, où J est un idéal à gauche de type fini de A , on a : $I = J$.

Alors, l'anneau A est noethérien à gauche.

Démonstration. Il suffit d'appliquer 1.3.5., à la chaîne des idéaux $N \supsetneq N^2 \supsetneq \ldots \supsetneq N^k \supset \ldots$.

En effet, pour chaque entier s , $s \geqslant 1$, le radical N/N^s de l'anneau A/N^s est nilpotent, l'anneau $(A/N^s)/(N/N^s)$ est semi-simple et la largeur gauche de l'anneau A/N^s est finie. D'après 1.3.2., l'anneau A/N^s est artinien à gauche et, par suite, il est noethérien à gauche. Le corollaire résulte, alors, directement de 1.3.5..

1.3.7. - Corollaire. - Soient A un anneau commutatif et N le radical de A . Supposons que les conditions suivantes soient réalisées :

1º) La largeur de A est finie ;

2º) Pour chaque idéal I de A , il existe un nombre entier s, $s > 0$, tel que si $I = J + (I \cap N^s)$, où J est un idéal de type fini de A , on a : $I = J$.

Alors, l'anneau A est noethérien.

Démonstration. Il suffit d'appliquer 1.3.6., puisque, la largeur de l'anneau A étant finie, l'anneau A/N est semi-simple.

§ 4.- Anneaux commutatifs noethériens

Sauf mention du contraire, tous les anneaux considérés dans ce paragraphe sont supposés commutatifs.

I. S. COHEN [7] a défini la notion de rang d'un anneau de la manière suivante : un anneau A est dit de rang k , si chaque idéal de A possède un système de générateurs de k éléments. Nous préférons, ici, définir le rang d'un anneau de rang fini, comme le plus petit entier k tel que tout idéal de l'anneau possède un système de générateurs de k éléments. Un anneau de rang fini est noethérien. D'après 1.2.3., un anneau noethérien de largeur n est de rang fini, au plus égal à n. Mais il existe des anneaux de rang fini dont la largeur est infinie. Par exemple, les anneaux de Dedekind dont le nombre des idéaux maximaux est infini.

Cependant, pour les anneaux noethériens locaux, les notions de "rang fini" et de "largeur finie" coïncident. Plus précisément, on a :

1.4.1. - Proposition. - <u>La largeur d'un anneau local</u> A <u>de rang</u> n <u>est égale à</u> n.

<u>Démonstration</u>. Soient $m(A)$ l'idéal maximal de A, $(x_\lambda)_{\lambda\in\Lambda}$ une famille finie d'éléments de A et I l'idéal de A engendré par les x_λ. Désignons par $\overline{x}_\lambda$ la classe de x_λ module $m(A)I$. Puisque $(\overline{x}_\lambda)_{\lambda\in\Lambda}$ est un système de générateurs du $A/m(A)$-espace vectoriel $I/m(A)I$, et que, A étant de rang n, le $A/m(A)$-espace vectoriel $I/m(A)I$ est de dimension au plus n, on peut extraire de $(\overline{x}_\lambda)_{\lambda\in\Lambda}$ une base : $\overline{x}_{\lambda_1},\dots,\overline{x}_{\lambda_n}$, $m \leqslant n$. Donc $I = \sum_{i=1}^{i=m} Ax_{\lambda_i} + m(A)I$ et, d'après le lemme de Nakayama, on a : $I = \sum_{i=1}^{i=m} Ax_{\lambda_i}$.

I. S. COHEN a prouvé (Loc. Cit) qu'<u>un anneau local de rang fini est de dimension inférieure à 1</u>, en appelant d'une manière générale dimension d'un anneau noethérien, la borne supérieure, si elle existe, des longueurs de ses chaînes d'idéaux premiers, ou bien l'infini. Nous allons établir la réciproque de cette propriété.

Rappelons que l'on appelle <u>caractéristique d'un anneau</u> A l'ordre additif de son élément unité, i.e. le plus petit entier $n \geqslant 0$ pour lequel $n.1 = 0$.

1.4.2. - THEOREME. - <u>La largeur d'un anneau</u> A, <u>local et noethérien, de dimension</u> $\leqslant 1$, <u>est finie</u>.

<u>Démonstration</u>. Soit $m(A)$ l'idéal maximal de A. Puisque le complété $\hat{A}$ de A pour la topologie $m(A)$-adique a même dimension que A (cf. [19] ; Chap. VIII ; § 8; Lemme 1 et § 9 p. 288), il suffit, d'après 1.3.4., de prouver le théorème pour un anneau complet. Si la dimension de A est 0, A est artinien et par suite de largeur finie, d'après 1.3.3. . Supposons que la dimension de A soit égale à 1. Nous démontrerons successivement 1.4.2. dans les cas suivants :

I. <u>L'anneau</u> A <u>est d'égales caractéristiques</u> (i.e. il a même caractéristique que son corps des restes).

II. <u>L'anneau</u> A <u>est d'inégales caractéristiques et si</u> p <u>est la caractéristique de son corps résiduel, l'idéal</u> pA <u>n'est contenu dans aucun idéal premier minimal de</u> A.

III. <u>L'anneau</u> A <u>est d'inégales caractéristiques et si</u> p <u>est la caractéristique de son corps résiduel, l'idéal</u> pA <u>est contenu dans tous les idéaux premiers minimaux de</u> A .

Le théorème 1.4.2. résultera alors de 1.2.16. . En effet, il suffit d'examiner le cas où l'idéal (0) admet une décomposition primaire dont le nombre des composants est $\geqslant 2$. On a : $Q_1 \cap \ldots \cap Q_s = (0)$, $s \geqslant 2$, où les Q_i sont des idéaux primaires de A ; l'anneau A/Q_i , $i = 1,\ldots, s$, ne possède qu'un seul idéal premier minimal ; il est donc de largeur finie d'après II et III et, d'après 1.2.16., la largeur de A est finie.

<u>Démonstration de</u> I. Dans ce cas, A contient un sous-corps K isomorphe à A/m(A) (cf. [15] ; Chap. V ; Théorème 31.1 ; p. 106) et A est un module de type fini sur l'anneau $K[[x]]$, où x est un élément de A qui engendre un idéal primaire pour m(A) (cf. [19] ; Chap. VIII ; § 11 ; Corollaire 2 du Théorème 24 ; p. 300). Puisque $K[[x]]$ est un anneau de largeur 1 , A est un anneau de largeur finie.

<u>Démonstration de</u> II. La caractéristique de A est 0 et celle de A/m(A) est $p \neq 0$. Puisqu'il n'existe pas d'idéal premier minimal P de A tel que $pA \subsetneq P$, la dimension de l'anneau A/pA est 0 . D'après la proposition 1 de ([18] ; Chap. IV ; § 3 ; p. 50), A est un module de type fini sur un sous-anneau B qui a même dimension de A ; l'anneau B est local noethérien régulier. Donc B est un anneau de valuation et A est un anneau de largeur finie.

<u>Démonstration de</u> III. La caractéristique de A est, dans ce cas, p^k , k entier > 0 . L'anneau A/pA est d'après I, de largeur finie. Par suite, le A-module A/pA est de largeur finie. Soit r un entier > 0 ; l'application : $x + pA \longrightarrow p^r x + p^{r+1}A$ détermine un homomorphisme, de A-modules, de A/pA sur $p^rA/p^{r+1}A$. Donc $p^rA/p^{r+1}A$ est un A-module de largeur finie et la largeur du A-module A/p^rA est finie, d'après 1.2.11. ; par suite la largeur de l'anneau A/p^rA est finie. En prenant $r = k$, on voit que la largeur de A est finie.

Soient A un anneau local noethérien de dimension d , m(A) son idéal maximal et Q un idéal de A , ouvert pour la topologie m(A)-adique. A partir d'un entier n , $n \geqslant 1$, la longueur du A-module A/Q^n est donnée par un polynôme en n de degré d , dit <u>polynôme caractéristique de</u> Q dont les coefficients sont des multiples entiers de $1/d!$. Le terme de degré d de ce polynôme est de la forme : $e(Q).n^d/d!$ et e(Q) est appelé la <u>multiplicité de l'idéal</u> Q . La multiplicité de l'idéal m(A) est appelé la <u>multiplicité de l'anneau</u> A .

Si la dimension de A est 0, le polynôme caractéristique de tout idéal propre Q de A est une constante égale à la longueur du A-module A_s. Par suite, la multiplicité de A est égale à la longueur du module A_s. Il existe donc des cas où la largeur de A est strictement inférieure à sa multiplicité. Il suffit de prendre le quotient d'un anneau de valuation par une puissance de son idéal maximal.

Si la dimension de A est égale à 1, la multiplicité de A mesure, à partir d'un certain entier n, $n \geqslant 1$, la dimension du $A/m(A)$-espace vectoriel $m(A)^n/m(A)^{n+1}$. On a, par suite, l'inégalité :

(1.4.3) multiplicité de $A \leqslant$ largeur de A.

Les théorèmes 1.4.5. et 1.4.6. suivants donnent des cas dans lesquels (1.4.3) est une égalité. Pour cela, rappelons que si A est un anneau local noethérien d'idéal maximal $m(A)$, un élément x de A est dit superficiel d'ordre s, sous-entendu : pour $m(A)$, si $x \in m(A)^s$ et s'il existe un entier c, $c \geqslant 0$, tel que l'on ait :

(1.4.4.0) $(m(A)^n : Ax) \cap m(A)^c = m(A)^{n-s}$,

à partir d'un certain n.

La démonstration du lemme suivant que nous reproduisons est contenue dans la démonstration du Théorème 22, § 10 ; Chap. VIII de [19].

1.4.4. - Lemme. - Soient A un anneau local noethérien de dimension 1, $m(A)$ son idéal maximal, x un élément de A superficiel d'ordre s. Si x n'est pas diviseur de zéro dans A, on a, à partir d'un certain n, l'égalité $m(A)^n = xm(A)^{n-s}$. Inversement, si cette égalité est satisfaite par un élément x de $m(A)^s$, non diviseur de zéro dans A, alors x est superficiel d'ordre s.

Démonstration. Puisque x n'est pas diviseur de zéro dans A, on a : $m(A)^n : Ax \subset m(A)^{t(n)}$ où $t(n)$ est une fonction à valeurs entières qui tend vers l'infini avec n (cf. [19] ; Chap. VIII ; § 5 ; Cor. 1 du Th. 13 ; p. 272). Compte tenu de l'égalité (1.4.4.0), on a, pour n assez grand, $m(A)^n : Ax = m(A)^{n-s}$. Puisque x n'est contenu dans aucun idéal premier minimal de A, l'anneau A/Ax est artinien. Il existe donc un entier m, $m > 0$, pour lequel on a : $m(A)^m \subseteq Ax$. Par conséquent, pour tout entier $t \geqslant \mathrm{Sup}(m,n)$, on a :

$$m(A)^t : Ax = m(A)^{t-s}$$
$$m(A)^t \subseteq Ax .$$

Il en résulte que $m(A)^t = m(A)^{t-s}x$. La seconde partie du lemme est évidente.

1.4.5. - THEOREME. - <u>Soient</u> A <u>un anneau local noethérien de dimension</u> 1, $m(A)$ <u>son idéal maximal. Si</u> A <u>possède un élément</u> v <u>superficiel d'ordre</u> 1 <u>et non diviseur de zéro dans</u> A <u>et si la largeur de</u> A <u>est égale à</u> 2, <u>alors la multiplicité de</u> A <u>est égale à</u> 2.

<u>Démonstration</u>. On a, d'après 1.4.4. et d'après la définition de la multiplicité e de A ,

$$m(A)^{n+1} = vm(A)^n$$

et

$$\left[\frac{m(A)^n}{m(A)^{n-1}} : \frac{A}{m(A)}\right] = e ,$$

à partir d'un certain entier n . Il suffit, puisque v n'est pas diviseur de zéro, de prouver que, si $e = 1$, alors la largeur du A-module $m(A)^n$ est 1 . Il en résultera, en effet, que la largeur de A est 1 , ce qui contredit l'hypothèse. Si $e = 1$, soient $z_i \in m(A)^n$, $i = 1,2,$. Il existe deux entiers $\geqslant 0$, t_i , $i = 1,2,$ tels que : $z_i = v^{t_i} y_i$ où $y_i \in m(A)^n$ et $y_i \notin m(A)^{n+1}$. Supposons que $t_1 \geqslant t_2$. On a : $y_1 \in Ay_2 + m(A)^{n+1}$. Par suite, si $y_1 \notin Ay_2$, il existe un entier $q \geqslant 1$, tel que $y_1 \in Ay_2 + m(A)^{n+q}$ et $y_1 \notin Ay_2 + m(A)^{n+q+1}$. D'où $y_1 =$ $= ay_2 + v^q x$, où $a \in A$ et $x \in m(A)^n$, $x \notin m(A)^{n+1}$. Mais on a : $x \in Ay_2 + m(A)^{n+1}$; d'où $y_1 \in Ay_2 + m(A)^{n+q+1}$; ce qui contredit le choix de q . Donc $y_1 \in Ay_2$ et $z_1 \in Az_2$.

<u>Exemple d'anneau local noethérien de dimension</u> 1, <u>de largeur</u> 2, <u>de multiplicité</u> 1, <u>qui possède un élément superficiel d'ordre</u> 1 .

Soient K un corps, $V = K[[Y]]$ l'anneau des séries formelles à une indéterminée Y sur K et $P = Kx$ un K-espace vectoriel à une dimension. Soit A l'anneau défini sur le groupe additif $V_+ \oplus P_+$ en posant : $x^2 = xY = Yx = 0$. Alors, A est un anneau commutatif unitaire dont l'élément unité est l'élément 1 de K . On a : $P = Ax$ et P est un idéal premier de A . Un élément $f(Y) + kx \in A$ est inversible si et seulement si $f(0) \neq 0$. Donc A est un anneau local d'idéal maximal $m(A) = VY \oplus P$. De plus, l'idéal $m(A)$ est de type fini : $m(A) = AY + Ax$. Soit Q un idéal premier de A . Puisque $x^2 = 0$, on a $x \in Q$; d'où $P \subsetneq Q$ et $Q =$ $= (V \cap Q) \oplus P$. Puisque V est un sous-anneau de A , l'idéal $V \cap Q$ est un idéal premier de V . Donc $Q \cap V = (0)$ ou bien $Q \cap V = YV$. Par suite, les seuls idéaux premiers de A sont P et $m(A)$. Comme A est un V-module de type fini, avec, pour générateurs 1 et x , c'est un anneau noethérien et c'est un anneau de largeur au plus 2 . La largeur de A est égale à 2 car les idéaux AY et Ax ne sont pas comparables. Puisque $m(A)^2 = AY^2$, la multiplicité de A est égale à 1 et Y est un élément superficiel d'ordre 1 .

Exemple d'anneau local noethérien de dimension 1 dont l'idéal maximal est un idéal premier de (0), qui possède des éléments superficiels d'ordre 1 et dont la multiplicité et la largeur sont égales à 2 .

Soient V_1 et V_2 des anneaux de valuation ayant le même corps des restes K . Soient $h_i : V_i \longrightarrow K$, $i = 1,2$, les homomorphismes surjectifs. Soit $A = \{(a_1,a_2),\ a_i \in V_i\ ,\ h_1(a_1) = h_2(a_2)\}$. On munit A de la structure d'anneau qui en fait un sous-anneau du produit cartésien $V_1 X V_2$. Un élément (a_1,a_2) de A est inversible si et seulement si a_i , $i = 1,2$, est inversible dans V_i . Donc A est un anneau local d'idéal maximal : $m(A) = A(x_1,0) + A(0,x_2)$, où x_i est un générateur de l'idéal maximal de V_i . Soit P un idéal premier de A . Puisque $(0,0) = (x_1,0)(0,x_2) \in P$, on a, par exemple, $(x_1,0) \in P$ et, si $P \neq m(A)$, $(0,x_2) \notin P$. Il en résulte que tout élément de P est de la forme $(a_1,0)$ où $a_1 \in V_1 x_1$. Par suite $P = A(x_1,0)$ et les seuls idéaux premiers de A sont $m(A)$, $A(x_1,0)$ et $A(0,x_2)$. Par conséquent A est un anneau noethérien de dimension 1 . La largeur de A est au moins égale à 2, car les idéaux $P_1 = A(x_1,0)$ et $P_2 = A(0,x_2)$ ne sont pas comparables. La largeur de A est effectivement égale à 2, car $P_1 \cap P_2 = (0)$ et A/P_i est isomorphe à V_i , pour $i = 1,2$. L'anneau A possède des éléments superficiels d'ordre 1, par exemple (x_1,x_2). La multiplicité de A est égale à 2 puisque l'on a : $m(A)^n = A(x_1^n,0) + A(0,x_2^n)$ pour tout n et que les classes de $(x_1^n,0)$ et de $(0,x_2^n)$ modulo $m(A)^{n+1}$, sont linéairement indépendantes dans le $A/m(A)$-espace vectoriel $m(A)^n/m(A)^{n+1}$.

1.4.6. - THEOREME. - Soient A un anneau local noethérien complet de dimension 1 et d'égales caractéristiques, $m(A)$ l'idéal maximal de A , x un élément superficiel d'ordre 1 , K un sous-corps de A isomorphe au corps résiduel $A/m(A)$. Si aucun élément non nul de $K[[x]]$ n'est diviseur de zéro dans A , alors la multiplicité de A et sa largeur sont égales.

Démonstration. L'élément x n'étant pas diviseur de zéro dans A et étant superficiel d'ordre 1, la multiplicité de l'idéal Ax est égale à la multiplicité de A (cf. démonstration Th. 22 ; Chap. VIII ; § 10 ; p. 294 à 295 de [19]). Puisque aucun élément non nul de $K[[x]]$ n'est diviseur de zéro dans A et que l'idéal Ax est primaire pour $m(A)$, il y a égalité, d'après le Cor. 2 du th. 24 de [19] ; Chap. VIII ; § 11 ; p. 300), entre la multiplicité de Ax et $[A : K[[x]]]$, où $[A : K[[x]]]$ désigne le nombre maximum d'éléments de A qui sont linéairement indépendants sur $K[[x]]$, i.e. la dimension de l'anneau total des fractions de A considéré comme espace vectoriel sur le corps des quotients de $K[[x]]$ (se rapporter à [19] Chap. VIII ; § 10 ; p. 297 ; Foot-Note). On a donc égalité entre la multiplicité de

A et $[A : K[[x]]]$. Il suffit, d'après 1.4.3., de prouver que la largeur de l'anneau A est inférieure à $[A : K[[x]]]$; puisque la largeur de l'anneau A est inférieure à la largeur du $K[[x]]$-module A , il suffit de prouver que la largeur du $K[[x]]$-module A est inférieure à $[A : K[[x]]]$; ou encore, en désignant par B l'anneau total des fractions de A , il suffit de prouver que la largeur du $K[[x]]$-module B est inférieure à la dimension du $K((x))$-espace vectoriel B . Mais ceci résulte de 1.2.12. .

On peut dans certains cas avoir un résultat plus complet que celui de 1.2.16. . De façon précise :

1.4.7. - Proposition. - Soient A un anneau local noethérien de dimension 1 , $m(A)$ l'idéal maximal de A , $P_1,\dots,P_m$ les idéaux premiers minimaux distincts de A . Si $m(A)$ n'est pas un idéal premier de (0), soit $Q_1 \cap \dots \cap Q_m = (0)$ une décomposition primaire de (0) dans laquelle Q_i et P_i - primaire, $i = 1,\dots,m$. Alors, la largeur de l'anneau A est égale à la somme des largeurs des anneaux A/Q_i .

Démonstration. Soient n la largeur de l'anneau A et n_i celle de l'anneau A/Q_i , $i = 1,\dots, m$. D'après 1.2.16., il suffit de prouver l'inégalité : $\sum_{i=1}^{m} n_i \leq n$, i.e. il suffit de trouver $\sum_{i=1}^{i=m} n_i$ éléments de A incomparables dans leur ensemble. Soit i un indice compris entre 1 et m . Puisque la largeur de l'anneau A/Q_i est égale à n_i , il existe n_i éléments de A , soient $y_1,\dots,y_{n_i}$, dont les classes modulo Q_i sont des éléments de A/Q_i incomparables dans leur ensemble. D'autre part les idéaux premiers minimaux P_i étant distincts, on peut trouver un élément $a_i \in Q_1 \cap \dots \cap Q_{i-1} \cap Q_{i+1} \cap \dots \cap Q_m$ dont aucun puissance n'appartient à Q_i . Puisque $a_i^h \notin Q_i$, quel que soit $h > 0$, et que Q_i est un idéal primaire de l'anneau A , les classes modulo Q_i des éléments $a_i y_1,\dots, a_i y_{n_i}$ sont des éléments de A/Q_i , incomparables dans leur ensemble. Par suite, pour $i = 1,\dots, m$, il existe n_i éléments de A , soient $x_1^{(i)},\dots, x_{n_i}^{(i)}$, qui appartiennent à l'intersection $Q_1 \cap \dots \cap Q_{i-1} \cap Q_{i+1} \cap \dots \cap Q_m$ et dont les classes modulo Q_i sont des éléments de A/Q_i incomparables dans leur ensemble. Il en résulte que les éléments $(x_k^{(i)})$, $i = 1,\dots, m$; $k = 1,\dots, n_i$, de A sont incomparables dans leur ensemble.

1.4.8. - Corollaire. - Soient A un anneau local noethérien de dimension 1 . Si la largeur n de A est égale au nombre des idéaux premiers minimaux de A , alors, l'anneau A ne possède pas d'éléments nilpotents non nuls, i.e. $P_1 \cap \dots \cap P_n = (0)$, où les P_i sont les idéaux premiers minimaux distincts de A .

<u>Démonstration</u>. Puisque la largeur de A est n, une décomposition primaire réduite de (0) comporte, au plus, n idéaux primaires. Comme A possède n idéaux premiers minimaux, l'idéal maximal de A ne peut être un idéal premier immergé de (0). Conservons les notations de 1.4.7.. Puisque $n = \sum_{i=1}^{n} n_i$, on a $n_i = 1$, pour tout i. Il est évident qu'un anneau noethérien de largeur 1 est soit un anneau artinien soit un anneau de valuation. Puisque la dimension de l'anneau A/Q_i est égale à 1, c'est un anneau de valuation et, par suite, $P_i = Q_i$, pour tout i.

1.4.9. - <u>Lemme</u>. - <u>Soient</u> A <u>un anneau local noethérien et</u> $m(A)$ <u>l'idéal maximal de</u> A. <u>Si</u> A <u>est de dimension</u> 1 <u>et ne possède qu'un idéal premier minimal</u> P, <u>la largeur de l'anneau</u> A <u>est égale à la somme de la largeur de l'anneau</u> A/P <u>et de la largeur du</u> A-<u>module</u> P.

<u>Démonstration</u>. Si $P = (0)$, il n'y a rien à démontrer. Supposons que $P \neq (0)$. Soit k un entier tel que $P \not\subseteq m(A)^{k+1}$. Soient m la largeur de l'anneau A/P et t_k la largeur du A-module $(P + m(A)^{k+1})/m(A)^{k+1}$. Puisque l'anneau A/P est intègre, sa largeur est égale à la largeur du A/P-module $(m(A)^k + P)/P$. Soient $x_1, x_2, \ldots, x_m$ des éléments de $m(A)^k$ dont les classes modulo P sont des éléments de A/P incomparables dans leur ensemble. Soient $y_1, \ldots, y_{t_k}$ des éléments de P dont les classes modulo $m(A)^{k+1}$ sont des éléments du A-module $(P + m(A)^{k+1})/m(A)^{k+1}$ incomparables dans leur ensemble. Par suite, aucun des x_i n'appartient à l'idéal de A engendré par $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_m, y_1, \ldots, y_{t_k}$. Soit n la largeur de A. Si l'on avait $n < m + t_k$, alors l'un des y_j appartiendrait à : $m(A)x_1 + \ldots + m(A)x_m + Ay_1 + \ldots + Ay_{j-1} + Ay_{j+1} + \ldots + Ay_{t_k}$. Donc $y_j \in m(A)^{k+1} + Ay_1 + \ldots + Ay_{t_k}$, ce qui est impossible. Donc la largeur de A est supérieure à la somme de la largeur de l'anneau A/P et de la largeur du A-module $(P + m(A)^{k+1})/m(A)^{k+1}$. Par suite, la largeur du A-module $P/(P \cap m(A)^{k+1})$ est inférieure à $n-m$. Il résulte de 1.2.14., que la largeur du A-module P est inférieure à $n-m$. Mais comme la largeur de A est inférieure à la somme de la largeur de l'anneau A/P et de la largeur du A-module P, il y a égalité entre n et $m+t$ où t est la largeur du A-module P.

1.4.10. - <u>THEOREME</u>. - <u>Soient</u> A <u>un anneau local noethérien de dimension</u> 1, $m(A)$ <u>l'idéal maximal de</u> A, $P_1, \ldots, P_m$ <u>les idéaux premiers minimaux distincts de</u> A, n <u>la largeur de</u> A, n_i <u>la largeur de l'anneau</u> A/P_i, $i = 1, \ldots, m$. <u>Si</u> $m(A)$ <u>n'est pas un idéal premier de</u> (0), <u>soit</u> $Q_1 \cap \ldots \cap Q_m = (0)$ <u>une décomposition primaire de</u> (0) <u>dans laquelle</u> Q_i <u>est</u> P_i-<u>primaire</u>, $i = 1, \ldots, m$. <u>Soit</u> m_i <u>la lar-</u>

geur du A-module P_i/Q_i. Alors on a : $n = \sum_{i=1}^{i=m} n_i + \sum_{i=1}^{i=m} m_i$.

Démonstration. Le théorème résulte de 1.4.7. et de 1.4.9. .

§ 5.- Anneaux intégralement clos.

Sauf mention du contraire, tous les anneaux considérés dans ce paragraphe sont supposés être des anneaux d'intégrité.

Soient A un anneau et K le corps des quotients de A . La famille F des anneaux de valuation de K qui contiennent A , possède des éléments minimaux ; en effet, soit $(V_i)_{i\in I}$ une sous-famille totalement ordonnée d'éléments de F ; l'anneau $V = \bigcap_{i\in I} V_i$ contient A . Si $a \in K$, $a \notin V$, il existe un indice i tel que $a \notin V_i$; donc $a \notin V_j$ si $V_j \subseteq V_i$. Par conséquent $a^{-1} \in V_i$ quel que soit i et $a^{-1} \in V$. Donc V est un anneau de valuation de K . D'autre part, tout anneau de valuation de K qui contient A , contient un élément minimal de la famille F.

Puisque un anneau intégralement clos est l'intersection des anneaux de valuation de son corps des quotients qui le contiennent, on a :

1.5.1. - Lemme. - Soient A un anneau intégralement clos et K le corps des quotients de A ; alors l'anneau A est l'intersection d'une famille d'anneaux de valuation de K , $(V_i)_{i\in I}$, telle que $V_i \not\subseteq V_j$ si $i \neq j$.

Rappelons le théorème suivant (cf. [15] ; Chap. I, § 11, Th. (11.11)) :

1.5.2. - THEOREME. - Soient $A_1,\dots,A_n$ des anneaux de valuation d'un corps K tels que $A_i \not\subseteq A_j$ si $i \neq j$. Soient P_i l'idéal maximal de A_i , A l'intersection des A_i et $Q_i = P_i \cap A$. Alors, on a :

1º) Un idéal M de A est maximal si et seulement s'il coïncide avec l'un des Q_i ;

2º) $A_i = A_{Q_i}$, pour $i = 1,\dots,n$.

Il résulte de ce théorème, le corollaire suivant :

1.5.3. - Corollaire. - Soient $A_1,\dots,A_n$ des anneaux de valuation d'un corps K , tels que $A_i \not\subseteq A_j$ si $i \neq j$. L'anneau A , intersection des A_i , possède exactement n idéaux maximaux.

1.5.4. - THEOREME. - Soient $A_1,\dots,A_n$ des anneaux de valuation d'un corps K ; la largeur de l'anneau $A = \bigcap_{i=1}^{n} A_i$ est, au plus, n . Un anneau intégralement clos de largeur n est intersection de n anneaux de valuation de son corps des quo-

<u>tients</u>.

<u>Démonstration</u>. La première partie du théorème résulte de 1.2.10.. D'autre part, un anneau A, intégralement clos est, d'après 1.5.1., l'intersection d'une famille d'anneaux de valuation $(V_i)_{i\in I}$ de son corps des quotients, telle que $V_i \not\subset V_j$, si $i \neq j$. Cette famille possède, au moins, n éléments ; sinon, d'après la première partie du théorème la largeur de A serait inférieure à $n-1$. La famille $(V_i)_{i\in I}$ possède, au plus, n éléments. Sinon, un anneau B, intersection de $n+1$ anneaux V_i, $i\in I$, possèderait, d'après 1.5.3., $n+1$ idéaux maximaux, ce qui contredit le fait que la largeur de B, sous-A-module de K est inférieure à n.

1.5.5. - <u>Corollaire</u>. - <u>Un anneau intégralement clos, local et de largeur finie est un anneau de valuation de son corps des quotients.</u>

1.5.6. - <u>Proposition</u>. - <u>Soient</u> A <u>un anneau de largeur</u> n, K <u>le corps des quotients de</u> A <u>et</u> x <u>un élément de</u> K, <u>entier sur</u> A. <u>Alors</u>, x <u>est racine d'un polynôme unitaire, à coefficients dans</u> A <u>de degré au plus</u> n.

<u>Démonstration</u>. Supposons, d'abord, l'anneau A local. Soit m le degré minimal des polynômes unitaires, à coefficients dans A, dont x est racine. On a :

(1.5.6.1) $x^m + a_1x^{m-1} + \dots + a_m = 0$ où $a_i \in A$.

Supposons que $m > n$ et considérons les sous-A-modules monogènes de K : Ax^m, $Ax^{m-1}, \dots, Ax$. Alors, Ax^m n'est pas contenu dans $Ax^{m-1} + \dots + Ax$; sinon, x serait racine d'un polynôme unitaire de $A[X]$, de degré $m-1$. Soit k le plus grand entier, $1 \leqslant k < m$, tel que : $x^k \in Ax^m + \dots + Ax^{k+1} + \dots + Ax$; on a :

(1.5.6.2) $x^k = b_mx^m + \dots + b_{k+1}x^{k+1} + b_{k-1}x^{k-1} + \dots + b_1x$;

les éléments $b_m, \dots, b_{k+1}$ appartiennent, en raison du choix de k, à l'idéal maximal $m(A)$ de A. Compte tenu de (1.5.6.1), l'égalité (1.5.6.2) s'écrit :

$x^k = c_{m-1}x^{m-1} + \dots + c_{k+1}x^{k+1} + c_kx^k + c_{k-1}x^{k-1} + \dots + c_o$;

et $c_k = -b_ma_{m-k}$ appartient à $m(A)$. Donc $1-c_k$ est inversible dans A et x^{k+1} appartient à $Ax^m + \dots + ax^{k+2} + Ax^k + \dots + Ax$, ce qui contredit le choix de k. Par conséquent, m est au plus, égal à n. Dans le cas général, soient $P_1, \dots, P_r$, $r \leqslant n$, les idéaux maximaux distincts de A. L'élément x de K, étant entier sur A, est entier sur A_{P_1} et, d'après la première partie de la démonstration, il vérifie une égalité de la forme :

(1.5.6.3) $sx^n + c_1x^{n-1} + \dots + c_n = 0$ où s et $c_i \in A$, $s \notin P_1$.

Si s n'appartient à aucun idéal maximal de A, il est inversible dans A et la proposition est démontrée. Sinon, $s \notin P_2, \dots, P_i$ et $s \in P_{i+1}$, pour $i \leqslant r-1$; d'où, puisque x est entier sur $A_{P_{i+1}}$, une relation de la forme :

(1.5.6.4) $s'x^n + b_1x^{n-1} + \ldots + b_n = 0$ où s' et $b_i \in A$, $s' \notin P_{i+1}$.
Comme $P_1 \cap \ldots \cap P_i$ n'est pas contenu dans P_{i+1} , il existe $h \in P_1 \cap \ldots \cap P_i$ et $h \notin P_{i+1}$. Il résulte des égalités (1.5.6.3) et (1.5.6.4) :

$$(hs' + s)x^n + d_1x^{n-1} + \ldots + d_n = 0$$

où $d_i \in A$, $hs' + s \in A$ et $hs' + s \notin P_1, \ldots, P_i, P_{i+1}$.

D.G. Northcott a prouvé (cf. [16]) que le nombre des idéaux maximaux de la clôture intégrale $\tilde{A}$ d'un anneau A , local, noethérien de dimension 1, est égale au nombre des idéaux premiers de (0) du complété $\hat{A}$ de A pour la topologie $m(A)$-adique, $m(A)$ désignant l'idéal maximal de A . Il résulte du cor. 1 du Th. 12 de ([19] ; Chap. VIII ; § 4 ; p.269) que l'idéal maximal $m(\hat{A})$ de $\hat{A}$ n'est pas un idéal premier de l'idéal (0) de $\hat{A}$.

On a le résultat suivant :

1.5.7. - Proposition. - *Soient* A *un anneau local noethérien de dimension* 1 , n *la largeur de* A , $m(A)$ *l'idéal maximal de* A , $\hat{A}$ *le complété de* A *pour la topologie* $m(A)$-*adique*, $(0) = Q_1^* \cap \ldots \cap Q_m^*$ *une décomposition primaire réduite de l'idéal* (0) *de* $\hat{A}$, *où les* Q_i^* *sont* p_i^*-*primaires, les* p_i^* , $i = 1,\ldots, m$, *étant les idéaux premiers minimaux de* $\hat{A}$. *Alors*, n *est égale à la somme des largeurs des anneaux* $\hat{A}/P_i^*$ *et des largeurs des* $\hat{A}$-*modules* P_i^*/Q_i^* . *Si* $n=m$, *la clôture intégrale de* A *est un* A-*module de type fini*.

Démonstration. La première partie de la proposition résulte de 1.4.10. et du fait que les largeurs de A et de $\hat{A}$ sont égales. La seconde partie résulte de la première et du Th. 8 de (D.G. Northcott ; loc. cit.).

§ 6.- *Idéaux multiplicatifs*.

On appelle *idéal multiplicatif à droite* (resp. à gauche ; resp. bilatère) d'un anneau A , tout idéal à droite (resp. à gauche ; resp. bilatère), non vide, du demi-groupe multiplicatif A_χ de A .

Si M est un A-module à gauche, une partie, non vide, S de M est dite *multiplicativement stable* si $ax \in S$, quel que soit $a \in A$, dès que $x \in S$.

Si a est un élément d'un anneau A , on notera $(a)_\chi$ l'idéal bilatère de A_χ engendré par a . Soient A un anneau, M un A-module, I une partie non vide de M ou de A et n un nombre entier, $n \geqslant 1$. On notera $\int_n I$, l'ensemble des sommes $\sum_{i=1}^{m} x_i$, où $m \leqslant n$ et où $x_i \in I$, $i = 1,\ldots, n$.

L'application $I \to \int_n I$ de l'ensemble des idéaux multiplicatifs (resp. des parties multiplicativement stables) de A (resp. de M), dans lui-même, possède les propriétés suivantes :

1.6.1.) *Elle est isotone* ;

1.6.2.) *On a* : $I = \int_1 I \subset \ldots \subset \int_n I \subset \ldots$

1.6.3.) *Si* I *est un idéal de* A (resp. *un sous-module de* M), *on a* : $\int_n I = I$, *quel que soit* n ;

1.6.4.) *S'il existe un nombre entier* n, $n \geqslant 1$, *tel que* $\int_n I = \int_{n+1} I$, *alors* $\int_n I$ *est un idéal de* A (resp. *un sous-module de* M).

1.6.5.) *Si* $I_1, \ldots, I_n$ *sont des idéaux de* A (resp. *des sous-modules de* M), *alors* $\int_n (\bigcup_{i=1}^{n} I_i)$ *est l'idéal de* A (resp. *le sous-module de* M) *engendré par les* I_i.

1.6.6. – THEOREME. – *Soient* A *un anneau et* n *un nombre entier*, $n \geqslant 1$; *considérons les conditions suivantes* :

(i) *Pour tout idéal multiplicatif* I *de* A, $\int_n I$ *est un idéal de l'anneau* A ;

(ii) *La largeur de* A *est, au plus*, n ;

(iii) *Pour tout élément* a *de* A, $(a)_x$ *est un idéal de l'anneau* A (*et coïncide, par conséquent, avec l'idéal principal de* A *engendré par* a) ;

Alors, (i) *implique* (ii) *et l'ensemble des conditions* (ii) *et* (iii) *implique* (i).

Démonstration. (i) $\Longrightarrow$ (ii). D'après la condition (i), on a, pour toute famille $(I_\lambda)_{\lambda \in \Lambda}$ d'idéaux de A, l'égalité :

$$(1.6.6.1) \quad \sum_{\lambda \in \Lambda} I_\lambda = \int_n (\bigcup_{\lambda \in \Lambda} I_\lambda).$$

Soient $I_1, \ldots, I_n, I_{n+1}$, $n+1$ idéaux de A tels que les n premiers ne soient pas contenus dans l'idéal engendré par les n autres. Il existe donc, pour $i = 1, \ldots, n$, un élément x_i de I_i qui n'appartient pas à $I_1 + \ldots + I_{i-1} + I_{i+1} + \ldots + I_{n+1}$. Comme, d'après (1.6.6.1), on a : $I_1 + \ldots + I_{n+1} = \int_n (\bigcup_{i=1}^{n+1} I_i)$, il existe, si x est un élément de I_{n+1}, des éléments $y_{i_1}, \ldots, y_{i_k}$, $k \leqslant n$, $y_{i_j} \in I_{i_j}$, tels que :

$$(1.6.6.2) \quad x_1 + x_2 + \ldots + x_n + x = y_{i_1} + \ldots + y_{i_k}.$$

D'après le choix des x_s, il existe, pour $s = 1, \ldots, n$, un y_{i_j} qui appartient à I_s et n'appartient pas à $I_1 + \ldots + I_{s-1} + I_{s+1} + \ldots + I_{n-1}$. Donc $x \in I_1 + \ldots + I_n$ et I_{n+1} est contenu dans $I_1 + \ldots + I_n$.

(ii) et (iii) $\Longrightarrow$ (i). Puisque la condition (ii) est vérifiée, on a, pour $n+1$ idéaux de $I_1, \ldots, I_{n+1}$ de A, l'égalité :

$$(1.6.6.3) \quad \int_n (\bigcup_{k=1}^{n+1} I_k) = I_1 + \ldots + I_{n+1}.$$

Soit J un idéal multiplicatif de A et soient $a_1, \ldots, a_{n+1} \in J$. Puisque, d'après (iii), on a : $(a_i) = (a_i)_X$, alors $\int_n \left(\bigcup_{i=1}^{n+1} (a_i)\right) \subseteq \int_n J$. D'après (1.6.6.3) appliquée à $I_i = (a_i)$ $(a_1) + \ldots + (a_{n+1}) \subseteq \int_{n+1} J$ et $\int_{n+1} J = \int_n J$.

Puisque dans un anneau commutatif, la condition (iii) de 1.6.6. est toujours vérifiée, on a :

1.6.7. – Corollaire. – Si tous les idéaux multiplicatifs d'un anneau A sont des idéaux de A, le treillis des idéaux de A est totalement ordonné. Si A est un anneau commutatif et si le treillis des idéaux de A est totalement ordonné, tout idéal multiplicatif de A est un idéal de l'anneau A. (cf. [10]).

La partie multiplicativement stable, engendrée par un élément a d'un module M sur un anneau A coïncide avec le sous-module de engendré par a. On prouve, à l'aide d'un raisonnement analogue à celui de (1.6.6.), la proposition suivante :

1.6.8. – Proposition. – Soient A un anneau, M un A-module et n un nombre entier, $n \geqslant 1$. Les conditions suivantes sont équivalentes :

(i) Pour toute partie multiplicativement stable I de M, $\int_n I$ est un sous-module de M ;

(ii) La largeur de M est au plus n.

§ 7.– Théorème de Krull-Akizuki.

On peut donner une autre démonstration du théorème de Krull-Akizuki [cf. [15] ; p. 115 ; Th. (33.2)].

1.7.1. – THEOREME. – Soient R un anneau intègre noethérien, K son corps des quotients, L une extension algébrique finie de K et R' un anneau tel que $R \subseteq R' \subseteq L$. Si la dimension de R est 1, alors pour tout idéal $\mathfrak{a}'$ de R' tel que $\mathfrak{a}' \neq (0)$, $R'/\mathfrak{a}'$ est un module de longueur finie sur $R/(\mathfrak{a}' \cap R)$. En particulier R' est un anneau noethérien de dimension au plus 1.

Preuve. On se ramène tout de suite au cas où R est semi-local comme dans [15] (Loc. cit.). Posons $\mathfrak{a} = \mathfrak{a}' \cap R$ et soient $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ tous les diviseurs premiers de $\mathfrak{a}$. Puisque $\mathfrak{a}' \neq (0)$, on a $\mathfrak{a} \neq (0)$ et donc les idéaux premiers $\mathfrak{p}_i$ $(i = 1, \ldots, s)$ sont maximaux. Soit S le complémentaire dans R de la réunion $\bigcup_{i=1}^{s} \mathfrak{p}_i$. On a $R'/\mathfrak{a}' \simeq R'_S/\mathfrak{a}' R'_S$ et $R/\mathfrak{a} \simeq R_S/\mathfrak{a} R_S$. Par conséquent, on peut supposer que R est un anneau semi-local et que $\mathfrak{a}$ est contenu dans le radical $\mathfrak{m}$ de R. Puisque R est un anneau noethérien intègre, semi-local, de dimension 1 il est de largeur finie. Donc K est un R-module de largeur finie d'après 1.2.8.. Comme L est une extension algébrique finie de K , c'est un R-module de largeur finie d'après 1.2.12. . Donc R' est un R-module de largeur finie, et , par suite, $R'/\mathfrak{a}'$ est un $R/\mathfrak{a}$-module de largeur finie. D'après 1.3.2. (ii), $R'/\mathfrak{a}'$ est un $R/\mathfrak{a}$-module de longueur finie. Par suite, pour tout idéal $\mathfrak{a}'$ de R' , $\mathfrak{a}' \neq (0)$, $\frac{R'}{\mathfrak{a}'}$ est un anneau artinien. Il en résulte que R' est noethérien et que sa hauteur est $\leqslant 1$.

CHAPITRE II

Anneaux et modules de largeur 1 .

§ 1.- Anneaux de largeur gauche 1.

D'après 1.6.8., la largeur gauche d'un anneau A est égale à 1 si et seulement si tout idéal multiplicatif à gauche de A est un idéal à gauche de l'anneau A .

Un anneau A , dont la largeur gauche est égale à 1, est un anneau local ; son radical est l'unique idéal à gauche maximal de A et c'est un idéal complètement premier.

Rappelons qu'on appelle idéal complètement premier d'un anneau A , un idéal propre I de A tel que si $ab \in I$, où a et $b \in A$, alors a ou $b \in I$.

Un anneau A est dit complètement premier si l'idéal (0) est complètement premier.

Si I est un idéal propre d'un anneau A , on notera $\delta_d I$ (resp. $\delta_g I$), l'ensemble des diviseurs de zéro à droite (resp. à gauche) de A modulo I , i.e. :

$\delta_d I = \{ z$; il existe $u \in A$; $u \notin I$ tel que $uz \in I \}$

$\delta_g I = \{ z$; il existe $u \in A$; $u \notin I$ tel que $zu \in I \}$

$\delta_d I$ (resp. $\delta_g I$) est un idéal multiplicatif à droite (resp. à gauche) de A .

2.1.1. - Proposition. - *Si I est un idéal propre d'un anneau A dont la largeur gauche est égale à 1, alors $\delta_d I$ et $\delta_g I$ sont des idéaux bilatères complètement premiers de A.*

Démonstration. Il résulte de la définition de $\delta_d I$ et de $\delta_g I$ que si $ab \in \delta_d I$ (resp. $ab \in \delta_g I$), alors a ou $b \in \delta_d I$ (resp. a ou $b \in \delta_g I$). Il suffit donc de prouver que $\delta_d I$ et $\delta_g I$ sont des idéaux bilatères de A . Puisque $\delta_d I$ est un idéal multiplicatif à droite et que la largeur gauche de A est 1, il suffit, pour montrer que $\delta_d I$ est un idéal bilatère de A , de prouver que c'est un idéal multiplicatif à gauche. Soit $z \in \delta_d I$; il existe $u \in A$, $u \notin I$, tel que $uz \in I$. Soit $x \in A$. Si $x = cu$, alors $xz \in I$; d'où $xz \in \delta_d I$. Si $u = dx$, alors $d \notin I$ et l'on a $dxz \in I$. Par suite, $xz \in \delta_d I$. Pour montrer que $\delta_g I$ est un idéal bilatère il suffit de montrer que c'est un idéal à droite. Soit $z \in \delta g I$; il existe et $m(A)$ l'idéal maximal de A.

(i) Si l'idéal $m(A)$ n'est pas idempotent, il est principal à gauche ;

(ii) Si $m(A) = Aa$, $a \in A$, les seuls idéaux à gauche de A qui contiennent $I = \bigcap_{n=1}^{\infty} Aa^n$ sont les Aa^n et ils sont bilatères.

(iii) Si $m(A) = Aa$ et si a est nilpotent, la longueur du module A_s est finie ; sinon l'idéal I est complètement premier.

Démonstration. (i) Soient a et b deux éléments de $m(A)$ qui n'appartiennent pas à $m(A)^2$. On a, par exemple, $b = xa$, où $x \in A$; x n'appartient pas à $m(A)$. Donc x est une unité de A et $Ab = Aa$. Par suite $m(A) = Aa$.

(ii) Soit n un nombre entier, $n > 1$; si $a^{n-1} \neq 0$, on a $(1-xa)a^{n-1} \neq 0$ pour tout $x \in A$. Donc $a^{n-1} \notin Aa^n \subset$ et $Aa^n \subsetneqq Aa^{n-1}$. Si $c \in Aa^{n-1}$ et $c \notin Aa^n$, on a $c = xa^{n-1}$ où $x \in A$ et $x \notin m(A)$. Donc x est inversible et $Ac = Aa^{n-1}$. Il n'existe donc pas d'idéal à gauche de A strictement compris entre Aa^n et Aa^{n-1}. Puisque le treillis des idéaux à gauche de A est totalement ordonné, les seuls idéaux à gauche de A qui contiennent I sont les Aa^n. Puisque Aa est un idéal bilatère de A, on a $aA \subseteq Aa$; d'où $a^nA \subseteq Aa^n$ pour tout n et Aa^n est un idéal bilatère de A.

(iii) Si a est nilpotent, la longueur du module A_s est finie, d'après (ii). Si a n'est pas nilpotent, soit $xy \in I$, et x et $y \notin I$. Alors, il existe deux entiers positifs n et m et deux unités c et d de A tels que $x = ca^n$ et $y = da^m$; on a $a^n da^m \in I$ et $a^n d \in I$; d'où $a^n d = fa^t$, où f est une unité de A et t un entier > 0. Par conséquent, $a^{t+m} \in I$, ce qui est impossible. Donc I est complètement premier.

2.1.6. - Définition. - Un anneau A est dit dual si l'on a : $Aa = aA$, pour tout $a \in A$.

2.1.7. - Proposition. - Soit A un anneau dont la largeur gauche est égale à 1 et dont l'idéal maximal $m(A)$ est principal à gauche ; soit $m(A) = Aa$.

(i) Si la largeur droite de A est égale à 1, on a $Aa = aA$ et A/I, où $I = \bigcap_{n=1}^{\infty} Aa^n$, est un anneau dual ;

(ii) Si $Aa = aA$, la largeur droite de l'anneau A/I est égale à 1.

Démonstration. (i) Puisque la largeur droite de A est 1 et que l'idéal maximal de A n'est pas idempotent, on a, d'après le symétrique de 2.1.5. (i), $m(A) = Aa = bA$, où $b \in A$. Puisque $b \notin m(A)^2$, on a $b = xa$, où x est une unité de A et $Aa = aA$. Il résulte de 2.1.5. (ii) et de son symétrique que l'anneau A/I est dual.

$u \in A$, $u \notin I$, tel que $zu \in I$. Soit $x \in A$; si x est inversible, on a $zu = zxx^{-1}u \in I$ et $x^{-1}u \notin I$; donc $zx \in \delta_g I$. Si x n'est pas inversible, $1+x$ l'est, par suite, $z(1+x) \in \delta_g I$; d'où $zx \in \delta_g I$.

Un idéal propre d'un anneau A est dit <u>premier</u> s'il vérifie l'une ou l'autre des conditions équivalentes suivantes :

$I.J \subseteq P$, I et J idéaux de A $\Longrightarrow$ I ou $J \subseteq P$

$aAb \subset P$, a et $b \in A$ $\Longleftrightarrow$ a ou $b \in P$.

Un anneau A est dit <u>premier</u> si l'idéal (0) est premier.

2.1.2. – <u>Définition</u>. – On appelle 1-E-<u>anneau</u> (1-equivalence ring) tout anneau B , non nécessairement unitaire, qui vérifie la condition suivante : (cf. [13]).

Si a et $b \in B$ et si $b \neq 0$, il existe p et $q \in B$ tels que $a = pbq$.

2.1.3. – THEOREME; – <u>Soient</u> A <u>un anneau dont la largeur gauche est égale à</u> 1 <u>et</u> I <u>un idéal propre de</u> A . <u>Si</u> I <u>est premier et n'est pas complètement premier, il existe un idéal minimum</u> M <u>le contenant</u> ; M <u>est complètement premier ; on a</u> $M = \delta_g I$; <u>l'anneau</u> M/I <u>est un</u> 1-E-<u>anneau</u>.

<u>Démonstration</u>. On peut passer au quotient par I et supposer que $I = (0)$. Puisque la largeur gauche de A est 1 , $\delta_g(0)$ est, d'après 2.1.1., un idéal complètement premier de A . Puisque A n'est pas complètement premier, on a $\delta_g(0) \neq (0)$. Soit J un idéal bilatère de A tel que $J \subsetneq \delta_g(0)$. Il existe $a \in \delta_g(0)$ et $a \notin J$. D'où $J \subset Aa$. Par définition de $\delta_g(0)$ il existe $u \in A$ $u \neq 0$, tel que $au = 0$; d'où $Ju = (0)$ et, puisque A est premier, $J = (0)$. Par conséquent $\delta_g(0)$ est un idéal minimum de A . Soit $x \in \delta_g(0)$, $x \neq 0$. L'ensemble $\{pxq,\ p$ et $q \in \delta_g(0)\}$, est un idéal multiplicatif bilatère de A . Donc, puisque la largeur gauche de A est 1 , c'est un idéal bilatère de A ; il n'est pas nul. Donc il coïncide avec $\delta_g(0)$. Par suite $\delta_g(0)$ est un 1-E-anneau.

2.1.4. – <u>Corollaire</u>. – <u>Soient</u> A <u>un anneau dont les largeurs droite et gauche, sont égales à</u> 1 . <u>Si</u> I <u>est un idéal premier et non complètement premier de</u> A , <u>il existe un idéal minimum</u> M <u>contenant</u> I ; M <u>est complètement premier et</u> $M = \delta_d I = \delta_g I$.

<u>Démonstration</u>. Puisque la largeur gauche de A est égale à 1 , $\delta_g I$ est l'idéal minimum qui contient I , d'où $\delta_g I \subseteq \delta_d I$. Puisque la largeur droite de A est 1 ; $\delta_d I$ est l'idéal minimum qui contient I . D'où $\delta_g I = \delta_d I$.

Le théorème 2.1.3. a été trouvé indépendamment par E. C. Posner [17].

2.1.5. – <u>Proposition</u>. – <u>Soient</u> A <u>un anneau dont la largeur gauche est égale à</u> 1

(ii) On peut supposer que $I = (0)$. Soient s un entier >0 et c une unité de A ; de l'égalité $Aa = aA$, il résulte que $ca^s = a^s c'$, où c' est une unité de A. Par suite, la largeur droite de A est égale à 1.

§ 2.- Anneaux complètement premiers de largeur gauche 1.

Tous les anneaux considérés dans ce paragraphe sont supposés complètement premiers.

Un anneau A est dit régulier à gauche (resp. à droite) si l'intersection de deux idéaux à gauche (resp. à droite) non nuls de A n'est pas nulle. Un anneau A, régulier à gauche, peut être plongé dans un corps K, appelé corps des quotients à gauche de A ; tout élément de K se met sous la forme $a^{-1}b$, où a et $b \in A$, $a \neq 0$. Si, de plus A est régulier à droite, K est isomorphe au corps des quotients à droite de A, dans un isomorphisme qui laisse inchangés les éléments de A (cf. [9] ; Chap. V ; p. 280-283) ; on identifiera, alors, ces deux corps à un même sur-corps de A que l'on appellera le corps des quotients de A.

Soient K un corps et A un sous-anneau de K. Nous aurons à considérer les ensembles suivants :

$$S_0 = \{s \in K \; ; \; s \text{ et } s^{-1} \notin A\}$$

$S_1 = \{s \in K \,,\, s \neq 0 \,,\, A \cap sA = (0)\}$ $\qquad$ $S_1' = \{s \in K \,,\, s \neq 0 \,,\, A \cap As = (0)\}$

$D = K - (A \cup S_1)$ (complémentaire de $A \cup S_1$ dans K) $\quad D' = K - (A \cup S_1')$

Alors : $D = \{x \in K \,,\, x \notin A \text{ et } x = ab^{-1} \,,\, \text{où } a \text{ et } b \in A\}$

$D' = \{x \in K \,,\, x \notin A \text{ et } x = b^{-1}a \,,\, \text{où } a \text{ et } b \in A\}$

On a l'inclusion : $S_1 \cup S_1' \subsetneq S_0$.

L'ensemble S_1' (resp. S_1) est vide si et seulement si K est le corps des quotients à gauche (resp. à droite) de A.

2.2.1. - THEOREME. - Les conditions suivantes sont équivalentes :

(i) $S_1 = S_0$;

(ii) La largeur gauche de l'anneau A est égale à 1 ;

(iii) D est une partie multiplicativement stable de K.

Démonstration. (i) $\Longrightarrow$ (ii) Soient x et $y \in A$, x et $y \neq 0$; on a $xy^{-1}.y = x$; donc $xy^{-1} \notin S_1$. D'où $xy^{-1} \notin S_0$; par suite, xy^{-1} ou bien $yx^{-1} \in A$ et la largeur gauche de A est égale à 1.

(ii) $\Longrightarrow$ (iii). Si (ii) est vérifiée, D est l'ensemble des éléments x de K tels que $x \notin A$ et $x^{-1} \in A$. Par suite, si x et $y \in D$, on a $(xy)^{-1} \in A$ et $xy \notin A$.

(iii) $\Longrightarrow$ (i). Soit $s \in S_0$; si $s \notin S_1$, alors $s^{-1} \notin S_1$. Donc s et $s^{-1} \in D$;

d'où $1 \in D$, ce qui est impossible ; donc $s \in S_1$ et $S_o = S_1$.

2.2.2. - Corollaire. - *Soient K un corps et A un sous-anneau de K ; les conditions suivantes sont équivalentes :*

(i) *Quel que soit* $x \in K$, *on a* x *ou* $x^{-1} \in A$;

(ii) *Le complémentaire de A dans K est une partie multiplicativement stable de K* ;

(iii) *La largeur du A-module à droite K est égale à 1* ;

(iv) *La largeur du A-module à gauche K est égale à 1* .

Démonstration. L'équivalence (i) $\Leftrightarrow$ (ii) résulte de 2.2.1. ; en effet, (i) signifie que S_o est vide ; donc S_1 est vide et $D = K - A$ est une partie multiplicativement stable de K . Si (ii) est vérifiée et si s et $s^{-1} \notin A$, alors $1 \in K - A$, ce qui est impossible ; donc $S_o = \emptyset$. Démontrons, par exemple, que (i) $\Leftrightarrow$ (iii). Soient x et $y \in K$, x et $y \neq 0$; on a soit $x^{-1}y$ soit $y^{-1}x \in A$; donc yA et xA sont comparables. Si (iii) est vérifiée et si $x \in K$, $x \notin A$, on a $A \subset xA$ et $x^{-1} \in A$.

Un anneau A , de largeur gauche 1 , est régulier à gauche et possède un corps des quotients à gauche.

2.2.3. - THEOREME. - *Soient A un anneau de largeur gauche 1 et K le corps des quotients à gauche de A . Les conditions suivantes sont équivalentes :*

(i) *Le A-module à gauche K est de largeur 1* ;

(ii) *La largeur droite de l'anneau A est égale à 1* ;

(iii) *L'anneau A est régulier à droite.*

Si ces conditions sont réalisées, les largeurs, droite et gauche, de tous les sur-anneaux de A , contenus dans K , sont égales à 1 .

Démonstration. L'implication (i) $\Rightarrow$ (ii) résulte de l'implication (2.2.2. (iii) $\Rightarrow$ (2.2.2. (iv)) . L'implication (ii) $\Rightarrow$ (iii) est évidente. Si (iii) est vérifiée $S_1 = \{s \in K \ , \ s \neq 0 \ , \ A \cap sA = (0)\}$ est vide. Donc l'ensemble $D = K - A \cup S_1$ est le complémentaire de A dans K . D'après 2.2.1., D est une partie multiplicativement stable de K . Donc, d'après 2.2.2., la largeur du A-module à gauche K est égale à 1 . La fin du théorème résulte de 2.2.2. .

Exemple d'anneau dont la largeur gauche est égale à 1 et qui n'est pas régulier à droite. Soient K un corps, gauche ou non, et H un sous-corps de K , $H \neq K$. Soit φ un isomorphisme de K sur H . Dans l'ensemble $A = K[[X]]_\varphi$ des "séries formelles", on pose $Xa = \varphi(a)X$ pour $a \in K$. Alors A est un anneau et un élément $f = \sum_{i \geqslant 0} a_i X^i$ est inversible si et seulement si $a_o \neq 0$. Si f et g sont deux éléments, non nuls, de A , on peut écrire $f = f'X^m$ et $g = g'X^n$ où f' et g' sont inversibles et où m et n sont des entiers $\geqslant 0$. Alors, $f = f'X^{m-n} g'^{-1} g$ si $m \geqslant n$; donc la largeur gauche de A est égale à 1 . Si $f = a_1 X + \ldots + a_n X^n + \ldots$ est une série formelle dont aucun des coefficients a_i n'appartient à $H = \varphi(K)$, alors $f \neq Xg$ et $X \neq fg$, quel que soit $g \in A$. La largeur droite de A est donc différente de 1 .

Rappelons la définition d'une valuation d'un corps K , non nécessairement commutatif [22].

2.2.4. - <u>Définition</u>. - Soit Γ un groupe totalement ordonné non nécessairement commutatif dont l'opération est notée additivement et auquel on adjoint un élément ∞ assujetti aux conditions suivantes :

$$\alpha < \infty \quad \text{pour tout} \quad \alpha \in \Gamma$$

$$\alpha + \infty = \infty + \alpha = \infty + \infty = \infty \quad \text{pour tout} \quad \alpha \in \Gamma$$

Soit K un corps gauche ; une application v de K sur $\Gamma \cup \infty$ est appelée une <u>valuation</u> de K si les conditions suivantes sont satisfaites :

(i) $v(a + b) \geqslant \text{Min.}(v(a), v(b))$ quels que soient a et $b \in K$;

(ii) $v(ab) = v(a) + v(b)$ quels que soient a et $b \in K$;

(iii) On a $v(a) = \infty$ pour un élément a de K si et seulement si $a = 0$.

Dans ces conditions, l'ensemble A des éléments a de K tels que $v(a) \geqslant 0$ est un anneau, appelé l'anneau de valuation de K relatif à la valuation v . L'anneau A est dual et le treillis de ses idéaux est totalement ordonné.

Le théorème suivant ([22] ; Chap. I ; § 3 ; th. 3) donne une caractérisation d'un anneau de valuation d'un corps gauche.

2.2.5. - THEOREME. - <u>Soient</u> K <u>un corps et</u> A <u>un sous-anneau de</u> K . <u>Alors</u> A <u>est l'anneau d'une valuation de</u> K <u>si et seulement si les conditions suivantes sont vérifiées</u> :

(i) <u>On a</u> : $a^{-1}Aa = A$ <u>pour tout élément non nul de</u> K ;

(ii) <u>Si</u> $a \in K$, <u>alors</u> a <u>ou</u> $a^{-1} \in A$.

Nous appellerons <u>automorphisme intérieur</u> d'un corps K tout automorphisme intérieur du groupe multiplicatif $K - (0)$.

2.2.6. - THEOREME. - <u>Soient</u> A <u>un anneau dont les largeurs, droite et gauche, sont égales à</u> 1 <u>et</u> K <u>le corps des quotients de</u> A ; <u>les conditions suivantes sont équivalentes</u> :

(i) A <u>est un anneau de valuation de</u> K ;

(ii) A <u>est un anneau dual</u> ;

(iii) <u>Le groupe des unités de</u> A <u>est un sous-groupe normal du groupe multiplicatif</u> $K - (0)$;

(iv) <u>Si</u> a <u>et</u> $b \in A$, <u>on a</u> $aA \subseteq bA$ <u>si et seulement si</u> $Aa \subseteq Ab$;

(v) <u>L'idéal maximal de</u> A <u>est invariant par tous les automorphismes intérieurs de</u> K ;

<u>Démonstration</u>. L'équivalence (i) $\rightleftarrows$ (ii) résulte de 2.2.5. . L'anneau A vérifie (iv) si et seulement si $Aa = aA$ quel que soit $a \in A$; i.e. si et seulement si A est un anneau dual.

(i) $\Rightarrow$ (iii). Pour tout élément non nul x de K on a : $xAx^{-1} = A$. Si a est une unité de A , alors, a et $a^{-1} \in A$; d'où xax^{-1} et $xa^{-1}x^{-1} \in A$ et xax^{-1} est une unité de A .

L'implication (iii) $\Rightarrow$ (v) résulte de ce que le groupe des unités de A est un sous-groupe normal de $K - (0)$ et du fait que $1 + y$ est une unité de A , si y appartient à l'idéal maximal de A .

(v) $\Rightarrow$ (i). Soient $x \in K$, $x \neq 0$, et $a \in A$. Si a appartient à l'idéal maximal $m(A)$ de A , alors, $xax^{-1} \in m(A) \subset A$. Si $a \notin m(A)$, alors $a^{-1} \notin m(A)$, puisque $a \in A$; donc $xa^{-1}x^{-1}$ n'appartient pas à $m(A)$; d'où, d'après 2.2.4., $xax^{-1} \in A$.

2.2.7. - THEOREME. - <u>Soient</u> A <u>un anneau dont les largeurs, droite et gauche, sont égales à</u> 1 , K <u>le corps des quotients de</u> A <u>et</u> $m(A)$ <u>l'idéal maximal de</u> A. <u>Les conditions suivantes sont équivalentes</u> :

(i) A <u>contient un anneau de valuation de</u> K ;

(ii) <u>Si</u> a <u>et</u> $b \in A$ <u>et si</u> $aA \subsetneq bA$, <u>alors</u> $Aa \subseteq Ab$;

(iii) <u>L'image de</u> $m(A)$ <u>par tout automorphisme intérieur de</u> K <u>est contenu dans</u> A .

<u>Démonstration</u>. (i) $\Rightarrow$ (ii). Soit B un anneau de valuation de K , $B \subseteq A$. Soient a et b dans A tels que $aA \subsetneq bA$; alors $b^{-1}a \in m(A)$. On a donc nécessairement $b^{-1}a \in B$ et, puisque B est un anneau dual, $Ba \subset Bb$. Par suite : $Aa \subseteq Ab$.

(ii) $\Rightarrow$ (iii). La condition (ii) est évidemment équivalente à la condition suivante : si x et $y \in K$ et si $xA \subsetneq yA$, alors $Ax \subseteq Ay$. Soient $a \in m(A)$ et $x \in K$, $x \neq 0$; alors $aA \subsetneq A$; d'où $xaA \subsetneq xA$. Par suite : $Axa \subseteq Ax$ et $xax^{-1} \in A$.

(iii) $\Rightarrow$ (i). L'ensemble $B = \{x \in A \text{ , } zxz^{-1} \in A \text{ quel que soit } z \in K - (0)\}$ est un sous-anneau de A et il contient $m(A)$. L'anneau B est évidemment conservé par tous les automorphismes intérieurs de K ; par suite il est dual. Soit $x \in K$, $x \notin B$. Si $x \notin A$ alors $x^{-1} \in m(A)$ et $x^{-1} \in B$. Si $x \in A$, il existe $z \in K$, $z \neq 0$, tel que $zxz^{-1} \notin A$. Donc $zx^{-1}z^{-1} \in m(A) \subset B$. Donc $x^{-1} \in B$ et B est un anneau de valuation de K.

Soient K un corps et S un sous-ensemble de $K - (0)$; nous noterons S^{-1} l'ensemble des $x \in K$, $x \neq 0$, $x^{-1} \in S$.

2.2.8. – THEOREME. – <u>Soient</u> A <u>un anneau de largeurs, droite et gauche, égales à</u> 1, K <u>le corps des quotients de</u> A <u>et</u> $m(A)$ <u>l'idéal maximal de</u> A. <u>Il existe une correspondance biunivoque entre l'ensemble des sur-anneaux de</u> A <u>contenus dans</u> K <u>et l'ensemble des idéaux complètement premiers de</u> A ; <u>celle qui à un anneau</u> B, $A \subseteq B \subseteq K$, <u>associe l'idéal maximal</u> $m(B)$ <u>de</u> B <u>et à un idéal complètement premier</u> P <u>de</u> A <u>associe l'anneau</u> $B = A \cup S^{-1}$, <u>où</u> S <u>est le complémentaire de</u> P <u>dans</u> A. <u>Dans cette correspondance, les anneaux de valuation de</u> K <u>qui contiennent</u> A <u>sont associés aux idéaux complètement premiers de</u> A <u>qui sont conservés par tous les automorphismes intérieurs de</u> K.

<u>Démonstration</u>. Soit B un sur-anneau de A contenu dans K ; les largeurs droite et gauche de B sont égales à 1. Donc B est un anneau local. Soit $m(B)$ son idéal maximal. Si $x \in B$ et $x \notin A$, alors $x^{-1} \in A$ et x est une unité de B. Donc $m(B) \subset A$. On a évidemment $B = A \cup S^{-1}$ où $S = m(A) - m(B)$. Soient P un idéal complètement premier de A et $S = m(A) - P$. L'ensemble $B = A \cup S^{-1}$ contient A. Puisque P est un idéal complètement premier, les ensembles S et S^{-1} sont multiplicativement stables. Puisque les largeurs, droite et gauche, du A-module K sont égales à 1, il suffit, d'après 1.6.8., pour prouver que B est un anneau, de prouver qu'il est multiplicativement stable à gauche et à droite par A. Si $a \in A$ et $b \in S^{-1}$ et si $ab \notin B$ (resp. $ba \notin B$), alors $b^{-1}a^{-1} \in P$ (resp. $a^{-1}b^{-1} \in P$). D'où $b^{-1} \in P$, ce qui est impossible. L'idéal P est évidemment l'idéal maximal de B. La fin du théorème résulte de 2.2.6. (v).

Un anneau de valuation propre B d'un corps K est de <u>rang 1</u> si les seuls idéaux premiers de B qui sont stables par tous les automorphismes intérieurs de K sont (0) et l'idéal maximal de B.

Dans un anneau dual tout idéal premier est complètement premier.

Soient K un corps et B un sous-anneau (resp. un sous-anneau dual) de K ; nous dirons que B est un <u>sous-anneau maximal</u> (resp. un <u>sous-anneau dual maximal</u>) de K, si une relation $B \subsetneq A \subseteq K$, où A est un anneau (resp. un anneau dual) entraîne : $K = A$.

Il résulte de 2.2.8., le corollaire suivant :

2.2.9. - Corollaire. - Soit B un anneau de valuation propre d'un corps K ; alors

(i) Le rang de B est égal à 1 si et seulement si B est un sous-anneau dual maximal de K ;

(ii) Les seuls idéaux premiers de B sont (0) et son idéal maximal si et seulement si B est un sous-anneau maximal de K.

2.2.10.- Proposition. - Soient A un anneau régulier à gauche, V son centre et F le corps des quotients de V. Les conditions suivantes sont équivalentes :

(i) L'anneau $S^{-1}A$, où $S = V - (0)$, est un corps ;

(ii) Quel que soit $x \in A$, il existe $y \in A$, $y \neq 0$, tel que $xy = yx \in V$.

Si ces conditions sont réalisées, l'anneau A est régulier à droite et le corps des quotients de A est $S^{-1}A$.

Démonstration. (i) $\Longrightarrow$ (ii). Si K est le corps des quotients à gauche de A, alors $K = S^{-1}A$. Donc, si $x \in A$, $x \neq 0$, on a $x^{-1} = s^{-1}y$, où $y \in A$ et $s \in V$, $s \neq 0$; d'où $xy = yx = s$ avec $s \in V$ et $y \neq 0$.

(ii) $\Longrightarrow$ (i). Soit $y \in K$; il existe a et $b \in A$, $a \neq 0$, tels que $ay = b$. Soit a' un élément non nul de A pour lequel $a'a = s \in V$. Alors $y = s^{-1}a'b$ et $K = S^{-1}A$.

Si la condition (i) est satisfaite, on a, quel que soit $x \in K$, $x = s^{-1}a = as^{-1}$, où $a \in A$ et $s \in V$, $s \neq 0$; donc A est régulier à droite.

2.2.11.- THEOREME. - Soient A un anneau dont les largeurs, droite et gauche, sont égales à 1, K le corps des quotients de A, V le centre de A, et F celui de K. Si K est algébrique sur F, on a : $K = V^{*-1}A$, où $V^* = V - (0)$.

Démonstration. Le centre V de A est contenu dans F et est un anneau de valuation de F. Donc F est contenu dans l'anneau $C = V^{*-1}A$. D'autre part, C est un sur-anneau de A contenu dans K ; donc, si $x \in K$ et si $x \notin C$, on a : $x^{-1} \in C$. Puisque K est algébrique sur F, on a $x^n + f_1x^{n-1} + \ldots + f_n = 0$, où $n > 1$ et $f_i \in F$. Donc $x + f_1 + f_2x^{-1} + \ldots + f_nx^{-n+1} = 0$ et $x \in C$, ce qui contredit le choix de x. Par suite, $C = K = V^{*-1}A$.

§ 3.- Anneaux commutatifs de largeur 1.

Tous les anneaux considérés dans ce paragraphe sont supposés commutatifs.

2.3.1. - Définition. - Un anneau A est complètement primaire si sa racine, i.e. l'ensemble de ses éléments nilpotents, est l'unique idéal maximal de A.

S. J. Bryant et J. L. Zemmer ont démontré le théorème suivant ([5]).

2.3.2. - THEOREME. - Soient B un anneau complètement primaire de caractéristique 0 et N l'idéal maximal de B. L'anneau B possède un sous-corps F qui est isomorphe au corps résiduel B/N et tout élément a de B peut s'écrire d'une manière unique sous la forme : $a = f + n$, où $f \in F$ et $n \in N$.

I. S. Cohen a démontré le théorème suivant, que nous utiliserons dans le cas où la caractéristique de l'anneau est $p \neq 0$ ([6]).

2.3.3. - THEOREME. - Si A est un anneau local artinien d'égales caractéristiques, A possède un sous-corps F qui est isomorphe au corps résiduel de A ; le groupe additif A_+ de A admet la décomposition en somme directe $A_+ = N \oplus F$, où N est l'idéal maximal de A.

Si P est un idéal premier d'un anneau A, on désignera par A_P l'anneau des fractions A_P à "dénominateurs" dans $A-P$.

2.3.4. - THEOREME. - Soit A un anneau de largeur 1 dont la racine N coïncide avec l'idéal des diviseurs de zéro de A. On suppose que l'une ou l'autre des conditions suivantes est réalisée :

(i) La caractéristique de A est 0 ;

(ii) La caractéristique de A est un nombre premier p et l'idéal N est nilpotent.

Alors, l'anneau A contient un sous-anneau V, isomorphe à l'anneau A/N ; V est un anneau de valuation d'un corps F ; N est une F-algèbre dont le treillis des idéaux est totalement ordonné ; le groupe additif de A est somme directe des groupes additifs de N et de V.

Démonstration. Puisque N est l'ensemble des diviseurs de zéro de A, l'anneau A est isomorphe à un sous-anneau de A_N auquel nous l'identifierons. La largeur de l'anneau A_N est égale à 1 et il a même caractéristique que A. L'anneau A_N est complètement primaire et son idéal maximal est NA_N. Si $a \in N$ et $s \in A$, $s \notin N$ il existe $b \in A$ tel que $a = bs$; puisque N est un idéal premier de A, on a : $b \in N$ et, par suite, $N = NA_N$. D'après 2.3.2. et 2.3.3., l'anneau A_N contient un sous-corps F isomorphe à A_N/N et tel que $(A_N)_+$ est somme directe de F et de N. Les idéaux de la F-algèbre N étant les idéaux de l'anneau A_N : le treillis des idéaux de la F-algèbre N est totalement ordonné. Soit $V = F \cap A$. On a : $A_+ = (N \oplus F) \cap A = N \oplus F$, puisque N est contenu dans A. Le corps F est évidemment le corps des quotients de l'anneau V, soient x et $y \in V$. On a, par exemple, $x = uy$ où $u \in A$. Donc $u = n + v$, où $n \in N$ et $v \in V$; donc $x = ny+vy$. Puisque x et $vy \in V$, on a $ny \in V \cap N$; d'où $ny = 0$ et $n = 0$. Par conséquent $u \in V$ et V est un anneau de valuation de F.

Rappelons le résultat suivant (cf. 8).

2.3.5. - Proposition. - *Soient K un corps de caractéristique $p \neq 0$ et H un groupe cyclique d'ordre p^m. Alors, l'algèbre $A = K[H]$ de H sur K est un anneau de largeur 1.*

2.3.6. - Proposition. - *Soient K un corps commutatif et H un groupe, $H \neq \{1\}$; si l'algèbre $K[H]$ de H sur K est de la forme $K[X]/(X^n)$, où $K[X]$ est l'anneau des polynômes en X sur K, alors la caractéristique de K est $p \neq 0$, H est un groupe cyclique d'ordre p^m et $n = p^m$.*

Démonstration. Le groupe H est nécessairement commutatif fini. Puisque H est supposé différent de $\{1\}$, l'entier n est strictement supérieur à 1. Puisque l'algèbre $K[H]$ n'est pas semi-simple, la caractéristique p du corps K n'est pas nulle et elle divise l'ordre de H. Soient H_p le p-sous-groupe maximal de H et $H = H_p . L$ la décomposition de H en produit direct correspondant. L'ordre du groupe L étant premier à p, l'anneau $K[L]$ est semi-simple ; par suite, $K[L]$ est somme directe finie : $K_1 \oplus \dots \oplus K_s$, de corps K_i qui sont des extensions de K. Donc $K[H] = K[H_p] \otimes_K K[L]$ est isomorphe à la somme directe des produits tensoriels $K[H_p] \otimes_K K_i$, $i = 1,\dots,s$. L'anneau $K[X]/(X^n)$ étant indécomposable, on a : $s = 1$ et $K[L]$ est un sur-corps de K. Mais K étant un sous-corps maximal de $K[X]/(X^n)$ on a : $K[L] = K$ et $L = \{1\}$. Par suite, H est un p-groupe ; soit p^m son ordre. Alors, p^m est égal à la dimension du K-espace vectoriel $K[H]$, i.e. à n. Le radical de $K[H]$, coïncidant avec l'idéal d'augmentation engendré par les éléments de la forme $b-1$, où $b \in H$, l'exposant du groupe H ne peut être strictement inférieur à p^m. Donc H possède un élément d'ordre p^m et il est cyclique.

2.3.7. - Proposition. - *Soient K un corps de caractéristique p et H un groupe multiplicatif isomorphe au groupe additif des entiers p-adiques et H_s le groupe quotient de H par H^{p^s}. Alors, l'algèbre complété A de H par K, i.e. la limite projective : $A = \varprojlim K[H_s]$ est un anneau de valuation discrète complet de son corps des quotients.*

Démonstration. Soit u_s l'isomorphisme de $K[H_s]$ sur $K[X]/(X^{p^s})$ qui au générateur a_s du groupe cyclique H_s fait correspondre la classe, modulo (X^{p^s}) de $1-X$. Les u_s forment un système projectif d'isomorphismes et l'anneau $A = \varprojlim K[H_s]$ est isomorphe à $\varprojlim K[X]/(X^{p^s})$ qui est l'anneau des séries formelles en X sur K.

§ 4.- Modules projectifs de largeur 1 .

Nous dirons qu'un anneau est noethérien (resp. artinien) s'il est noethérien à droite et à gauche (resp. artinien à droite et à gauche).

Rappelons qu'un idempotent e , non nul, d'un anneau A est dit primitif s'il n'est pas somme de deux idempotents non nuls orthogonaux.

2.4.1. - THEOREME. - *Soient A un anneau noethérien à gauche et N le radical de A ; les conditions suivantes sont équivalentes :*

(i) *Tout A-module à gauche de type fini indécomposable et projectif est de largeur 1 ;*

(ii) *Le A-module à gauche A_s admet une décomposition en somme directe :*

(2.4.1.1) $A_s = \bigoplus_{i=1}^{n} Ae_i$

dans laquelle les e_i sont des idempotents primitifs deux à deux orthogonaux et les seuls sous-modules de Ae_i sont les $N^k e_i$ (k entier $\geqslant 0$) et, éventuellement, (0).

Démonstration. (i) $\Longrightarrow$ (ii). Soit $A_s = \bigoplus_{i \in I} L_i$ une décomposition de A_s en somme directe de sous-modules indécomposables ; alors l'ensemble d'indice I est fini, on a $L_i = Ae_i$, $i \in I$ où e_i est un idempotent primitif de A , les e_i sont deux à deux orthogonaux et $1 = \sum_{i \in I} e_i$. D'après (i), la largeur de Ae_i est égale à 1 . Si k est un entier $\geqslant 0$, et si $N^k e_i \neq (0)$, on a, d'après le lemme de Nakayama, $N^k e_i \neq N^{k+1} e_i$. Le A-module $N^k e_i / N^{k+1} e_i$, étant semi-simple et de largeur 1 , est simple. Alors, si M est un sous-A-module de Ae_i et si $M \subseteq N^k e_i$, $M \not\subseteq N^{k+1} e_i$, on a : $N^k e_i = M + N^{k+1} e_i$; d'où, d'après le lemme de Nakayama, $M = N^k e_i$ et les seuls sous-modules de Ae_i sont (0) et les $N^k e_i$.

(ii) $\Longrightarrow$ (i). De la décomposition (2.4.1.1), il résulte la décomposition $A/N = \bigoplus_{i=1}^{n} (A/N)\bar{e}_i$, où $\bar{e}_i$ désigne la classe de e_i modulo N . Puisque e_i est un idempotent et que $(A/N)\bar{e}_i$, isomorphe à Ae_i/Ne_i , est un module simple, $\bar{e}_i$ est un idempotent primitif de A/N et l'anneau A/N est semi-simple ; donc si M est un A/N-module simple, il existe un e_i tel que M soit isomorphe à Ae_i/Ne_i . Soient P un A-module à gauche de type fini, indécomposable et projectif, et M un module simple, facteur direct du A-module semi-simple P/NP ; il existe un idempotent $e = e_i$ de la décomposition de A_s , tel que M est isomorphe à Ae/Ne . Il existe donc un homomorphisme surjectif $\varphi : P \longrightarrow Ae/Ne$. Puisque P est projectif, il existe un homomorphisme $f : P \longrightarrow Ae$ tel que $\theta f = \varphi$, où θ désigne l'homomorphisme canonique : $Ae \longrightarrow Ae/Ne$. Puisque φ est surjectif et que $f(P) = N^s e$, s entier $\geqslant 0$, on a : $s = 0$ et $f(P) = Ae$. Donc f est surjectif. Puisque Ae est un module projectif, il existe un homomorphisme $g : Ae \longrightarrow P$ tel que fg est l'identité de Ae. Alors P est égal à la somme directe $gf(P) \oplus Q$, où Q est le noyau de f et, puisque P est indécomposable, on a : $Q = (0)$. Par suite f est un isomorphisme et P est de largeur 1.

En utilisant les décompositions en somme directe de modules à gauche (resp. à droite) indécomposables des anneaux artiniens, on prouve facilement la proposition suivante :

2.4.2. – Proposition. – Soient A un anneau et N son radical ; si A est séparé et complet pour la topologie N-adique et si quel que soit l'entier k, $k > 0$, l'anneau A/N^k est artinien, alors, l'anneau A admet les décompositions en somme directe $A = \bigoplus_{i=1}^{n} Ae_i = \bigoplus_{i=1}^{n} e_iA$, où les e_i sont des idempotents primitifs deux à deux orthogonaux de A.

Un anneau A est dit involutif s'il vérifie l'une ou l'autre des conditions suivantes :

(i) L'anneau A est artinien et les modules A_s et A_d sont injectifs ;

(ii) L'anneau A est artinien et l'on a : $0^{\cdot}.(0.^{\cdot}L) = L$ et $0.^{\cdot}(0^{\cdot}.R) = R$ pour tout idéal à gauche L et tout idéal à droite R.

Dans un anneau involutif, le socle gauche, idéal engendré par les idéaux à gauche minimaux, et le socle droit, idéal engendré par les idéaux à droite minimaux, coïncident et cet idéal est l'annulateur, à droite ou à gauche, du radical de l'anneau. Si e est un idempotent primitif de A, le module Ae (resp. eA) possède un sous-module minimal unique qui est Se (resp. eS), où S est le socle de A. Pour tout ce qui concerne les anneaux involutifs, nous renvoyons à [8].

2.4.3. – Définition. – Soient A un anneau, N son radical. Nous dirons que A est involutif restreint s'il est noethérien, séparé et complet pour la topologie N-adique et si, pour tout entier $k > 0$, l'anneau A/N^k est involutif et a pour socle N^{k-1}/N^k, si $N^{k-1} \neq (0)$.

2.4.4. – THEOREME. – Si A est un anneau involutif restreint, tout A-module, à droite ou à gauche, de type fini, indécomposable et projectif, est de largeur 1 ; si, de plus, A est artinien tout A-module indécomposable est de largeur 1.

Démonstration. D'après 2.4.2., on a : $A_s = \bigoplus_{i=1}^{n} Ae_i$, où e_i est un idempotent primitif. Soit L un sous-module non nul de Ae_i et soit k le plus grand entier pour lequel on a : $L \subseteq N^k e_i$. D'après 2.4.3., $N^k e_i/N^{k+1} e_i$ est l'unique sous-module minimal de $Ae_i/N^{k+1} e_i$. Donc $L + N^{k+1} e_i = N^k e_i$ et, d'après le lemme de

Nakayama, on a : $L = N^k e_i$; donc les seuls sous-modules de Ae_i sont (0) et les $N^k e_i$. Si A est artinien, soit k l'ordre de nilpotence de N . Soit M un A-module à gauche. On peut supposer que $N^{k-1}M \neq (0)$; donc il existe $x \in M$ tel que $N^{k-1}x \neq (0)$ et, par suite, il existe un idempotent primitif de la décomposition de A_s , soit e_i , pour lequel on a : $N^{k-1}e_i x \neq (0)$. Par suite, l'application $ae_i \longrightarrow ae_i x$ de Ae_i sur $Ae_i x$ est un isomorphisme. Donc $Ae_i x$ est un sous-module injectif de M ; puisque M est indécomposable, il est isomorphe à Ae_i .

Si A est un anneau involutif, on appelle <u>permutation structurale</u> de A , la permutation de l'ensemble des classes d'idempotents primitifs de A qui à la classe de l'idempotent primitif e de A fait correspondre la classe de l'idempotent primitif f de A tel que Ae/Ne est isomorphe à l'unique sous-module minimal de Af , où N désigne le radical de A .

2.4.5. – THEOREME. – <u>Soient</u> A <u>un anneau involutif restreint et</u> N <u>le radical de</u> A . <u>On suppose que les permutations structurales des différents anneaux involutifs</u> A/N^k <u>sont l'identité. Alors tout</u> A-<u>module injectif artinien indécomposable est de largeur</u> 1 .

<u>Démonstration</u>. Soit M un module à gauche artinien injectif indécomposable ; alors, M ne possède qu'un sous-module simple M_1 de M_1 est isomorphe à Ae/Ne, où e est un idempotent primitif de A . Soit k un entier >0 . Puisque les permutations structurales de A sont l'identité, il existe un isomorphisme de A-modules $\varphi : N^{k-1}e/N^k e \longrightarrow N^k e/N^{k+1}e$. Puisque l'anneau A/N^{k+1} est involutif, φ se prolonge en un monomorphisme de A-modules : $\varphi_{k,k+1} : Ae/N^k e \longrightarrow Ae/N^{k+1}e$. Posons pour $s \leqslant k$, $\varphi_{s,k} = \varphi_{k-1,k} \cdots \varphi_{s,s+1}$: on forme un système inductif de A-modules : $(Ae/N^k e , \varphi_{s,k})$. Soit $P = \varinjlim Ae/N^k e$. Alors, P est un module artinien de largeur 1 et il est isomorphe à un sous-module de M. Il suffit donc de prouver que P est injectif. Le module P peut être considéré comme la réunion de sous-modules P_k , $k = 1,2,\dots,$ où P_k est isomorphe à $Ae/N^k e$. Soient J un idéal à gauche de A et f un homomorphisme : $J \longrightarrow P$. Si f est surjectif, soit J_k l'image réciproque de P_k par f . Puisque A est noethérien à gauche, la chaîne des idéaux à gauche : $J_1 \subseteq \dots \subseteq J_k \subseteq \dots$ est finie. Donc il existe un entier n tel que $P = P_n$. On a $N^n = (0)$, et P est isomorphe à Ae . L'anneau A étant alors involutif, il existe un homomorphisme : $A_s \to P$ qui prolonge f . Si N n'est pas nilpotent, l'homomorphisme f n'est pas surjectif. Soit $f(J) = P_k$; on a $f(N^k J) = (0)$ et f induit un homomorphisme de A/N^k-modules : $J/N^k J \longrightarrow P_k$ qui, puisque A/N^k est involutif, se prolonge en un homomorphisme $\bar{f} : A/N^k J \to P_k$. Si θ désigne l'homomorphisme canonique $A \longrightarrow A/N^k J$, alors $g = \bar{f}\theta$ est un homomorphisme

de A-modules : $A \longrightarrow P$ qui prolonge f .

Soient A un anneau de valuation discrète de rang 1 complet et $m(A)$ l'idéal maximal de A ; si la caractéristique du corps résiduel de A est $p \neq 0$, soit G un groupe fini d'ordre premier à p . Pour tout entier $k > 0$, les anneaux $A[G]/m(A)^k[G]$ et $(A/m(A)^k)[G]$ sont isomorphes. Donc l'anneau $A[G]/m(A)^k[G]$ est involutif et sa permutation structurale est l'identité. Par suite, l'anneau $A[G]$ est involutif restreint et ses différentes permutations structurales sont l'identité.

Soient A un anneau, M un A-module à gauche et N un A-module à droite. Si f est une forme bilinéaire de $M \times N$ dans A , on pose :

$\mathrm{Ann}_f(L) = \{ y \in N \ ; \ f(L,y) = 0 \}$ $\qquad \mathrm{Ann}_f(R) = \{ x \in M \ ; \ f(x,R) = 0 \}$

pour tous les sous-modules L et R de M et N respectivement.

La forme bilinéaire f est <u>non dégénérée</u> si l'on a : $\mathrm{Ann}_f(M) = (0)$ et $\mathrm{Ann}_f(N) = (0)$.

2.4.6. - THEOREME. - <u>Soient</u> A <u>un anneau involutif</u>, M (resp. N) <u>un</u> A-<u>module à gauche</u> (resp. <u>à droite</u>) <u>de type fini et</u> f <u>une forme bilinéaire non dégénérée de</u> $M \times N$ <u>dans</u> A . <u>Alors, pour tous les sous-modules</u> L <u>de</u> M <u>et</u> R <u>de</u> N , <u>on a</u> : $\mathrm{Ann}_f(\mathrm{Ann}_f(L)) = L$ <u>et</u> $\mathrm{Ann}_f(\mathrm{Ann}_f(R)) = R$. (cf. [8] ; Chap. VIII : § 58 ; Th. 58-8; p. 397).

2.4.7. - <u>Lemme</u>. - <u>Soient</u> A <u>un anneau involutif</u>, B <u>un anneau muni d'une structure de</u> A-<u>bimodule</u>. <u>Désignons par</u> B_s (resp. B_d) <u>la structure de</u> A-<u>module à gauche</u> (resp. <u>à droite</u>) <u>de</u> B . <u>On suppose que les conditions suivantes sont réalisées</u> :

1º) <u>Les</u> A-<u>modules</u> B_s <u>et</u> B_d <u>sont de type fini</u> ;

2º) <u>Tout idéal à gauche</u> (resp. <u>à droite</u>) <u>de l'anneau</u> B <u>est un sous</u>-A-<u>module de</u> B_s (resp. B_d) ;

3º) <u>Il existe une forme</u> A-<u>linéaire</u> ω <u>du</u> A-<u>bimodule</u> B <u>dans</u> A <u>dont le noyau, ensemble des éléments</u> x <u>de</u> B <u>tels que</u> $\omega(x) = 0$, <u>ne contient aucun idéal, à droite ou à gauche, non nul de l'anneau</u> B ; i.e. :

(i) $\omega(x+y) = \omega(x) + \omega(y)$; $\omega(ax) = a\omega(x)$; $\omega(xa) = \omega(x)a$ <u>si</u> $x, y \in B$, $a \in A$;

(ii) <u>Si</u> $\omega(xB) = (0)$ <u>ou</u> $\omega(Bx) = (0)$, <u>pour</u> $x \in B$, <u>on a</u> : $x = 0$.

<u>Alors l'anneau</u> B <u>est involutif</u>.

<u>Démonstration</u>. Puisque l'anneau A est artinien, les A-modules B_s et B_d , étant de type fini sont artiniens ; donc, d'après 2º), l'anneau B est artinien. Soit f la forme bilinéaire de $B_s \times B_d$ dans A définie par $f(x,y) = \omega(xy)$ si x et $y \in B$. Si, pour $x \in B$, on a : $f(x,B_d) = (0)$ ou $f(B_s,x) = (0)$, alors, d'après 3º), $x = 0$. Donc f est non dégénérée. Soient L un idéal à gauche et

R un idéal à droite de B . On a $\mathrm{Ann}_f(L) = \{x \in B \ ; \ f(L,x) = 0\} = \{x \in B \ ; \ \omega(Lx) = (0)\}$; donc, d'après 3º), on a : $\mathrm{Ann}_f(L) = 0.^{\bullet}L$.. De la même façon, on a : $\mathrm{Ann}_f(R) = 0.^{\bullet}R$. Le théorème 2.4.6., appliqué au système formé de A , B_s , B_d , f , prouve que l'anneau B est involutif.

2.4.8. - THEOREME. - <u>Soient</u> B <u>un anneau,</u> A <u>un sous-anneau de</u> B <u>de la forme</u> $K[X]/(X^n)$, <u>où</u> K <u>est un corps commutatif,</u> N <u>le radical de</u> A . <u>On suppose qu'il existe un sous-anneau semi-simple</u> C <u>de</u> B <u>qui est l'algèbre sur</u> K <u>d'un groupe fini</u> G <u>d'ordre premier à la caractéristique de</u> K , <u>de telle sorte que</u> :

1º) <u>Le</u> A-<u>module à gauche</u> (resp. <u>à droite</u>) B <u>s'identifie à</u> $A \otimes_K C$ (resp. $C \otimes_K A$) ;

2º) <u>On a</u> : $NB = BN$;

3º) <u>Les éléments de</u> A <u>et</u> C <u>commutent modulo</u> $N \otimes_K C$;

4º) <u>On a</u> : $g^{-1}Ag = A$ <u>quel que soit</u> $g \in G$;

5º) <u>Si</u> g <u>et</u> $h \in G$ <u>et si</u> $a \in A$, <u>on a</u> $(a \otimes h)g = a \otimes hg$ <u>et</u> $g(a \otimes h) = (gag^{-1}) \otimes gh$.

<u>Alors, l'anneau</u> B <u>est artinien et involutif restreint.</u>

<u>Démonstration</u>. D'après 1º), B est un A-module à droite et à gauche de type fini ; donc B est artinien. D'après 2º), l'idéal NB est nilpotent ; il est donc contenu dans le radical de B . D'après 3º), les anneaux B/NB et $(A/N) \otimes_K C (\cong C)$ sont isomorphes ; donc NB est le radical de B . Puisque B/N^iB vérifie, pour tout entier $i > 0$ les mêmes conditions que B , il suffit de prouver que B est involutif et que son socle est $N^{n-1}B$. Soit g_1 l'élément unité de G et soit f l'application de B dans A qui à $x = \sum_{g_i \in G} a_i \otimes g_i$ fait correspondre a_1 .

Alors, f est une forme A-linéaire du A-bimodule B dans A . Si $f(xB) = 0$, alors $f(xg_i^{-1}) = 0$, quel que soit $g_i \in G$; donc, d'après 5º), on a : $x = 0$. Si $f(Bx) = 0$, alors $g_i^{-1}x = \sum_{g_j \in G} (g_i^{-1}a_jg_i) \otimes (g_i^{-1}g_j)$ et $g_i^{-1}a_ig_i = 0$ quel que soit $g_i \in G$. Donc $a_i = 0$ et $x = 0$.

D'après 2.4.7., B est involutif. On a évidemment $N^{n-1}B \subseteq 0^{\bullet}.(NB)$. Soit $x = \sum_{g_i \in G} a_i \otimes g_i$ $0^{\bullet}.(NB)$; alors $Nx = (0)$ et, quel que soit a_i , on a : $Na_i = (0)$; d'où $a_i \in N^{n-1}$ et $x \in N^{n-1}B$. Par suite, $N^{n-1}B$ est le socle de B .

2.4.9. - <u>Corollaire</u>. - <u>Soient</u> C <u>l'algèbre sur un corps</u> K <u>d'un groupe fini</u> G <u>dont l'ordre est premier à la caractéristique de</u> K . <u>Posons</u> $A_n = K[X]/(X^n)$ <u>et soit</u> B_n <u>un sur-anneau de</u> A_n <u>tel que les conditions de</u> 2.4.8. <u>soient vérifiées par</u> C , B_n <u>et</u> A_n . <u>Posons</u> $A = \varprojlim A_n$ <u>et soit</u> N <u>le radical de</u> A . <u>Alors</u>

l'anneau $B = \varprojlim B_n$ *est involutif restreint.*

Démonstration. L'anneau B s'identifie comme A-module à gauche à $\varprojlim(A_n \otimes_K C)$. On a, pour tout n, un homomorphisme surjectif $A \otimes_K C \to A_n \otimes_K C$ dont le noyau est $N^n \otimes_K C$ tel que le diagramme :

$$\begin{tikzcd} A \otimes_K C \arrow[r] \arrow[dr] & A_n \otimes_K C \arrow[d] \\ & A_m \otimes_K C \end{tikzcd}$$

où $m \leqslant n$, est commutatif. Donc $A \otimes_K C$ est isomorphe à $\varprojlim(A_n \otimes_K C)$, puisque $\bigcap_{n=1}^{\infty} (N^n \otimes_K C) = 0$. Donc B s'identifie, comme A-module à $A \otimes_K C$. On a : $NB = BN$, puisque $NB_k = B_k N$ pour tout k et que $\bigcap_{k=1}^{\infty} BN^k = (0)$. L'anneau B est complet pour la topologie NB-adique ; donc NB est contenu dans le radical de B. Les éléments de A et de C commutent modulo $N \otimes_K C$; donc l'anneau B/NB est semi-simple et NB est le radical de B. Pour tout entier $n > 0$, B/N^nB est isomorphe à B_n ; donc B est involutif restreint, d'après 2.4.8. .

Soient G un groupe, H un sous-groupe normal de G et U un sous-groupe de G. On dit que G est le *produit semi-direct* de H par U si $U \cap H = \{1\}$ et $G = H.U$.

2.4.10.- THEOREME. - *Soient* G *un groupe produit semi-direct d'un groupe cyclique* H *d'ordre* p^n *par un groupe fini* U *dont l'ordre est premier à* p *et* K *un corps de caractéristique* p. *Alors l'anneau* $K[G]$ *est involutif restreint.*

Démonstration. D'après 2.3.5., l'anneau $A = K[H]$ est isomorphe à $K[X]/(X^{p^n})$. Puisque H est un sous-groupe normal de G, on a : $u^{-1}Au = A$, quel que soit $u \in U$. Puisque G est produit semi-direct de H par U tout élément x de B se met d'une manière unique sous la forme : $x = b_1u_1 + \ldots + b_su_s$, où $b_i \in A$ et $u_k \in U$. Donc B est isomorphe au A-module à gauche $A \otimes_K C$. Soient a un générateur du groupe cyclique H, u un élément de U et k un nombre entier ; puisque H est un sous-groupe normal de G, il existe un entier s tel que $ua^k = a^s u$; d'où $ua^k = a^k u + (a^s - a^k)u$ et $a^s - a^k$ appartient au radical N de A, d'après 2.3.5. . Donc les éléments de A et C commutent modulo $N \otimes_K C$. La condition 5º) de 2.4.8. est évidemment vérifiée. Donc B est involutif restreint.

Il résulte de 2.4.9. et 2.3.7., le corollaire suivant :

2.4.11.- *Corollaire.* - *Soient* G *un groupe produit semi-direct d'un groupe* H *isomorphe au groupe additif des entiers* p-*adiques par un groupe fini* U *dont l'ordre est premier à* p, G_s *le groupe quotient de* G *par* H^{p^s} *et* K *un corps de ca-*

<u>ractéristique</u> p . <u>Alors, l'anneau</u> $B = \varprojlim K[G_s]$ <u>est involutif restreint.</u>

CHAPITRE III

Quasi-valuations

Sauf mention du contraire tous les groupes considérés dans ce chapitre sont supposés commutatifs.

§ 1.- Quasi-valuations de modules simples.

Nous désignerons par Γ un ensemble totalement ordonné, par une relation d'ordre notée $\leqslant$ et qui, s'il n'est pas réduit à un seul élément, ne possède ni plus grand ni plus petit élément. Il en est, en particulier, ainsi, lorsque Γ est muni d'une structure de groupe, commutatif ou non, compatible avec sa structure d'ensemble ordonné.

On adjoint à Γ un élément, noté 0, assujetti à la condition suivante :
$0 < \alpha$ quel que soit $\alpha \in \Gamma$.

On appelle section commençante généralisée d'un ensemble ordonné E, un sous-ensemble Δ de E qui satisfait à la condition suivante :
$\alpha \in \Delta \, ; \, \rho \in E \, ; \, \rho \leqslant \alpha \Longrightarrow \rho \in \Delta$.

Soient M un module à gauche simple et fidèle sur un anneau B et F le corps commutant de B sur M. On désignera par F^* le groupe multiplicatif de F.

3.1.1. - Définition. - Appelons quasi-valuation du système constitué par M, F et B, une application v de M sur $\Gamma \cup \{0\}$ qui vérifie les axiomes suivants :

I_1.- On a : $v(x + y) \leqslant \mathrm{Max}(v(x), v(y))$ quels que soient x et $y \in M$;

I_2.- On a : $v(x) = 0$, pour un élément x de M, si et seulement si $x = 0$;

II_1.- Si $0 \neq v(x) \leqslant v(y)$, où x et $y \in M$, il existe $f \in F^*$ pour lequel on a $v(fy) \leqslant v(x)$;

II_2.- Si, pour $x \in M$ et $f \in F$, on a : $v(fx) < v(x)$, alors : $v(fy) \leqslant v(y)$ quel que soit $y \in M$;

III.- Si $v(x) \leqslant v(y)$, où x et $y \in M$, il existe $\varphi \in B$ tel que $x = \varphi y$ et tel que $v(\varphi z) \leqslant v(z)$ quel que soit $z \in M$.

La quasi-valuation v sera dite <u>triviale</u> si Γ ne possède qu'un élément.

De l'axiome III, il résulte la propriété suivante :

3.1.2. - <u>Si</u> $v(x) \leqslant v(y)$, <u>pour</u> x <u>et</u> $y \in M$, <u>alors</u> $v(fx) \leqslant v(fy)$ <u>quel que soit</u> $f \in F$.

3.1.3. - <u>Si</u> $f \in F^*$ <u>et si</u> $x \in M$, <u>on a</u> $v(fx) < v(x)$ (resp. $v(fx) = v(x)$) <u>si et seulement si</u> $v(x) < v(f^{-1}x)$ (resp. $v(x) = v(f^{-1}x)$) ; en effet, si $v(fx) \leqslant v(x)$, on a, d'après 3.1.2., $v(x) \leqslant v(f^{-1}x)$. On a : $v(fx) = v(x)$ si et seulement si $v(fx) \leqslant v(x)$ et $v(x) \leqslant v((f^{-1})^{-1}x)$; c'est-à-dire si et seulement si $v(x) =$ $= v(f^{-1}x)$.

3.1.4. - <u>Si, pour un élément</u> $x \in M$ <u>et un élément</u> $f \in F^*$, <u>on a</u> $v(x) < v(fx)$, <u>alors</u> $v(y) \leqslant v(fy)$ <u>quel que soit</u> $y \in M$; en effet, sinon, il existerait un $y \in M$ pour lequel : $v(y) > v(fy)$; d'où, d'après II_2, $v(fx) \geqslant v(x)$, ce qui contredit l'hypothèse faite sur x.

3.1.5. - <u>On a</u> : $v(-x) = v(x)$, <u>quel que soit</u> $x \in M$; soit 1 l'élément unité de F; si, pour $x \in M$, on a : $v(-x) = v((-1)x) \leqslant v(x)$, il résulte de 3.1.3., que $v(x) \leqslant v((-1)x)$; d'où $v(x) = v(-x)$.

3.1.6. - THEOREME. - <u>L'ensemble</u> $V = \{f \; ; \; f \in F \; ; \; v(fx) \leqslant v(x)$ <u>quel que soit</u> $x \in M\}$ <u>est un anneau de valuation du corps</u> F.

<u>Démonstration</u>. On prouve facilement que V est un sous-anneau de F. Il suffit, d'après 2.2.5., de vérifier que V satisfait aux conditions suivantes :

(i) Quel que soit $f \in F$, on a : f ou $f^{-1} \in V$;
(ii) Quel que soit $f \in V$, $f \neq 0$, on a : $f^{-1}Vf = V$.

Soit $f \in F$, $f \notin V$. Il existe donc un élément $x \in M$ pour lequel on a l'inégalité stricte $v(x) < v(fx)$. Il en résulte, d'après 3.1.4., que $v(y) \leqslant v(fy)$, pour tout $y \in M$; d'où, d'après 3.1.3., $v(f^{-1}y) \leqslant v(y)$, pour tout $y \in M$. Par conséquent $f^{-1} \in V$ et V vérifie (i). Soient $g \in V$ et $f \in F^*$; on a, par définition de V, $v(gfx) \leqslant v(fx)$, quel que soit $x \in M$. D'où, d'après 3.1.2., $v(f^{-1}gfx) \leqslant v(x)$, pour tout $x \in M$ et $f^{-1}gf \in V$. Donc, pour tout $f \in F^*$ on a : $f^{-1}Vf \subseteq V$. D'où $f^{-1}Vf = V$, si $f \in V-(0)$.

Nous désignerons par Γ_F le groupe de la valuation du corps F qui correspond à l'anneau V et nous désignerons par $\mathcal{V}$ la valuation correspondante de F (ceci, évidemment, à une équivalence près).

3.1.7. - <u>Lemme</u>. - <u>Soient</u> f <u>et</u> $g \in F$; <u>on a</u> : $v(fx) = v(gx)$ <u>quel que soit</u> $x \in M$, <u>si et seulement si</u> $\mathcal{V}(f) = \mathcal{V}(g)$.

Démonstration. Il n'y a rien à démontrer si f ou si g est nul. Supposons donc que $f \neq 0$ et $g \neq 0$. Si $v(fx) = v(gx)$, quel que soit $x \in M$, on a, d'après 3.1.3. et 3.1.6., $f^{-1}g$ et $g^{-1}f \in V$; donc $f^{-1}g$ est une unité de V et $\Upsilon(g) = \Upsilon(f)$. Inversement, si $\Upsilon(f) = \Upsilon(g)$, i.e. si $g^{-1}f$ et $f^{-1}g \in V$, on a, quel que soit $x \in M$, $v(g^{-1}fx) \leqslant v(x)$ et $v(f^{-1}gx) \leqslant v(x)$; d'où $v(fx) = v(gx)$ quel que soit $x \in M$.

3.1.8. - Lemme. - Soit ρ un élément du groupe Γ_F et soit $f \in F^*$. L'application $\Theta_\rho : v(x) \longrightarrow v(fx)$ est un isomorphisme de l'ensemble ordonné Γ, si $\rho = \Upsilon(f)$.

Démonstration. Nous notons Θ_ρ cette application, car, d'après 3.1.7., elle ne dépend que de ρ. L'application Θ_ρ est surjective ; en effet, si $v(y) \in \Gamma$, où $y \in M$, on a : $y = f(f^{-1}y)$; d'où $v(y) = \Theta_\rho\, v(f^{-1}y)$ et $v(f^{-1}y) \in \Gamma$. Elle est injective ; si pour deux éléments $v(x)$ et $v(y)$ de Γ, on a : $\Theta_\rho\, v(x) = \Theta_\rho\, v(y)$, alors $v(fx) = v(fy)$; d'où $v(x) = v(y)$. Enfin, si $v(x) \leqslant v(y)$, on a, d'après 3.1.2., $v(fx) \leqslant v(fy)$ et $\Theta_\rho v(x) \leqslant \Theta_\rho v(y)$.

Si E est un ensemble totalement ordonné, on désignera par Aut. E, le groupe ordonné, par la relation d'ordre induite par celle de E, des automorphismes de l'ensemble ordonné E.

3.1.9. - THEOREME. - L'application qui à l'élément ρ du groupe Γ_F fait correspondre l'automorphisme Θ_ρ de Γ est un isomorphisme du groupe Γ_F dans le groupe Aut.Γ.

Démonstration. Soient ρ et $\lambda \in \Gamma_F$; il existe donc f et $g \in F^*$ tels que $\rho = \Upsilon(f)$, et $\lambda = \Upsilon(g)$. On a : $\rho \leqslant \lambda$, (resp. $\rho = \lambda$), si et seulement si $g^{-1}f \in V$ (resp. $g^{-1}f$ et $f^{-1}g \in V$) ; i.e. si et seulement si on a, quel que soit $x \in M$, $\Theta_\rho v(x) \leqslant \Theta_\rho v(x)$ (resp. $\Theta_\rho\, v(x) = \Theta_\lambda\, v(x)$) ; i.e. si et seulement si on a : $\Theta_\rho \leqslant \Theta_\lambda$ (resp. $\Theta_\rho = \Theta_\lambda$). Par conséquent, l'application $\rho \longrightarrow \Theta_\rho$ est une application injective d'ensembles ordonnés. Soient ρ et $\mu \in \Gamma_F$; il existe f et $h \in F^*$ tel que $\rho = \Upsilon(f)$ et $\mu = \Upsilon(h)$. Alors $\rho\mu = \Upsilon(fh)$. Soit $x \in M$; on a : $\Theta_{\rho\mu}(v(x)) = v(fhx) = \Theta_\rho(v(hx)) = \Theta_\rho\, \Theta_\mu(v(x))$. Par conséquent $\Theta_{\rho\mu} = \Theta_\rho\, \Theta_\mu$.

Les axiomes II_1 et II_2 entraînent, respectivement, les propriétés II_1' et II_2' suivantes :

(II_1'). - Si $\lambda \leqslant \mu$, où λ et $\mu \in \Gamma$, il existe $\rho \in \Gamma_F$ tel que $\Theta_\rho \mu \leqslant \lambda$;

(II_2'). - Si $\Theta_\rho\, \lambda < \lambda$, où $\lambda \in \Gamma$ et $\rho \in \Gamma_F$, on a : $\Theta_\rho \mu \leqslant \mu$ quel que soit $\mu \in \Gamma$.

De la propriété (II_1'), il résulte la proposition suivante :

3.1.10.- Proposition. - La valuation $\mathscr{V}$ du corps F est triviale si et seulement si la quasi-valuation v du système (M,F,B) est triviale.

3.1.11.- L'ensemble A des éléments $\varphi \in B$ pour lesquels on a : $v(\varphi x) \leqslant v(x)$ quel que soit $x \in M$, est un sous-anneau de B, qui sera appelé l'anneau de la quasi-valuation v ; d'après la définition de l'ensemble A, l'élément unité de B appartient à A et si φ et $\psi \in A$, on a : $\varphi\psi \in A$. On a aussi : $\varphi - \psi \in A$, d'après l'axiome I_1 et 3.1.5.

3.1.12.- Le treillis des sous-A-modules de M est totalement ordonné et est isomorphe à l'ensemble totalement ordonné des sections commençantes généralisées de $\Gamma \cup \{0\}$; en effet, à un sous-A-module N de M, on fait correspondre le sous-ensemble de $\Gamma \cup \{0\}$ suivant : $\Delta(N) = \{v(x) \ ; \ x \in N\}$; puisque l'application $v : M \longrightarrow \Gamma \cup \{0\}$ est surjective, il résulte de l'axiome III, que $\Delta(N)$ est une section commençante généralisée de $\Gamma \cup \{0\}$. Si N_1 et N_2 sont deux sous-A-modules de M et si $N_1 \subseteq N_2$, on a, de façon évidente, $\Delta(N_1) \leqslant \Delta(N_2)$. Soit Δ une section commençante généralisée de $\Gamma \cup \{0\}$; l'ensemble $N(\Delta) = \{x \in M \ ; \ v(x) \in \Delta\}$ est un sous-A-module de M ; en effet, $N(\Delta)$ est un sous-groupe additif de M, d'après 3.1.7.. Enfin, l'application $\Delta \longrightarrow N(\Delta)$ est croissante et les applications $N \longrightarrow \Delta(N)$ et $\Delta \longrightarrow N(\Delta)$ sont inverses l'une de l'autre.

3.1.13.- Si $x \in M$, le sous-A-module monogène de M, engendré par x, est l'ensemble des éléments $y \in M$ pour lesquels on a : $v(y) \leqslant v(x)$; en effet, on a : $v(y) \leqslant v(x)$ si et seulement si $y = \varphi x$, où $\varphi \in A$; i.e. si et seulement si $y \in Ax$.

3.1.14.- Si G est un sous-A-module non nul de M, il résulte de l'axiome II_1 et de 3.1.13., que, pour tout $x \in M$, il existe $f \in F^*$ tel que $fx \in G$.

Il résulte de 3.1.14., les propriétés suivantes :

3.1.15.- Si G est un sous-A-module non nul de M et aussi un sous-F-espace vectoriel de M, on a : $G = M$.

3.1.16.- L'annulateur dans A, d'un sous-A-module non nul de M est (0). En particulier, l'anneau A est premier.

3.1.17.- Tout sous-A-module G de M est, en particulier, un V-module ; et si G n'est pas nul, le V-module M est une extension essentielle du V-module G. Soient $f \in V$ et $x \in G$; on a, par définition de V, $v(fx) \leqslant v(x)$; d'où $fx \in G$, d'après 3.1.11.. Soient N un sous-V-module de M tel que $N \cap G = (0)$ et $x \in N$. Il existe, d'après 3.1.14., $f \in F^*$ tel que $fx \in G$. D'où, puisque f ou $f^{-1} \in V$, on a : $x = 0$ et $N = (0)$.

3.1.18.- Proposition. - Si l'anneau B est l'anneau des endomorphismes du F-espace vectoriel M , B est aussi l'anneau des endomorphismes du V-module M .

Démonstration. L'anneau B est contenu dans l'anneau C des endomorphismes du V-module M . Si $\varphi \in C$, $f \in F$, $f \notin V$ et $x \in M$, alors $f^{-1} \in V$; $y = fx$; on a : $\varphi(f^{-1}y) = f^{-1}\varphi(y)$. D'où $f\varphi(x) = \varphi(fx)$.

Nous dirons qu'un sous-A-module de M est propre, s'il est différent de M et de (0).

3.1.19.- THEOREME. - Soit G un sous-A-module propre de M . Si B est l'anneau des endomorphismes du F-espace vectoriel M , l'anneau A_1 des V-endomorphismes de G est isomorphe au sous-anneau de B , formé des éléments de B qui conservent G . Si la quasi-valuation v n'est pas triviale, l'ensemble Γ_1 des sous-A_1-modules monogènes non nuls de M est totalement ordonné et ne possède ni plus petit ni plus grand élément. L'application v_1 de M sur $\Gamma_1 \cup \{0\}$, définie par $v(x) = A x$ est une quasi-valuation du système constitué par M , F et B .

Démonstration. Soient $\varphi \in A_1$ et $x \in M$. D'après 3.1.14., il existe $f \in F^*$ tel que $fx \in G$. L'élément $f^{-1}\varphi(fx)$ de M ne dépend pas de f ; i.e. si, pour un autre élément $g \in F^*$, on a $gx \in G$, alors, $f^{-1}\varphi(fx) = g^{-1}\varphi(gx)$; en effet, puisque V est un anneau de valuation de F , on a, par exemple : $fg^{-1} = h \in V$. D'où $f^{-1}\varphi(fx) = g^{-1}h^{-1}\varphi(hgx) = g^{-1}\varphi(gx)$. Posons $\overline{\varphi}(x) = f^{-1}\varphi(fx)$. L'application $\overline{\varphi}$ est un endomorphisme du groupe M . En effet, soient x et $y \in M$; il existe f et $g \in F^*$ tels que fx et $gy \in G$ et l'on a : $\overline{\varphi}(x) = f^{-1}\varphi(fx)$, $\overline{\varphi}(y) = g^{-1}\varphi(gy)$ Si $g = hf$, où $h \in V$, alors hfx et $hfy \in G$; d'où $g(x+y) \in G$ et $\overline{\varphi}(x+y) =$ $= g^{-1}\varphi(gx) + g^{-1}\varphi(gy) = \overline{\varphi}(x) + \overline{\varphi}(y)$. L'application $\overline{\varphi}$ est un F-endomorphisme de M . Il suffit, d'après 3.1.18., de vérifier que $\overline{\varphi}$ est un V-endomorphisme de M . Soient $g \in V$ et $x \in M$. Si $x \in G$, on a : $\overline{\varphi}(gx) = \varphi(gx) = g\,\varphi(x) = g\,\overline{\varphi}(x)$ Si $x \notin G$, il existe $h \in V$, $h \neq 0$, tel que $hx \in G$. D'où $\overline{\varphi}(x) = h^{-1}\varphi(hx)$ et $g\,\overline{\varphi}(x) = gh^{-1}\varphi(hx)$. Si $gh^{-1} \in V$, on a $gh^{-1}\varphi(hx) = \varphi(gh^{-1}hx) = \overline{\varphi}(gx)$; sinon, hg^{-1} appartient à V et $gh^{-1}\varphi(hx) = gh^{-1}\varphi(hg^{-1}gx) = \overline{\varphi}(gx)$. Le prolongement $\overline{\varphi}$ de φ à M , ainsi défini, est unique et l'application $\varphi \longrightarrow \overline{\varphi}$ est un isomorphisme de A_1 dans B . Si l'on identifie A_1 au sous-anneau de B auquel il est isomorphe, A_1 est l'ensemble des éléments de B qui respectent G ; par suite on a : $A \subsetneq A_1$. Donc, l'ensemble Γ_1 des sous-A_1-modules monogènes non nuls de M est totalement ordonné. Si Γ_1 possèdait un plus grand élément, M serait un A_1-module monogène ; on aurait $M = A_1 x$, $x \in M$ et, pour un élément $f \in F^*$, fx appartiendrait à G ; d'où $M = G$, ce qui contredit l'hypothèse faite sur G .

Si Γ_1 possédait un plus petit élément, il existerait un sous-A_1-module minimal de M, soit A_1y, $y \in M$, $y \neq 0$. Le A_1-module A_1y serait un F-espace vectoriel. D'après 3.1.15., on aurait $M = A_1y$, ce qui est impossible. Les axiomes I et III sont visiblement vérifiés par v_1. Soient x et $y \in M$, $x \neq 0$; si l'on a : $v_1(x) < v_1(y)$, i.e. $A_1x \subsetneq A_1y$, alors, puisque $A \subseteq A_1$, on a $v(x) < v(y)$. Donc il existe $f \in F^*$ tel que $v(fy) \leqslant v(x)$. D'où $v_1(fy) \leq v_1(x)$ et l'axiome II_2 est vérifié. Si, pour $f \in F$ et $x \in M$, on a : $v_1(fx) < v_1(x)$, alors, si $f \in V$, on a : $v(fy) \leqslant v(y)$, quel que soit $y \in M$; par suite $v_1(fy) \leqslant v_1(y)$, quel que soit $y \in M$. Nous allons prouver que f appartient nécessairement à V, ce qui achèvera la démonstration. Si l'on avait $f \notin V$, alors $f^{-1} \in V$; d'où $f^{-1}x \in$ $\in Ax \subseteq A_1x$. Par suite, A_1x serait contenu dans A_1fx, i.e. $v_1(x) \leq v_1(fx)$, ce qui est impossible.

§ 2.- <u>Anneaux complètement premiers</u>.

3.2.1. - <u>Définition</u>. - Soient K un corps gauche et F le centre de K ; nous appellerons <u>quasi-valuation de</u> K une quasi-valuation du système constitué par K, F et le K-module K_s.

3.2.2. - THEOREME. - <u>Soient</u> K <u>un corps et</u> A <u>un sous-anneau de</u> K. <u>Pour que</u> A <u>soit l'anneau d'une quasi-valuation de</u> K, <u>il faut et il suffit que la largeur gauche de</u> A <u>soit égale à</u> 1 <u>et que</u> $K = A \otimes_V F$, <u>où</u> V <u>est le centre de</u> A <u>et</u> F <u>est le corps des quotients de</u> V.

<u>Démonstration</u>. La condition est nécessaire. Si A est l'anneau d'une quasi-valuation de K, le treillis des sous-A-modules à gauche de K est totalement ordonné d'après 3.1.12.. D'après 2.2.2., K est le corps des quotients (à gauche et à droite) de A et les largeurs gauche et droite de A sont égales à 1. D'après 3.1.6., le centre V de A est l'anneau d'une valuation du corps F. Soit $C = V^{*-1}A$, où $V^* = V - (0)$. Alors, C est un sur-anneau de A contenu dans K. Si $k \in K$ et $k \notin A$, il existe, d'après 3.1.14., $f \in F$, $f \neq 0$, tel que $fk \in A$. Puisque $k \notin A$, on a : $k^{-1} \in A$; donc $f \in V^*$. Par suite, $k \in C$ et $K = C$ $= V^{*-1}A$.

La condition est suffisante. Si $K = A \otimes_V F$, où V est le centre de A et F le corps des quotients de V, l'anneau A est régulier à droite et K est le corps des quotients de A, d'après 2.2.10.. Il résulte alors de 2.2.3. que les largeurs droite et gauche de A sont égales à 1 et que le treillis des sous-A-modules à gauche de K est totalement ordonné. Soit Γ l'ensemble des sous-A-modules à gauche monogènes non nuls de K. L'ensemble Γ ne possède ni plus petit ni plus grand élément, à moins que l'anneau A ne coïncide avec K. Soit v

l'application de K sur $\Gamma \cup \{0\}$ définie par $v(x) = Ax$. Les axiomes I et III de 3.1.1. sont évidemment vérifiés, et l'on a : $A = \{a \in K \; ; \; v(ax) \leqslant v(x)$ quel que soit $x \in K\}$. Si a et $b \in K$ et si $0 \neq v(a) \leqslant v(b)$, alors $a = xb$, $x \in A$, $x \neq 0$. Donc, il existe un élément s du centre de A, $s \neq 0$, tel que $x^{-1} = s^{-1}y$, où $y \in A$. Par suite, $ab = ya$ et $v(sb) \leqslant v(a)$. Le centre de A, étant contenu dans le centre F de K, on a : $s \in F$; l'axiome II_1 est donc vérifié. Soit $a \in K$; si, pour $f \in F$, on a : $v(fa) < v(a)$, alors $f \in A$; sinon, $f^{-1} \in A$ et $Aa \subseteq Afa$, ce qui est impossible. Puisque $f \in A$, on a : $v(fx) \leqslant v(x)$ quel que soit $x \in K$ et l'axiome II_2 est vérifié.

D'après 2.2.11., si un corps K est algébrique sur son centre, en particulier si K est de rang fini sur son centre, et si K est valué, la valuation de K est aussi une quasi-valuation.

§ 3.- C-groupes.

Les anneaux considérés dans ce paragraphe ne sont pas nécessairement unitaires.

3.3.1. - Définition. - Nous dirons qu'un groupe G vérifie la condition (C) ou que G est un C-groupe, si le treillis des sous-groupes complètement invariants de G est totalement ordonné ; i.e. si G est un module de largeur 1 sur l'anneau de ses endomorphismes.

Puisque tout sous-groupe complètement invariant du groupe additif d'un anneau est un idéal de cet anneau, le groupe additif d'un anneau de largeur 1 est un C-groupe ; nous dirons qu'un anneau, non unitaire, est de largeur 1 si le treillis de ses idéaux est totalement ordonné.

Il résulte de la décomposition d'un groupe de torsion en somme directe de sous-groupes primaires et du fait que la composante p-primaire (p premier) d'un groupe de torsion est un sous-groupe complètement invariant, le lemme suivant :

3.3.2. - Lemme. - S'il n'est pas nul, le sous-groupe de torsion maximal d'un C-groupe est un groupe primaire.

3.3.3. - Lemme. - Il existe, au plus, un nombre premier par lequel un C-groupe donné n'est pas divisible.

Démonstration. Soient p et q deux nombres premiers distincts ; il existe deux entiers u et v, tels que $1 = up + vq$; d'où $G = pG + qG$. Les sous-groupes pG et qG étant complètement invariants, on a, soit $G = pG$ soit $G = qG$.

Si T est un p-groupe (p premier) et si k est un nombre entier positif, on désigne par $T[p^k]$ le sous-groupe de T constitué par les éléments d'ordre p^n, où n k. Le sous-groupe $T[p]$ est appelé le socle de T. Un p-groupe T est dit <u>borné</u> s'il existe un entier $n > 0$, pour lequel on a : $T[p^n] = T$, i.e. $p^n T = (0)$.

Nous désignerons, respectivement, par G_t et δG , le sous-groupe de torsion maximal et le sous-groupe divisible maximal d'un groupe G .

Un groupe G est dit <u>réduit</u>, si $\delta G = (0)$.

3.3.4. - <u>Lemme</u>. - <u>S'il n'est pas nul, le sous-groupe divisible maximal d'un</u> C-<u>groupe</u> G <u>contient le sous-groupe de torsion maximal de</u> G .

<u>Démonstration</u>. Les sous-groupes δG et G_t , étant complètement invariants dans G , sont comparables. Si $\delta G \subseteq G_t$, δG est un sous-groupe divisible de G_t et, par suite, c'est un facteur direct de G_t (Voir, exemple, [1]) ; on a : $G_t = \delta G \oplus H$. Mais, d'après 3.3.2., G_t est un p-groupe ; comme p divise δG , le socle de G_t , qui est un sous-groupe complètement invariant de G , est contenu dans δG . Par suite, le socle de H est contenu dans δG . D'où $H = (0)$ et $G_t = \delta G$.

3.3.5. - <u>Lemme</u>. - <u>Soit</u> H <u>un sous-groupe complètement invariant d'un groupe</u> G . <u>Si</u> G <u>admet les décompositions en sommes directes</u> : $G = G_1 \oplus G_1'$ <u>et</u> $G = G_2 \oplus G_2'$ <u>et si</u> φ <u>est un isomorphisme de</u> G_1 <u>sur</u> G_2 , <u>la restriction de</u> φ <u>à</u> $H_1 = G_1 \cap H$ <u>est un isomorphisme de</u> H_1 <u>sur</u> $H_2 = G_2 \cap H$.

<u>Démonstration</u>. Soient i_2 et p_1 , respectivement, l'injection de G_2 dans G et la projection de G sur G_1 . Puisque H est complètement invariant dans G , l'endomorphisme $i_2 \varphi p_1$ de G , applique H dans H_2 . La restriction de $i_2 \varphi p_1$ à H_1 coïncide avec la restriction de φ à H_1 ; puisque φ est injectif la restriction de φ à H_1 est un monomorphisme de H_1 dans H_2 . On prouve de la même façon que la restriction de φ^{-1} à H_2 est un monomorphisme de H_2 dans H_1 et le lemme en résulte.

On déduit de 3.3.5., le corollaire suivant :

3.3.6. - <u>Corollaire</u>. - <u>Un sous-groupe complètement invariant</u> H <u>d'un groupe</u> G , <u>qui est somme directe d'une famille de sous-groupes</u> G_i , $i \in I$, <u>deux à deux isomorphes, est une somme directe de sous-groupes</u> H_i , $i \in I$, <u>deux à deux isomorphes; pour tout</u> $i \in I$, H_i <u>est un sous-groupe complètement invariant de</u> G_i ; <u>pour</u> i <u>et</u> $j \in I$, <u>un isomorphisme de</u> H_i <u>sur</u> H_j <u>est donné par la restriction à</u> H_i <u>d'un isomorphisme de</u> G_i <u>sur</u> G_j .

3.3.7. - <u>Lemme</u>. - <u>Soit</u> G <u>un groupe de la forme</u> : $G = H \oplus M$, <u>où</u> M <u>est un groupe sans torsion et</u> H <u>un groupe divisible non nul. Le seul sous-groupe complète-</u>

ment invariant de G *contenu dans* M *est* (0).

Démonstration. Soit L un sous-groupe complètement invariant de G contenu dans M. Si $L \neq (0)$, soient $x \in L$, $x \neq 0$ et (x) le groupe cyclique engendré par x. Il existe un homomorphisme non nul φ de (x) dans H. Puisque H est divisible, φ se prolonge en un homomorphisme ψ de G dans H. D'où $\psi(L) \subseteq L \cap H = (0)$ et $\varphi(x) = 0$, ce qui est impossible.

Nous désignerons par Q le corps des nombres rationnels, par $C(p^{\infty})$ le groupe quasi-cyclique relatif au nombre premier p, i.e. le groupe U_p/Z, U_p étant le sous-groupe de Q formé des fractions s/p^k, où k est un nombre entier 0.

3.3.8. - *Lemme*. - *Les sous-groupes complètement invariants d'un groupe* G *de la forme suivante :* $G = T \oplus M$, *où* M *est un groupe sans torsion et* T *est un* p-*groupe divisible* (p *premier*) *sont les sous-groupes* $T[p^k]$, k *entier* $\geqslant 0$, $T \oplus H$, *où* H *est un sous-groupe complètement invariant du groupe* M.

Démonstration. Soit K un sous-groupe complètement invariant de G ; il admet la décomposition en somme directe : $K = (K \cap T) \oplus (K \cap M)$; $K \cap T$ et $K \cap M$ sont, respectivement, des sous-groupes complètement invariants de T et de M. Puisque un p-groupe divisible est somme directe d'une famille de groupes quasi-cycliques et que les sous-groupes complètement invariants de $U = C(p^{\infty})$ sont U et les $U[p^k]$, k entier $\geqslant 0$, il résulte de 3.3.6., que les sous-groupes complètement invariants de T sont T et les $T[p^k]$, k entier $\geqslant 0$. Par suite, si $K \cap T \neq T$, on a : $K \cap T = T[p^k]$, k entier $\geqslant 0$. Mais, si $K \cap T = T[p^k]$, alors d'après 3.3.7., $K \cap M = (0)$; sinon, $p^k(K \cap M)$ serait un sous-groupe complètement invariant de G contenu dans M.

3.3.9. - *Lemme*. - *Soit* G *un groupe sans torsion*. *Tous les sous-groupes complètement invariants non nuls de* G *contiennent* $\mathcal{S}G$.

Démonstration. Supposons que $\mathcal{S}G \neq (0)$; le groupe G admet une décomposition en somme directe de la forme $G = \mathcal{S}G \oplus M$, où, s'il n'est pas nul, M est un groupe réduit sans torsion. Si H est un sous-groupe complètement invariant de G, on a : $H = (H \cap \mathcal{S}G) \oplus (H \cap M)$, où $H \cap \mathcal{S}G$ et $H \cap M$ sont, respectivement, des sous-groupes complètement invariants de $\mathcal{S}G$ et de M. Puisque $\mathcal{S}G$ est un groupe divisible sans torsion, i.e. une somme directe de groupes isomorphes à Q, il résulte de 3.3.6. que les seuls sous-groupes complètement invariants de $\mathcal{S}G$ sont (0) et $\mathcal{S}G$. Par suite, si $\mathcal{S}G \nsubseteq H$, on a : $H \cap \mathcal{S}G = (0)$; d'où d'après 3.3.7., $H = (0)$.

Puisque les sous-groupes complètement invariants d'un groupe divisible sans torsion H sont (0) et H, il résulte de la forme générale des groupes divisibles (cf. [11] ; Chap. III ; § 19) et de 3.3.8., le théorème suivant :

3.3.10.- THEOREME. - *Soit* G *un groupe divisible. Le treillis des sous-groupes complètement invariants de* G *est totalement ordonné si et seulement si* G *est de la forme suivante* : $G = \bigoplus_{\mathfrak{m}} Q \oplus \bigoplus_{\mathfrak{n}} C(p^{\infty})$, *où* $\mathfrak{m}$ *et* $\mathfrak{n}$ *sont des nombres cardinaux.*

3.3.11.- *Corollaire.* - *Si le groupe additif* A_+ *d'un anneau* A *de largeur* 1 *est divisible, il est de l'une des formes suivantes* : $A_+ = C(p^{\infty}) \oplus \bigoplus_{\mathfrak{m}} Q$ *ou* $A_+ = \bigoplus_{\mathfrak{m}} Q$, *où* $\mathfrak{m}$ *est un nombre cardinal. Dans le premier cas, le groupe* $C(p^{\infty})$ *est contenu dans l'annulateur de l'anneau* A . *Si* A *est unitaire,* A_+ *est sans torsion.*

Démonstration. Le corollaire résulte de 3.3.10 et du fait que chacun des groupes quasi-cycliques qui apparaissent dans la décomposition de A_+ est contenu dans l'annulateur de A (cf. [11] ; Chap. XII ; lemme 72.3).

3.3.12.- *Définition.* - Soit p un nombre premier. Un groupe G est dit *p-réduit*, s'il vérifie les conditions suivantes :

1º) G est un groupe sans torsion ;

2º) G est divisible par tous les nombres premiers différents de p ;

3º) G ne possède pas de sous-groupe, autre que (0), divisible par p .

Compte tenu de la condition 1º), la condition 3º) de 3.3.12. est équivalente à la condition suivante :

3º)' G est réduit.

D'après 3.3.3. *un* C-*groupe réduit sans torsion est un groupe* p-*réduit*.

3.3.13.- *Lemme.* - *Soit* G *un groupe de la forme suivante* : $G = T \oplus B \oplus M$, *où* T *est un* p-*groupe divisible* (p premier) B *un groupe divisible sans torsion et* M *un groupe réduit sans torsion. Les sous-groupes complètement invariants de* G *sont* $T[p^k]$, k *entier* $\geqslant 0$, T *et* $T \oplus B \oplus H$, *où* H *est un sous-groupe complètement invariant de* M .

Démonstration. Soit K un sous-groupe complètement invariant de G ; on a : $K = (K \cap T) \oplus K \cap (B \oplus M)$, où $K \cap T$ et $K \cap (B \oplus M)$ sont des sous-groupes complètement invariants de T et de $B \oplus M$, respectivement. Il résulte de 3.3.8., que $K = T[p^k]$, k entier positif ou nul, ou bien $K = T \oplus (K \cap (B \oplus M))$, où $K \cap (B \oplus M)$ est un sous-groupe complètement invariant de $B \oplus M$. D'après 3.3.9., $K \cap (B \oplus M)$, s'il n'est pas nul, contient B ; donc $K = T \oplus B \oplus (K \cap M)$, où $K \cap M$ est un sous-groupe complètement invariant de M .

On a donc démontré le théorème suivant :

3.3.14.- THEOREME. - Un groupe G, non réduit, vérifie la condition (C) si et seulement s'il est de la forme suivante : $G = T \oplus B \oplus M$, où T est un q-groupe divisible, B un groupe divisible sans torsion et M un C-groupe p-réduit ; p et q étant des nombres premiers.

Nous avons, en 3.3.9., démontré la première partie du théorème suivant, que nous nous proposons de démontrer tout au long de ce paragraphe :

3.3.15.- THEOREME. - Si un groupe G vérifie la condition (C), alors :

(i) Si G n'est pas réduit, on a : (1) $G = T \oplus B \oplus M$, où T est un q-groupe divisible (q premier), B un groupe divisible sans torsion et M un C-groupe p-réduit (p premier) ;

(ii) Si G est réduit et sans torsion, c'est un C-groupe p-réduit (2) ;

(iii) Si G est réduit et possède des éléments non nuls de torsion, on a :
(3) $G = \bigoplus_{\mathfrak{m}} C(p^k) \oplus \bigoplus_{\mathfrak{n}} C(p^{k-1})$, où $\mathfrak{m}$ et $\mathfrak{n}$ sont des nombres cardinaux, k est un entier supérieur ou égal à 1, p un nombre premier et $C(p^k)$ désigne le groupe cyclique d'ordre p^k.

Inversement, si G est de l'une des formes (1), (2) ou (3) précédente, alors il vérifie la condition (C).

On peut caractériser les C-groupes p-réduits, à l'aide des quasi-valuations ; pour cela rappelons que si U est un groupe sans torsion et $\overline{U}$ l'enveloppe injective du Z-module U, l'anneau $\mathcal{L}(U)$ des endomorphismes de U est isomorphe à un sous-anneau de $\mathcal{L}(\overline{U})$ auquel nous l'identifierons ; tout endomorphisme φ du groupe U est donc considéré comme la restriction à U de l'endomorphisme $\overline{\varphi}$ de $\overline{U}$ défini par :

Si $x \in \overline{U}$ et si $nx \in U$, $n \in Z$, $n \neq 0$, on a $n\overline{\varphi}(x) = \varphi(nx)$.

3.3.16.- THEOREME. - Soit M un groupe divisible sans torsion ; s'il existe une quasi-valuation non triviale v du système (M,B,F), où B est l'anneau des endomorphismes du groupe M et où F est le centre de B, et si A est l'anneau de quasi-valuation, alors, tout sous-A-module G de M, différent de M et de (0), est un C-groupe p-réduit. Inversement, soient G un C-groupe p-réduit $\mathcal{L}(\overline{G})$ l'anneau des endomorphismes de l'enveloppe injective $\overline{G}$ du Z-module G ; il existe une quasi-valuation v du système $(\mathcal{L}(\overline{G}),\overline{G},F)$, où F est le centre de $\mathcal{L}(\overline{G})$; l'anneau de cette quasi-valuation étant l'anneau $\mathcal{L}(G)$ des endomorphismes de G.

Démonstration. Tout élément x, non nul de M pouvant être plongé dans un facteur direct de M isomorphe à Q, le centre F de l'anneau B est isomorphe au corps Q . La quasi-valuation v , n'étant pas triviale, induit une valuation non triviale de F , d'après 3.1.10.. L'anneau de valuation V de F correspondant est, par suite, isomorphe à l'anneau Q_p , sous-anneau de Q formé des fractions r/s , où s est premier à p et où p est un nombre premier. Un sous-A-module G de M est, d'après 3.1.17., un Q_p-module ; par suite, G est divisible par tous les nombres premiers différents de p . Il est sans torsion, comme sous-groupe de M . D'après 3.1.15., δG est nul ; donc G est un groupe p-réduit. D'après 3.1.12., G est un C-groupe.

Inversement, soient a et $b\in\overline{G}$; il existe un entier positif n , pour lequel on a $p^n a$ et $p^n b\in G$ et il existe $\varphi\in\mathcal{L}(G)$ tel que $p^n a = \varphi(p^n b)$, par exemple. Donc $a = \varphi(b)$. Soit Γ l'ensemble totalement ordonné des sous-$\mathcal{L}(G)$-modules monogènes non nuls de $\overline{G}$; puisque G ne possède pas de sous-groupe divisible non nul, Γ ne possède pas de plus grand élément. L'application v de $\overline{G}$ sur $\Gamma\cup\{0\}$ définie par $v(x) = Ax$, où $A =$ (G), vérifie évidemment les axiomes I et III. Elle vérifie l'axiome II_1 , car, si H et K sont deux sous-groupes complètement invariants, non nuls de G , ils sont comparables aux sous-groupes complètement invariants de G de la forme p^kG , k entier $\geqslant 0$; par suite, il existe s , $s \geqslant 0$, tel que, si $H\subseteq K$, on a : $p^sK\subseteq H$. L'application v vérifie l'axiome II_2 , car, si, pour $f = n/m\in F$, on a : $Afx\subsetneq Ax$, où $x\in\overline{G}$, alors, p divise n ; d'où $Afy\subseteq Ay$, quel que,soit $y\in\overline{G}$.

3.3.17.- THEOREME. - <u>Soit</u> G <u>un groupe réduit possèdant des éléments, non nuls, d'ordre fini. Le treillis des sous-groupes complètement invariants de</u> G <u>est totalement ordonné si et seulement si</u> G <u>est un</u> <u>p-groupe borné de la forme suivante</u> $G = \bigoplus_{\mathfrak{m}} C(p^k) \oplus \bigoplus_{\mathfrak{n}} C(p^{k-1})$, <u>où</u> $\mathfrak{m}$ <u>et</u> $\mathfrak{n}$ <u>sont des nombres cardinaux et où</u> k <u>est un entier</u> $\geqslant 1$.

<u>Démonstration</u>. La condition est suffisante. Soit p le seul nombre premier qui, d'après 3.3.3., ne divise pas G ; le sous-groupe de torsion maximal G_t de G est, d'après 3.3.2., un groupe primaire, relativement à un nombre premier q . Puisque G_t n'est pas nul et que G est réduit, q est nécessairement égal à p , et p ne divise pas G_t . Par suite, G_t n'est pas contenu dans $\bigcap_{k=1}^{\infty} p^kG$; il existe donc un entier positif k tel que $p^kG\subseteq G_t$. Par conséquent tous les éléments de G sont d'ordre fini et G est un p-groupe. On a, alors :

$$(3.3.17.1) \qquad G = \bigcup_{k=1}^{\infty} G[p^k] .$$

Soit s un entier $\geqslant 0$; si, pour tous les entiers positifs h , le sous-groupe $G[p^h]$ était strictement contenu dans p^sG , G coïnciderait avec p^sG , d'après

(3.3.17.1) et p diviserait G. Par suite, il existe un entier positif n pour lequel on a : $p^sG \subseteq G[p^n]$; donc G est un p-groupe borné. D'après le théorème 31.3 de (Fuchs ; Abelian Groups ; Ch. V), il existe une décomposition de G en somme directe : $G = G_1 \oplus G_2 \oplus \dots \oplus G_n$, où $G_i = \bigoplus_{\mathcal{M}_i} C(p^{k_i})$ ($\mathcal{M}_i$ étant un nombre cardinal et k_i un entier > 1) et où $k_1 > k_2 > \dots > k_n$. Supposons $n > 1$. Puisque G_n est contenu dans le sous-groupe complètement invariant $G\left[p^{k_n}\right]$, l'inclusion $G\left[p^{k_n}\right] \subseteq pG$ ne peut avoir lieu ; donc $p^{k_n+1} G = (0)$. On a donc $k_1 = k_n + 1$; $n = 2$ et $G = G_1 \oplus G_2$.

La condition est suffisante. Si le groupe G est somme directe d'une famille de sous-groupes cycliques d'ordre p^k, k entier >0, il résulte de 3.3.6., que les seuls sous-groupes complètement invariants de G sont les sous-groupes p^hG, pour $h = 1,\dots,k$. Supposons que $G = \bigoplus_{\mathcal{M}} C(p^k) \oplus \bigoplus_{\mathcal{N}} C(p^{k-1})$, où $\mathcal{M}$ et $\mathcal{N}$ sont des nombres cardinaux et où k est un entier strictement supérieur à 1. Si H est un sous-groupe complètement invariant de G, on a : $H = p^rG_1 \oplus p^tG_2$, où r et t sont des entiers tels que $0 \leqslant r \leqslant k$ et $0 \leqslant t \leqslant k-1$. Soit a_1 (resp. a_2) un élément de G_1 (resp. G_2) d'ordre p^k (resp. p^{k-1}). Soit (a_i) le groupe cyclique engendré par (a_i), $i = 1,2$. D'après [21], (a_i) est fecteur direct de G_i. On a : $G_i = (a_i) \oplus G_i'$, $i = 1,2$. Soit φ l'endomorphisme de G, défini par :

$$\varphi(na_2) = npa_1 \text{ si } n \in Z \text{ ; } \varphi(x) = 0 \text{ si } x \in G_2' \text{ ; } \varphi(y) = y \text{ si } y \in G_1' .$$

Puisque $p^ta_2 \in H$, on a : $p^{t+1}a_1 \in H$; donc $r \leqslant t+1$. Soit ψ l'endomorphisme de G défini par :

$$\psi(a_1) = a_2 \text{ ; } \psi(x) = x \text{, si } x \in G_2 \text{ ; } \psi(y) = 0 \text{ si } y \in G_1' .$$

Puisque $p^ra_1 \in H$, on a : $p^ra_2 \in H$; donc $r \leq t$. Par conséquent $r = t$ ou bien $r = t+1$. Si $r = t$, on a : $H = p^rG$. Si $r = t+1$, on a $H = p^rG_1 \oplus p^{r-1}G_2 = G\left[p^{k-r}\right]$. Soit K un second sous-groupe complètement invariant de G. Si $H = p^rG$ (resp. $G[p^r]$) et $K = p^sG$ (resp. $G[p^s]$) alors H et K sont évidemment comparables. Si, par exemple, $H = p^rG$ et si $K = G[p^s] = p^{k-s}G_1 \oplus p^{k-s-1}G_2$, on a : $p^{k-s}G \subset K \subset p^{k-s-1}G$; d'où H est comparable à K.

Il résulte de 3.3.11. et de 3.3.17., le corollaire suivant :

3.3.18.- <u>Corollaire</u>. - <u>Si le groupe additif d'un anneau de largeur</u> 1 <u>est périodique, c'est un</u> p-<u>groupe borné ou un groupe quasi-cyclique, suivant qu'il est ou non réduit</u>.

§ 4.- Anneaux nilpotents de largeur 1 .

Nous noterons A^n , n entier >0 , l'idéal d'un anneau A , non unitaire, engendré par les produits de n éléments de A . L'anneau A est dit nilpotent, s'il existe un entier $h > 1$, pour lequel on a : $A^h = (0)$. L'ordre de nilpotence de A est le plus petit des entiers positifs h pour lesquels l'idéal A^h est nul.

Soit B un anneau de valuation discrète et de rang 1 d'un corps gauche K , dont le corps résiduel est le corps premier de caractéristique p . Soit A l'idéal maximal de B . Pour tout entier $n > 1$, l'anneau A/A^n est nilpotent. D'autre part, les largeurs, droite et gauche, de l'anneau A sont égales à 1 ; en effet, si a et $b \in A$, il existe $x \in B$ tel que $a = xb$, par exemple. Si $x \notin A$, il existe un entier m tel que : $x - m.1 \in A$ et $a = mb + (x-m1)b$. Par conséquent, l'anneau nilpotent A/A^n est de largeur 1 .

3.4.1. - Lemme. - Si x et y sont deux éléments d'un anneau A de largeur 1 , on a : $xy - yx \in \bigcap_{n=1}^{\infty} A^n$.

Démonstration. Il suffit de prouver que, si l'on a : $xy - yx \in A^n$, pour un entier positif n , quels que soient x et $y \in A$, alors, on a : $xy - yx \in A^{n+1}$. Soient a et $b \in A$. Si, par exemple, a appartient à l'idéal engendré par b , on a :

$$a = mb + bx + x'b + \sum_{i=1}^{i=t} y_i by'_i , \text{ où } m \in Z , x , x' , y_i \text{ et } y'_i \in A .$$

Donc :

$$ab - ba = b(xb - bx) + (x'b - bx')b + \sum_{i=1}^{i=t} (y_i by'_i b - by_i by'_i).$$

Par hypothèse, $xb - bx$ et $x'b - bx'$ appartiennent à A^n ; donc $b(bx - xb) + (x'b - bx')b$ appartient à A^{n+1} . On a, d'autre part,

$$y_i by'_i b - by_i by'_i = y_i b(y'_i b - by'_i) + (y_i b - by_i)by'_i \in A^{n+2} .$$

Par conséquent $ab - ba \in A^{n+1}$.

3.4.2. - Corollaire. - Un anneau nilpotent de largeur 1 est commutatif.

3.4.3. - Corollaire. - Si un corps K possède une valuation discrète de rang 1 et si le corps résiduel est le corps premier de caractéristique p , alors K est commutatif.

Démonstration. Soient B l'anneau de valuation de K et A l'idéal maximal de B . Puisque la valuation est discrète de rang 1 , $\bigcap_{n=1}^{\infty} A^n = (0)$; puisque A

est de largeur 1 , il est commutatif, d'après 3.4.1.. Puisque, pour toute unité x de B , on a : $x - m1 \in A$, où $m \in Z$, l'anneau B est commutatif. Donc A est commutatif.

Soient K un corps non nécessairement commutatif, v une valuation propre de K dont le groupe des valeurs Γ est commutatif, et $\mathcal{T}_v$ la topologie de K qui en résulte (se reporter à [4] ; paragraphe 5 ; numéro 1 ; page 117) ; $\mathcal{T}_v$ est l'unique topologie sur K , compatible avec la structure de groupe additif de K , pour laquelle les ensembles : $V = \{x \in K \ ; \ v(x) > \alpha\}$, $\alpha \in \Gamma$, forment un système fondamental de voisinages de 0 . Alors, si K est localement compact pour la topologie $\mathcal{T}_v$, et si le corps résiduel de K est le corps premier, il résulte de 3.4.3. que K est commutatif.

Nous dirons qu'un anneau A est <u>trivialement de largeur</u> 1 , si le treillis des sous-groupes du groupe additif A_+ de A est totalement ordonné ; i.e. si A_+ est un groupe cyclique d'ordre primaire ou un groupe quasi-cyclique.

Si A est un anneau zéro, i.e. si $A^2 = (0)$ et si A est de largeur 1, alors A est trivialement de largeur 1 .

3.4.4. - THEOREME. - <u>Soit</u> A <u>un anneau nilpotent, d'ordre de nilpotence</u> k , $k > 2$. <u>Si</u> A <u>est de largeur</u> 1 <u>non trivialement, alors, pour</u> $i = 1, 2, \dots, k-1$, <u>le groupe additif de l'anneau quotient</u> A^i/A^{i+1} <u>est un groupe cyclique d'ordre</u> p , p <u>étant un nombre premier indépendant de</u> i .

<u>Démonstration</u>. Pour tout i , l'anneau A^i/A^{i+1} est un anneau zéro. D'autre part, les sous-groupes de A^i_+ , qui contiennent A^{i+1} , sont des idéaux de l'anneau A . Donc, l'anneau A^i/A^{i+1} est trivialement de largeur 1 . Il en résulte que le groupe A_+ est périodique. Par hypothèse A_+ n'est pas cyclique. Donc d'après 3.3.8., A_+ est un p-groupe borné. On a, par suite pour tous les i , $(A^i/A^{i+1})_+ = C(p^{\alpha_i})$, où α_i est un entier positif. Donc, l'anneau A est fini. Le groupe A_+ n'étant pas cyclique, le groupe $A_+ p$ n'est pas cyclique (cf. [11] , Chap. I ; § 3 ; p. 33). Puisque le groupe A^{k-1}_+ est cyclique, on a l'inclusion : $A^{k-1} \subset A[p]$. Par conséquent, $\alpha_{k-1} = 1$. Nous prouverons successivement :

1º) <u>L'idéal</u> A^{k-1} <u>est le seul parmi les</u> A^i <u>dont le groupe additif est cyclique</u> ;

2º) <u>Le groupe</u> A^{k-2}_+ <u>est somme directe de deux groupes cycliques d'ordre</u> p ;

3º) <u>Si</u> $k > 3$, <u>le groupe additif de l'anneau</u> A/A^{k-1} <u>n'est pas cyclique</u> ;

4º) <u>Si, pour</u> $j = 2, \dots, k$, <u>le groupe cyclique</u> $(A^{j-1}/A^j)_+$ <u>est d'ordre stric-</u>

<u>tement supérieur à</u> p , <u>alors</u> $(A/A^j)_+$ <u>est cyclique</u> ;

5º) <u>Si</u> A^h <u>est le plus petit des idéaux</u> A^i , $i = 1,\dots,k-1$, <u>pour lequel le groupe</u> $(A/A^h)_+$ <u>est cyclique, alors</u> $h = 2$.

6º) <u>Le groupe</u> A/A^2 <u>est cyclique d'ordre</u> p .

Le théorème sera alors démontré.

<u>Démonstration de</u> 1º). S'il existe un entier m , $1 \leq m \leq k-1$, pour lequel A^m_+ est cyclique, on a, puisque A_+ n'est pas cyclique, $A^m \subset A[p]$. Donc $pA^m = (0)$ et $A^m = A^{k-1}$; donc $m = k-1$.

<u>Démonstration de</u> 2º). D'après 1º), le groupe A^{k-2}_+ n'est pas cyclique. Puisque A^{k-1}_+ et $(A^{k-2}/A^{k-1})_+$ sont cycliques, il existe deux éléments indépendants, et deux seulement, dans le p-groupe A^{k-2}_+ ; soient a et b deux tels éléments. Si, par exemple, b appartient à l'idéal de A engendré par a , on a : $b = ma + x$, où $m \in Z$ et $x \in A^{k-1}$. Donc $pb = pma = 0$ et l'ordre de b est p . De $A^{k-2}_+ = (b) \oplus (a)$, il résulte que $pA^{k-2}_+ = p(a)$. D'où $A^{k-1} \subseteq pA^{k-2}$ et $b-ma$ appartient à $p(a)$; par suite $b \in (a)$, ce qui n'est pas. Donc $pa = 0$.

<u>Démonstration de</u> 3º). Si le groupe additif de l'anneau $B = A/A^{k-1}$ était cyclique, $B^{k-3}_+ = (A^{k-3}/A^{k-1})_+$ serait cyclique. Donc, puisque A^{k-3} n'est pas cyclique et que A^{k-1} est cyclique, A^{k-3}_+ possèderait deux générateurs c et d . Soient p^r et p^s les ordres respectifs des éléments c et d . Si r était strictement supérieur à s , on aurait, $p^{r-1}A^{k-3} = p^{r-1}(c) = A^{k-1}$. Donc $A^{k-3}_+/A^{k-1}_+ = A^{k-3}_+/p^{r-1}A^{k-3}_+ = (d) \oplus ((c)/p^{r-1}(c))$, ce qui contredit le fait que A^{k-3}_+/A^{k-1}_+ est cyclique. Par suite, $r = s$. Si, par exemple, c appartient à l'idéal de A engendré par d , on a : $c = nd + y$, où $n \in Z$ et $y \in A^{k-2}$. Donc $pc = pnd = 0$ et $r = 1$. Par conséquent, $A^{k-2} = A^{k-3}$, ce qui est impossible. Donc B_+ n'est pas cyclique.

<u>Démonstration de</u> 4º). Puisque l'anneau A/A^j est de largeur 1, nilpotent, d'ordre de nilpotence j , et puisque $(A/A^j)^{j-1} = A^{j-1}/A^j$, si l'ordre du groupe cyclique A^{j-1}_+/A^j_+ était strictement supérieur à p , le groupe A/A^j serait cyclique, d'après 1º).

<u>Démonstration de</u> 5º). D'après l'hypothèse faite sur h , le groupe additif de l'anneau nilpotent et de largeur 1 , $A' = A/A^{h+1}$ n'est pas cyclique. Puisque le groupe additif de l'anneau A'/A'^h est cyclique, il résulte de 3º), que $h+1 = 3$; d'où $h = 2$.

<u>Démonstration de</u> 6º). D'après 5º), le groupe additif de l'anneau $C = A/A^3$ n'est pas cyclique. Le groupe C^2_+ est cyclique d'ordre p . D'après 2º), C_+ est

somme directe de deux groupes cycliques d'ordre p et, par suite, $(A/A^2)_+$ est cyclique d'ordre p.

3.4.5. - THEOREME. - <u>Soient</u> A <u>un anneau nilpotent et</u> k <u>son ordre de nilpotence. Si, pour</u> $i = 1,2,\dots, k-1$, <u>le groupe additif de l'anneau</u> A^i/A^{i+1} <u>est un groupe cyclique d'ordre</u> p, <u>les seuls idéaux de</u> A <u>sont les</u> A^i.

<u>Démonstration</u>. Soit I un idéal non nul de A. Il existe un entier i, $1 \leqslant i \leqslant k-1$, pour lequel on a : $I \subseteq A^i$ et $I \nsubseteq A^{i+1}$. Par suite, A^i coïncide avec l'idéal $A^{i+1} + I$ engendré par A^{i+1} et I : $A^i = I + A^{i+1}$. Si $k = i+1$, alors $A^i = I$; sinon, on a, puisque $A^k = (0)$, $A^{k-1} = IA^{k-i-1} \subset I$. Supposons que $A^s \subset I$, pour un entier $s > i+1$. On a, alors, $A^{s-1} = A^s + IA^{s-1-i} \subset I$. Par conséquent $A^{i+1} \subset I$; d'où $A^i = I$.

Nous poserons, dans le théorème suivant, $T_e = Z/p^eZ$, où p est un nombre premier et e un entier >1. Nous noterons $T_e[X]$ l'anneau des polynômes en X sur l'anneau T_e.

3.4.6. - THEOREME. - <u>Un anneau</u> A <u>nilpotent, d'ordre de nilpotence</u> $k > 2$, <u>est de largeur</u> 1 <u>non trivialement, si et seulement s'il est isomorphe à un anneau de la forme</u> : $B/\mathfrak{a}$, <u>où</u> $B = (XT_e[X])/(X^kT_e[X])$ <u>et où</u> $\mathfrak{a}$ <u>est un idéal de</u> B <u>qui ne contient aucune puissance de</u> B <u>autre que</u> $B^k = (0)$ <u>et tel que</u> : $B^2 + pB = B^2 + \mathfrak{a}$.

<u>Démonstration</u>. Soient A un anneau nilpotent, non trivialement de largeur 1, p^e la borne supérieure des ordres de ses éléments et k son ordre de nilpotence. Soit a un générateur de l'idéal A. Tout élément de A est donc combinaison linéaire à coefficients entiers des a^i, $i = 1,\dots, k-1$. Soit $B = (XT_e[X])/(X^kT_e[X]) = T_eu \oplus \dots \oplus T_eu^{k-1}$, où u est la classe de X modulo $X^kT_e[X]$. On définit un homomorphisme de l'anneau B sur l'anneau A, en faisant correspondre l'élément a à l'élément u. Donc A est isomorphe à $B/\mathfrak{a}$, où $\mathfrak{a}$ est un idéal de B. Pour démontrer le théorème il suffit donc de prouver que l'anneau $B/\mathfrak{a}$ est d'ordre de nilpotence k et de largeur 1 si et seulement si : $B^i \nsubseteq \mathfrak{a}$, pour $i \neq k$ et $B^2 + pB = B^2 + \mathfrak{a}$. Il est évident que l'ordre de nilpotence de $B/\mathfrak{a}$ est k si et seulement si $B^i \nsubseteq \mathfrak{a}$, pour $i \neq k$. La condition $B^2 + pB = B^2 + \mathfrak{a}$ signifie que le groupe $B/(B^2 + \mathfrak{a}) (\cong (B/\mathfrak{a})/(B/\mathfrak{a})^2)$ est cyclique d'ordre p. Cette condition est satisfaite d'après 3.4.4., dès que $B/\mathfrak{a}$ est de largeur 1. Il suffit donc de prouver que si $B^i \nsubseteq \mathfrak{a}$, pour $i \neq k$, et si $B/(B^2 + \mathfrak{a})$ est cyclique d'ordre p, alors $(B^i + \mathfrak{a})/(B^{i+1} + \mathfrak{a})$ est cyclique d'ordre p, pour $i = 2,\dots, k-1$. L'homomorphisme surjectif évident du groupe $B/(B^2 + \mathfrak{a})$ sur $(B^i + \mathfrak{a})/$

$/(B^{i+1}+\mathfrak{G})$ est aussi injectif car $B/(B^2+\mathfrak{G})$ est cyclique d'ordre p et que $B^i \not\subset \mathfrak{G}$. Donc $(B^i+\mathfrak{G})/(B^{i+1}+\mathfrak{G}) = (B/\mathfrak{G})^i/(B/\mathfrak{G})^{i+1}$ est cyclique d'ordre p.

CHAPITRE IV

Groupes p-réduits

Tous les groupes considérés dans ce chapitre sont supposés commutatifs.

§ 1.- Préliminaires.

Nous donnons ici des propriétés des groupes p-réduits, qui ont été introduits en 3.3.12..

Pour qu'un sous-groupe d'un groupe p-réduit soit lui-même p-réduit, il faut et il suffit qu'il soit divisible par tous les nombres premiers différents de p .

Tout sous-groupe pur d'un groupe p-réduit est p-réduit. Un sous-groupe p-réduit S d'un groupe p-réduit G est pur si : $pG \cap S = pS$.

Le groupe additif de l'anneau $\mathfrak{I}$ des entiers p-adiques est p-réduit, ainsi que chaque sous-groupe pur de $\mathfrak{I}$. En particulier, le groupe additif de l'anneau Q_p , sous-anneau du corps des rationnels Q formé des fractions r/s , où s est premier à p , est p-réduit.

Un groupe p-réduit G peut être muni d'une structure de module sur l'anneau Q_p ; ce module est sans torsion. La topologie induite sur G par celle de Q_p admet le système des p^kG comme base de voisinages de 0 et elle est séparée, puisque, d'après 3.3.12., on a : $\bigcap_{k=1}^{\infty} p^kG = (0)$. Inversement, le groupe additif sous-jacent d'un Q_p-module sans torsion et dont la topologie p-adique est séparée est un groupe p-réduit.

Tous les résultats de ce chapitre sont valables pour des modules sans torsion sur un anneau commutatif V qui est un anneau de valuation discrète de rang 1 , pourvu que ces modules soient séparés pour la topologie induite par celle de V .

Si G est un groupe p-réduit, le complété $\hat{G}$ de G pour la topologie p-adique est muni d'une structure de module sur l'anneau $\mathfrak{I}$ et il est séparé et complet pour cette topologie (cf. [3] ; Chap. III; § 6 ; nº 6). Par suite, le groupe $\hat{G}$ est divisible par tous les nombres premiers différents de p et il est réduit. On prouve, comme dans [14] que G est un sous-groupe pur de $\hat{G}$ et que le groupe $\hat{G}$ est sans torsion. Par suite, le groupe $\hat{G}$ est p-réduit.

Rappelons que, dans un groupe sans torsion, G, un système d'éléments $(a_\lambda)_{\lambda\in\Lambda}$ est dit <u>indépendant</u>, s'il est linéairement indépendant dans le Q-espace vectoriel $Q \otimes_Z G$. Chaque système indépendant de G peut être plongé dans un système indépendant maximal, i.e. dans une base de $Q \otimes_Z G$. Deux systèmes indépendants maximaux ont le même nombre cardinal, auquel on donne le nom de <u>rang</u> de G et qui est la dimension du Q-espace vectoriel $Q \otimes_Z G$.

De la caractérisation des groupes sans torsion de rang 1 (cf. [11] ; Chap. VII; § 42), <u>il résulte que tout groupe p-réduit de rang 1 est isomorphe à</u> Q_p.

Une famille $(a_\lambda)_{\lambda\in\Lambda}$ d'éléments non nuls d'un p-groupe G est dite <u>indépendante</u> si une relation de la forme suivante :

$$\sum_{i=1}^{i=n} m_i a_{\lambda_i} = 0 \qquad \lambda_i \in \Lambda \quad \text{et} \quad m_i \in Z$$

entraîne que l'ordre de a_{λ_i} divise m_i, pour $i = 1,\dots,n$.

4.1.1. - <u>Définition</u>. - Soit G un groupe sans torsion. Une famille $(a_\lambda)_{\lambda\in\Lambda}$ d'éléments de G est dite <u>indépendante modulo</u> p^kG, k entier > 0, si $(\bar{a}_\lambda)_{\lambda\in\Lambda}$, où $\bar{a}_\lambda$ désigne la classe de a_λ modulo p^kG, est un système indépendant du p-groupe G/p^kG.

4.1.2. - <u>Lemme</u>. - <u>Soit</u> G <u>un groupe sans torsion. Un système</u> $(a_\lambda)_{\lambda\in\Lambda}$ <u>d'éléments de</u> G <u>est indépendant modulo</u> p^kG, k <u>entier</u> >0, <u>si et seulement s'il est indépendant modulo</u> pG.

<u>Démonstration</u>. D'après 4.1.1., tout système indépendant modulo p^kG est indépendant modulo pG. Le groupe G, étant sans torsion, tout système indépendant modulo pG est indépendant modulo p^kG.

Soit G un groupe sans torsion ; un système $(a_\lambda)_{\lambda\in\Lambda}$, indépendant modulo p^kG peut être plongé dans un système $(b_\mu)_{\mu\in M}$, indépendant modulo p^kG et maximal vis-à-vis de cette propriété. Nous dirons que le système $(b_\mu)_{\mu\in M}$ est <u>maximalement indépendant modulo</u> p^kG (en abrégé : m-indépendant mod. pG).

Il résulte de 4.1.2., qu'un système est m-indépendant mod. pG si et seulement s'il est m-indépendant mod. p^kG, k entier $\geqslant 1$.

4.1.3. - <u>Définition</u>. - On appelle <u>base</u> d'un groupe p-réduit G, tout système m-indépendant mod. pG, i.e. tout système d'éléments de G dont l'image dans G/pG est une base du F_p-espace vectoriel G/pG, où F_p désigne le corps à p éléments.

4.1.4. – *Proposition*. – *Toute base d'un groupe* p–*réduit* G *est une base de son complété*.

Démonstration. Puisque G est pur dans $\hat{G}$, une base S de G est un système indépendant mod. $p\hat{G}$. Le système S est une base de $\hat{G}$, puisque pour tout $x \in G$, il existe $y \in \hat{G}$, tel que $x - y \in p\hat{G}$.

Deux bases d'un groupe p–réduit G ont le même nombre cardinal, qui est la dimension du F_p–espace vectoriel G/pG .

4.1.5. – *Définition*. – On appelle *dimension* d'un groupe p–réduit le nombre cardinal d'une de ses bases.

Un système indépendant mod. pG d'un groupe p–réduit G étant, en particulier un système indépendant du groupe sans torsion G , *la dimension de* G *est inférieure à son rang*.

Un système indépendant mod. pG d'un groupe p–réduit G étant, en particulier, un système indépendant du groupe sans torsion G , *la dimension de* G *est inférieure à son rang*.

Un groupe sans torsion est dit complètement décomposable s'il est isomorphe à une somme directe de groupes de rang 1 (cf. [11] ; Chap. VII ; § 46). Par suite, *un groupe* p–*réduit est complètement décomposable si et seulement s'il est somme directe d'une famille de sous-groupes isomorphes à* Q_p .

Soient G un groupe p–réduit, $L = (a_\lambda)_{\lambda \in \Lambda}$ une base de G et S_λ le sous-groupe de rang 1 , pur dans G , engendré par $a_\lambda \in L$ (cf. [11] ; Chap. IV ; § 24 ; N).

4.1.6. – *Définition*. – Nous dirons que le groupe $B = \bigoplus_{\lambda \in \Lambda} S_\lambda$ est le *sous-groupe de base* de G associé à la base L .

Deux sous-groupes de base d'un groupe p–réduit sont isomorphes.

4.1.7. – *Proposition*. – *Un sous-groupe* B *d'un groupe* p–*réduit* G *est un sous-groupe de base de* G *si et seulement s'il vérifie les conditions suivantes* :

1º) B *est un groupe* p–*réduit complètement décomposable* ;

2º) B *est un sous-groupe pur de* G ;

3º) *Le groupe* G/B *est divisible*.

Démonstration. Si B est un sous-groupe de base de G associé à la base $L = (a_\lambda)_{\lambda \in \Lambda}$, il vérifie, par définition, la condition 1º). Soit $px \in B$, où $x \in G$. D'après la définition de B , il existe un entier n , premier à p , tel que :

$npx = m_1 a_{\lambda_1} + m_2 a_{\lambda_2} + \ldots + m_s a_{\lambda_s}$, où m_i Z et $a_{\lambda_i} \in L$. Par suite, p divise m_i , $i = 1,\ldots,s$. On a donc $nx \in B$ et, puisque B est p-réduit, $x \in B$. Le groupe G étant homomorphe à G/B , le groupe G/B est divisible par tous les nombres premiers différents de p . Il suffit donc pour prouver 3º), de vérifier que p divise G/B . Soit $x \in G$, $x \notin B$; le système $\{x\} \cup L$, étant dépendant modulo pG , il existe $b \in B$ et $g \in G$ tel que $x - pg \in B$; d'où p divise G/B. Réciproquement, si $B = \bigoplus_{\lambda \in \Lambda} S_\lambda$, où les groupes S_λ sont isomorphes à Q_p , on obtient, en choisissant, pour chaque λ un élément et un seul $a_\lambda \in S_\lambda$, $a_\lambda \notin pS_\lambda$, une base L du groupe p-réduit B ; puisque B est pur dans G , le système L est indépendant modulo pG ; il résulte de 3º) que L est m-indépendant mod. pG . Il est évident que B est le sous-groupe de base de G associé à la base L.

4.1.8. - THEOREME. - <u>Pour un groupe</u> p-<u>réduit</u> G , <u>les deux conditions suivantes sont équivalentes</u> :

(i) <u>Le rang de</u> G <u>est fini et est égal à la dimension de</u> G ;

(ii) <u>Le groupe</u> G <u>coïncide avec chacun de ses sous-groupes de base</u>.

<u>Démonstration</u>. (i) $\Rightarrow$ (ii). Si (i) est vérifiée, une base L de G est aussi un système indépendant maximal du groupe sans torsion G . Puisque L est fini, si B est le sous-groupe de base de G qui lui est associé, le groupe G/B est un groupe de torsion. Donc puisque B est pur dans G , on a : G = B .

(ii) $\Rightarrow$ (i). Si (ii) est vérifiée, le rang de G et sa dimension sont égaux. Nous allons prouver que tout sous-groupe pur S de G est facteur direct de G et que, si la dimension de G est infinie, il existe un sous-groupe pur de G qui ne peut être facteur direct. Si S est un sous-groupe pur de G , soit U = $= (a_\lambda)_{\lambda \in \Lambda}$ une base du groupe p-réduit S . Puisque S est pur dans G , le système U est indépendant mod. pG . On peut donc plonger U dans une base L de G ; posons $L = U \cup V$, où $V = (b_\mu)_{\mu \in M}$. Par hypothèse, on a : $G = \bigoplus_{\lambda \in \Lambda} S_\lambda \oplus \bigoplus_{\mu \in M} T_\mu$, où S_λ et T_μ sont, respectivement, les sous-groupes de rang 1, purs dans G , engendrés par a_λ et b_μ . On a : $\bigoplus_{\lambda \in \Lambda} S_\lambda \subseteq S$ et $S \cap \bigoplus_{\mu \in M} T_\mu = (0)$; donc $S = \bigoplus_{\lambda \in \Lambda} S_\lambda$ et, par suite, S est facteur direct de G . D'autre part, si la dimension et, par suite, le rang de G est infini, il existe une infinité dénombrable d'éléments indépendants de G ; soit $(a_i)_{i \in N}$ une telle famille et soit H le sous-groupe pur de G engendré par les éléments : $a_k - (k+1)a_{k+1}$, où $k \in N$; l'élément a_1 n'appartient pas à H et le groupe G/H contient un sous-groupe divisible engendré par les images des a_i , $i \in N$. Donc, puisque G est réduit, H ne peut être facteur direct de G . (cf. [12]).

§ 2.- Sous-groupes ouverts des groupes p-réduits.

Un sous-groupe ouvert H d'un groupe p-réduit G est un sous-groupe ouvert de G pour la topologie p-adique, i.e. un sous-groupe pour lequel il existe un entier k , $k \geqslant 0$, tel que $p^k G \subseteq H$.

Un sous-groupe ouvert d'un groupe p-réduit est évidemment p-réduit.

4.2.1. - Définition. - Soient G un groupe p-réduit et H un sous-groupe de G, $pG \subsetneq H \subset G$. Si G est différent de H , nous dirons qu'une famille $(b_\mu)_{\mu \in M}$ d'éléments de G est indépendante modulo H , si la famille $(\bar{b}_\mu)_{\mu \in M}$, où $\bar{b}_\mu$ est la classe de b_μ modulo H , est linéairement indépendante dans le F_p-espace vectoriel G/H .

4.2.2. - Lemme. - *Soient G un groupe p-réduit, H un sous-groupe de G , $pG \subsetneq H \subset G$ et $L = (a_\lambda)_{\lambda \in \Lambda}$ une base de G . Si le système L est indépendant modulo H , on a : $H = pG$.*

Démonstration. En effet, $(\bar{a}_\lambda)_{\lambda \in \Lambda}$, où $\bar{a}_\lambda$ désigne la classe de a_λ modulo H , est alors une base de G/H sur F_p .

4.2.3. - Lemme. - *Soient G un groupe p-réduit, H un sous-groupe de G tel que $pG \subset H \subset G$, $L = (a_\lambda)_{\lambda \in \Lambda}$ une base de G et M un système d'éléments de G indépendants modulo H et contenu dans L . Alors :*

1º) *Il existe un système $S = (a_\gamma)_{\gamma \in N}$, $M \subset S \subset L$, indépendant modulo H et maximal ;*

2º) *Il existe un système T de G , indépendant modulo pG , tel que $S \cup T$ est une base de G ;*

3º) *Le sous-groupe de base de G , associé à la base $S \cup T$ coïncide avec le sous-groupe de base de G associé à la base L ;*

4º) *Le système $pS \cup T$ est une base du groupe p-réduit H , où l'on pose $pS = (pa_\nu)_{\nu \in N}$.*

Démonstration. Puisque $H \neq G$, L n'est pas contenu dans H . La famille $\mathfrak{F}$ des sous-systèmes de L qui contiennent M et qui sont indépendants modulo H est inductive. Il existe donc un élément maximal $S = (a_\nu)_{\nu \in N}$ de $\mathfrak{F}$. D'après 4.2.2. et puisque $H \neq pG$, S est différent de L . Par conséquent $L = S \cup R$ et $R \neq \emptyset$. Posons $R = (a_\mu)_{\mu \in \rho}$ où ρ est le complémentaire de N dans Λ . Puisque S est un élément maximal de la famille $\mathfrak{F}$, on a , pour chaque $a_\mu \in R$, une relation de la forme : $a + \sum_{i=1}^{k} r_i a_{\nu_i}$ H , où $r_i \in Q_p$ et $a_{\nu_i} \in S$. Posons

$b = a + \sum_{i=1}^{k} r_i a_{\nu_i}$ pour une relation de la forme précédente qui correspond à l'élément a_μ . Soit $T = (b_\mu)_{\mu \in \rho}$. Alors $S \cup T$ est évidemment une base de G , car, en raisonnant modulo pG , on a effectué un changement de base dans le F_p-espace vectoriel G/pG . Le sous-groupe de base de G associé à la base $S \cup T$ coïncide avec le sous-groupe de base B de G associé à la base L ; en effet, on a : $B = \bigoplus_{\mu \in \rho} Q_p a_\mu \oplus \bigoplus_{\nu \in N} Q_p a_\nu$; d'après sa définition, b_μ appartient à B . Donc $\bigoplus_{\mu \in \rho} Q_p b_\mu \oplus \bigoplus_{\nu \in N} Q_p a_\nu$ est contenu dans B . Puisque $a_\mu = b_\mu - \sum_{i=1}^{k} r_i a_{\nu_i}$, on a : $B = \bigoplus_{\mu \in \rho} Q_p b_\mu \oplus \bigoplus_{\nu \in N} Q_p a_\nu$. Le système $pS \cup T$, où $pS = (pa_\nu)_{\nu \in N}$, est contenu dans H et il est indépendant modulo pH , puisque $S \cup T$ est indépendant modulo pG et que S est indépendant modulo H . Nous allons prouver que $pS \cup T$ est une base de H . Soit $x \in H$. Puisque $S \cup T$ est une base de G , on a :

(4.2.3.1) $nx + \sum_{i=1}^{s} n_i a_{\nu_i} + \sum_{i=1}^{t} n'_i b_{\mu_i} \in pG$ où n_i et $n'_i \in Z$, $a_{\nu_i} \in S$ et $b_{\mu_i} \in T$

et n est un entier premier à p . Puisque $x \in H$, que $T \subset H$ et que $pG \subset H$, on a : $\sum_{i=1}^{s} n_i a_{\nu_i} \in H$. Puisque S est indépendant modulo H , p divise les n_i . La relation (4.2.3.1) s'écrit :

(4.2.3.2) $nx + \sum_{i=1}^{t} n'_i b = pg$ où $g \in G$.

Le système $\{g\} \cup S \cup T$, étant dépendant modulo pG , le système $\{g\} \cup S$ est dépendant modulo H ; on a donc : $mg + \sum_{i=1}^{k} m_i a_{\nu_i} \in H$, où m est premier à p . D'après (4.2.3.2), $mnx + \sum_{i=1}^{t} mn'_i b_{\mu_i} + \sum_{i=1}^{k} m_i pa_{\nu_i} \in pH$. Donc, puisque mn est premier à p , le système $\{x\} \cup (b_\mu)_{\mu \in \rho} \cup (pa_\nu)_{\nu \in N}$ est dépendant modulo pH .

4.2.4. - Lemme. - Soient G un groupe p-réduit, H un sous-groupe de G tel que $p^k G \subset H \subset G$ et $L = (a_\lambda)_{\lambda \in \Lambda}$ une base de G . Alors il existe une base U de G telle que :

1º) Le sous-groupe de base de G associé à U est le même que celui associé à L ;

2º) On a : $U = U_1 \cup U_2 \cup \dots \cup U_{k+1}$, où les U_i sont des sous-ensembles disjoints de U , dont certains peuvent être vides, tels que $U_1 \cup pU_2 \cup \dots \cup p^k U_{k+1}$ est une base de H .

Démonstration. Pour $k = 1$, le lemme a été démontré en 4.6.3.. Supposons que $k \neq 1$ et que le lemme soit démontré pour $k-1$. Posons $K = \{x \in G \; ; \; px \in H\}$; K est un sous-groupe de G et $p^{k-1} G \subset K \subset G$. Soit $L = (a_\lambda)_{\lambda \in \Lambda}$ une base de G . D'après l'hypothèse de récurrence il existe une base V de G tel que le sous-groupe de base de G associé à L coïncide avec celui associé à V. On a : $V = V_1 \cup V_2 \cup \dots \cup V_k$ où les V_i sont disjoints et où $V_1 \cup pV_2 \cup \dots \cup p^{k-1}V_k$ est une base de K. D'après la définition de K, le système $pV_2 \cup \dots \cup p^{k-1}V_k$ de K est indépendant modulo H. Puisque $pK \subset H \subset K$, il existe, d'après 4.2.3. 1º) un système $U = T_1 \cup pV_2 \cup \dots \cup p^{k-1}V_k$, où $T_1 \subset V_1$ qui est indépendant modulo H et maximal. D'après 4.2.3. 2º), il existe un système T_1' de K indépendant modulo pK, tel que $T_1' \cup T_1 \cup pV_2 \cup \dots \cup p^{k-1}V_k$ est une base de K. De plus le sous-groupe de base de K associé à la base $T_1' \cup T_1 \cup pV_2 \cup \dots \cup p^{k-1}V_k$ coïncide avec le sous-groupe de base de K associé à $V_1 \cup pV_2 \cup \dots \cup p^{k-1}V_k$. Par suite, le sous-groupe de base de G associé à V coïncide avec le sous-groupe de base de G associé à $T_1' \cup T_1 \cup V_2 \cup \dots \cup V_k$. D'après 4.2.3. 4º), $T_1' \cup pT_1 \cup p^2V_2 \cup \dots \cup p^kV_k$ est une base de H.

4.2.5. - THEOREME. - <u>Soient</u> G <u>un groupe</u> p-<u>réduit</u>, H <u>un sous-groupe ouvert de</u> G, s <u>le plus petit entier</u> $\geqslant 0$ <u>pour lequel</u> : $p^sG \subseteq H$, ℓ <u>le plus grand entier</u> $\geqslant 0$ <u>pour lequel</u> $H \subseteq p^\ell G$ <u>et</u> $k = s-1$. <u>Alors, pour tout sous-groupe de base</u> B <u>de</u> G, <u>il existe une décomposition en somme directe</u> : $B = B_1 \oplus \dots \oplus B_{k+1}$ <u>telle que</u> $p^\ell B_1 \oplus \dots \oplus p^{k+\ell}B_{k+1}$ <u>soit un sous-groupe de base du groupe</u> p-<u>réduit</u> H <u>et que</u> H <u>soit l'adhérence, dans</u> G, <u>pour la topologie</u> p-<u>adique de</u> $p^\ell(B_1 \oplus \dots \oplus p^kB_{k+1})$.

<u>Démonstration</u>. Puisque $H = p^\ell V$, où V est un sous-groupe ouvert de G, $p^kG \subset V \subset G$ et $V \not\subset pG$, on peut supposer que $\ell = 0$. On a donc : $p^kG \subset H \subset G$, $H \not\subset pG$ et $p^{k-1}G \not\subset H$. On peut supposer que $H \neq G$. Soit C un sous-groupe de base du groupe p-réduit H. Puisque H est un sous-groupe fermé de G, l'adhérence de C dans G est contenue dans H. D'autre part, d'après 4.1.2., on a, quel que soit $n \geqslant 0$, $H = C + p^nH$; donc $H \subset C + p^nG$ et H est contenu dans l'adhérence de C dans G. Par suite, H est l'adhérence de C dans G. Il suffit donc de prouver que, pour tout sous-groupe de base B de G, il existe une décomposition en somme directe : $B = B_1 \oplus \dots \oplus B_{k+1}$ telle que $B_1 \oplus pB_2 \oplus \dots \oplus p^kB_{k+1}$ soit un sous-groupe de base de H. Soit L une base de G à laquelle est associé le sous-groupe de base B. D'après 4.2.4., il existe une base U de G telle que le sous-groupe de base associé à U soit B. On a : $U = U_1 \cup \dots \cup U_{k+1}$, où les U_i sont deux à deux disjoints. Si U_i n'est pas vide, posons : $U_i = (b_\mu^{(i)})_{\mu \in M_i}$ Soit $B_i = \bigoplus_{\mu \in M_i} S_\mu^{(i)}$, où $S_\mu^{(i)}$ est le sous-groupe pur de rang 1 de G engendré par un élément $b_\mu^{(i)}$ de U_i. Si $U_i = \emptyset$, on posera $B_i = (0)$. Alors, on a : $B = \bigoplus_{i=1}^{k} B_i$. De plus, pour $i = 0,\dots,k$, $p^iS_\mu^{(i+1)}$ est un sous-groupe de rang 1 et pur de H. Donc $B_1 \oplus pB_2 \oplus \dots \oplus p^kB_{k+1}$ est un sous-groupe de base de H,

puisque $U_1 \cup \ldots \cup p^k U_{k+1}$ est, d'après 4.2.4., une base de H .

Soit $(G_i)_{i\in I}$ une famille de sous-groupes p-réduits d'un groupe p-réduit G ; le sous-groupe de G , engendré par cette famille, et l'intersection des G_i sont des sous-groupes p-réduits de G (on admet que (0) est p-réduit). Par suite :

4.2.6. - Proposition. - *La famille des sous-groupes p-réduits d'un groupe p-réduit G est un sous-treillis complet du treillis des sous-groupes de G .*

4.2.7. - THEOREME. - *Pour qu'un sous-groupe d'un groupe p-réduit G soit un sous-groupe maximal de G , il faut et il suffit qu'il soit maximal dans le treillis des sous-groupes p-réduits de G .*

Démonstration. La condition est nécessaire. Soit M un sous-groupe maximal de G . Le groupe G/M étant simple et G étant divisible par tous les nombres premiers différents de p , le groupe G/M est cyclique d'ordre p ; d'où $pG \subseteq M$ et M est p-réduit. Le groupe M est évidemment maximal dans le treillis des sous-groupes p-réduits de G . La condition est suffisante. Soit M un élément maximal du treillis des sous-groupes p-réduits de G . Il suffit de prouver que $pG \subseteq M$. Si $pG \subseteq M$, il existe $g \subseteq G$ tel que $pg \notin M$. Soit $S = \{rpg \ ; \ r \in Q_p\}$. L'ensemble S est un sous-groupe p-réduit de G . On a : $G=M+S$. D'où $g = x+mpg$ $x \in M$ et $m \in Z$. Comme M est p-réduit et que $1-mp$ est premier à p , g appartient à M , ce qui contredit l'hypothèse. Donc M contient pG .

4.2.8. - THEOREME. - *Un sous-groupe M d'un groupe p-réduit G est maximal si et seulement si il existe un sous-groupe de base B de G et une décomposition en somme directe $B = B_1 \oplus B_2$ telle que B_2 soit un groupe de rang 1 et que M soit l'adhérence dans G de $B_1 \oplus pB_2$.*

Démonstration. Si M est un sous-groupe maximal de G , il est ouvert et $pH \subseteq M$, d'après la démonstration de 4.2.7.. Les sous-systèmes d'une base L de G qui sont indépendants modulo M , possèdent un et un seul élément, puisque, si y et $z \in G$, on a : $y = x + nz$, où $x \in M$ et $n \in Z$. La proposition résulte donc de 4.2.5.. Réciproquement, si M est l'adhérence dans G de $B_1 \oplus pB_2$, où $B_1 \oplus B_2$ est un sous-groupe de base de G et où B_2 est de rang 1 , soit H un sous-groupe de G tel que $M \subsetneq H \subset G$; alors : $B_2 \notin H$. Si $y \in H$, on a $y=b_1+b_2+pg$, où $b_1 \in B_1$, $b_2 \in B_2$ et $g \in G$; puisque $b_1 \in M$ et que $pg \in M$, on a : $b_2 \in M$ et $y \in M$. D'où $H = M$.

§ 3.- Sous-groupes complètement invariants des groupes p-réduits.

Soient G un groupe p-réduit, $\hat{G}$ le complété de G et $\mathcal{L}(G)$ l'anneau des endomorphismes de G . Si $\varphi \in \mathcal{L}(G)$, φ est compatible avec la filtration $p^n G$; donc φ est continue. Par suite, si $x = \lim(x_n) \in \hat{G}$, où (x_n) est une suite de Cauchy de G , $(\varphi(x_n))$ est une suite de Cauchy de G et l'application $\hat{\varphi}$, qui à x fait correspondre $y = \lim(\varphi(x_n)) \in \hat{G}$ est un endomorphisme du groupe $\hat{G}$. L'application qui à $\varphi \in \mathcal{L}(G)$ fait correspondre $\hat{\varphi}$ dans l'anneau $\mathcal{L}(\hat{G})$ des endomorphismes de $\hat{G}$, est un isomorphisme de $\mathcal{L}(G)$, sur un sous-anneau de $\mathcal{L}(\hat{G})$. Dans la suite, nous identifierons $\mathcal{L}(G)$ au sous-anneau de $\mathcal{L}(\hat{G})$ auquel il est isomorphe.

Soient G un groupe p-réduit et π un entier p-adique, on notera $G\{\pi\}$ l'ensemble des éléments x de G pour lesquels l'élément πx de $\hat{G}$ appartient à G .

4.3.1. - <u>Proposition</u>. - <u>Quel que soit l'entier</u> p-<u>adique</u> π , <u>l'ensemble</u> $G\{\pi\}$ <u>est un sous-groupe pur et complètement invariant de</u> G .

<u>Démonstration</u>. On a évidemment $\pi(x-y) \in G$, dès que πx et $\pi y \in G$. Si $p\pi x \in G$, on a puisque G est pur dans $\hat{G}$, $\pi x \in G$; donc $G\{\pi\}$ est un sous-groupe pur de G . Enfin, si $\varphi \in \mathcal{L}(G)$ et si $\pi x \in G$, où $x \in G$ et $\pi \in \mathcal{P}$, on a : $\varphi(\pi x) = \hat{\varphi}(\pi x) = \pi\hat{\varphi}(x) = \pi\varphi(x)$. Donc $\pi\varphi(x) \in G$ et $G\{\pi\}$ est un sous-groupe complètement invariant de G .

4.3.2. - <u>Définition</u>. - Un groupe p-réduit G est dit homogène si, pour tout entier p-adique π on a , soit $G\{\pi\} = G$ soit $G\{\pi\} = (0)$.

Tout C-groupe p-réduit est homogène.

Puisque les sous-groupes complètement invariants du groupe Q_p sont les sous-groupes $p^k Q_p$, k entier $\geqslant 0$, et (0), il résulte de 3.3.6., que les sous-groupes complètement invariants d'un groupe p-réduit complètement décomposable G sont (0) et les $p^k G$, k entier $\geqslant 0$.

4.3.2. - <u>Proposition</u>. - <u>Soit</u> G <u>un</u> $\mathcal{P}$-<u>module sans torsion séparé pour la topologie</u> p-<u>adique. Les sous-groupes complètement invariants de</u> G <u>sont</u> (0) <u>et les sous-groupes</u> $p^k G$, k <u>entier</u> $\geqslant 0$.

<u>Démonstration</u>. D'après le théorème 44.3 de ([11] ; Chap. VII), tout élément x , non nul de G peut être plongé dans un facteur direct S de G isomorphe à $\mathcal{P}$; en particulier, si $x \notin pG$, on a : $S = \mathcal{P}x$. Soit H un sous-groupe complètement invariant non nul de G et soit $a \in H$, $a \neq 0$; alors, $a = p^n x$, où $x \in G$ et $x \notin pG$. On a : $p^n \mathcal{P} x \subseteq \mathcal{P} x \cap H$. D'où, d'après 3.3.5., $p^n y$ appartient à H quel que soit $y \in G$. Par conséquent, il existe un entier k , $k \geqslant 0$, pour lequel on a : $H = p^k G$.

BIBLIOGRAPHIE

[1] R. BAER. - The subgroup of the elements of finite order of an abelian group. Ann. Math. 37 (1936) 766-781.

[2] R. BAER. - Abelian groups without elements of finite order. Duke Math. Jour. 3 (1937) 68-122.

[3] N. BOURBAKI. - Topologie Générale, Livre III, ch. III, 3e éd. Hermann - Paris.

[4] N. BOURBAKI. - Algèbre Commutative, Ch. VI. Hermann - Paris.

[5] S. J. BRYANT et J. L. ZEMMER. - A note on completely primary rings. Proc. Amer. Soc. 8 (1957) 140-141.

[6] I. S. COHEN. - On the structure and ideal theory of complete local rings. Trans. Amer. Math. Soc. 59 (1946) 54-106.

[7] I. S. COHEN. - Commutative rings with restricted minimum condition. Duke Math. Jour. 17 (1950) 27-42.

[8] C. W. CURTIS et I. REINER. - Representation theory of finite groups and associative algebra. Pure and Applied Mathematics, Vol. XI. Interscience Publishers - London.

[9] P. DUBREIL. - Algèbre I. Gauthiers-Villars - Paris.

[10] P. DUBREIL. - Problèmes d'algèbre liés à la théorie des demi-groupes. Colloque de Bruxelles 1957 29-44.

[11] L. FUCHS. - Abelian groups. Budapest, Hungarian Academy of Sciences, 1958.

[12] L. FUCHS, A. KERTESZ, T. SZELE. - Abelian groups in which every serving subgroup is a direct summand. Publ. Math. Debrecen. 3 (1953) 95-105.

[13] R. E. JOHNSON. - Equivalence rings. Duke Math. Jour. 15 (1948) 65-74.

[14] I. KAPLANSKY. - Infinite Abelian Groups. Ann. Arbor. Univ. Michigan Press. 1954.

[15] M. NAGATA. - Local rings. Interscience tracts in pure and applied Mathematics, nº 13.

[16] D. G. NORTHCOTT. - A general theory of one dimensional local rings. Proc. Glasgow Math. Ass. 2 (1954-1956) 159-169.

[17] E. C. POSNER. - Left valuation rings and simple radical rings. Trans. Amer. Math. Soc. 107 (1962) 458-465.

[18] P. SAMUEL. - Algèbre locale. Gauthiers-Villars - Paris.

[19] P. SAMUEL et O. ZARISKI. - Commutative algebra II. Univ. series in higher Math. 1959.

[20] J. P. SERRE. - Corps locaux. Hermann - Paris.

[21] T. SZELE. - On direct decomposition of abelian groups. J. London Math. Soc. 28 (1953) 247-250.

[22] O. F. G. SCHILLING. - The theory of valuations. Amer. Math. Soc. 1950

Joseph FLOCH, Maître-Imprimeur à Mayenne - 28-6-1967 - n° 2829