RÉDACTION N° 158

COTE : NBR 060

TITRE : SPÉCIALISATIONS ET VALUATIONS (ÉTAT 3)

ASSOCIATION DES COLLABORATEURS DE NICOLAS BOURBAKI

NOMBRE DE PAGES : 102

NOMBRE DE FEUILLES : 102

Archives
Janv. 52
M. Weil

NBR 060

2

SPÉCIALISATIONS et VALUATIONS (Etat 3)

Table des matières.

Commentaires :

L'esprit de la rédaction est sensiblement le même que celui de la précédente ; le rédacteur s'était proposé principalement : a) de décanuler les anneaux normaux, précédemment entachés d'une pétition de principe qui n'était même pas "sans importance" ; b) d'étendre la notion de spécialisation, et le théorème fondamental de prolongement, aux anneaux avec diviseurs de zéro ; c) d'augmenter le rôle des "places" dans la théorie des valuations. En ce qui concerne b), il avoue ne pas connaître d'application du théorème de prolongement pour les anneaux avec diviseurs de zéro, sauf celle qui est donnée au § 4 du présent chapitre (il lui avait semblé très choquant, dans la précédente rédaction, que toute la théorie des entiers puisse être faite très simplement, au moyen du théorème de prolongement, dans les anneaux d'intégrité, alors qu'il fallait des méthodes tout à fait différentes pour aboutir exactement aux mêmes résultats dans les anneaux avec diviseurs de 0) ; il est vrai que, comme ce théorème est nouveau, on n'a pas encore eu le temps de lui trouver des applications ; et comme la méthode de démonstration est exactement la même que pour les anneaux d'intégrité (avec une légère complication due à la nécessité de passer au quotient pour former les anneaux de fractions uzkoviens), il semblerait antibourbachique de traîner après soi une hypothèse qui s'est avérée n'avoir aucun rapport avec le théorème à démontrer.

...

Pour arriver à ce résultat, il a été obligé de revenir aux Foundations et définir les spécialisations de familles quelconques d'éléments d'un anneau (plutôt que de "domaines" définis d'une manière assez spéciale) ; cela lève l'objection faite en Congrès, par Sammy et d'autres, qu'on n'arrivait pas à comprendre au juste ce qu'on spécialisait (à présent on spécialise n'importe quoi !). D'autre part, il a obéi aux ordres du Congrès en commencant par un préliminaire sur les anneaux de fractions ; mais la ligne de démarcation exacte à tracer entre ce § et le § des spécialisations est assez floue sur certains points ; le rédacteur s'est assujetti à ne pas parler d'idéaux premiers au § 1 (sinon par prétérition, suivant la formule "Si j'étais un salaud ...") ; si on abandonnait cette règle, la ligne de démarcation en question s'évanouirait complètement.

D'autre part, il s'est laissé entraîner à un enrichissement assez notable du § 3 (valuations) (cf. nos 5, 6, 7, 8) ; il pense n'avoir rien introduit qui ne soit tout à fait à sa place ici ; il s'agit d'ailleurs de notions et résultats d'une grande importance, qu'il recommande à l'approbation de son illustre Maître.

En plus du décanulage des anneaux normaux, on a pu, grâce à la notion de diviseur, y donner un théorème sur ces anneaux qui contient tout l'essentiel des résultats sur les anneaux factoriels et de Dedekind, grâce à quoi la théorie de ceux-ci n'est plus guère qu'un exercice de traduction.

Remarques diverses : 1) Le rédacteur, ne sachant plus très bien à quoi s'en tenir sur ce sujet, a procédé comme si la notion générale d'idéal fractionnaire (principal ou non) était déjà acquise ; si cette assomption (comme disait autrefois Chevalley) n'était pas correcte, il n'y aurait qu'à insérer la définition de ces anneaux quelque part (Où te l'accroches-tu ?). Dans la plus grande partie du chapitre, on ne fait pas la convention qui consiste à écrire AB pour l'idéal engendré par les produits ab d'éléments des idéaux A et B , et AB dénote l'ensemble de ces produits. Cette convention est spécifiquement introduite en son lieu (au 5,n°3) et subsiste pour toute la fin du chapitre. Si la convention a déjà été faite dans Bourbaki, il faudrait une déclaration d'intention sur ce point au début du chapitre.

2) Pour les "places", il y a deux notations possibles, $x \to \varphi(x)$ ou $x \to x(\pi)$, la seconde étant usuelle quand on spécialise un corps de fonctions ; on s'est servi des deux, mais en définitive, dans ce chapitre, la première est de beaucoup la plus utile, et il y aurait peut-être lieu de s'y tenir, en indiquant la seconde en remarque.

3) Le rédacteur s'est autocanulé dans ses notations en écrivant quelquefois $k[(X_\iota)_{\iota \in I}]$ ou $k[(X_\iota)]$ là où il aurait dû écrire $k[X_\iota]_{\iota \in I}$ ou $k[X_\iota]$ (il est vrai que cette dernière notation prête fâcheusement à confusion), et $k((X_\iota)_{\iota \in I}$ ou $k((X_\iota))$ au lieu de $k(X_\iota)_{\iota \in I}$; il s'en excuse humblement.

.....

4) Le rédacteur ne s'excuse pas s'avoir couramment écrit A-B au lieu de l'affreux $C_A(B)$; il lui semble que ce canular a assez duré, et qu'on ne peut raisonnablement se passer de A-B, en dépit de l'argument des groupes abéliens. On n'a qu'à convenir une fois pour toutes que dans ceux-ci on n'écrira jamais A-B pour l'ensemble des a-b, mais A+(-B). Si l'on veut une distinction typographique, ce ne saurait être au moyen d'un signe baroque, mais ce pourrait être, si on veut, par un - gras pour l'opération de théorie des ensembles. Il va de soi que A-B ne doit être écrit que quand A contient B (le croirait-on, mais aux origines de Bourbaki cela a été considéré comme une objection sérieuse contre cette manière d'écrire : c'était une loi de composition non partout définie).

5) Dans la définition des idéaux premiers, il faut choisir si on inclut ou non les spécialisations triviales, c'est-à-dire si (0) est premier ou non dans un anneau d'intégrité ; le rédacteur a adopté le premier parti (il ne sait d'ailleurs auquel des deux s'était rallié son prédécesseur : p.5 de la précédente rédaction, l'exemple 1 est en contra diction avec la définition !) ; dans un cas comme dans l'autre, le risque est très grand d'oublier fréquemment, en cours de rédaction, qu'on a inclus (resp. exclus) l'idéal (0) ; il semble que le premier système soit logiquement plus satisfaisant, et ait pratiquement moins d'inconvénients, que le second.

6) Ayant feuilleté une dernière fois sa rédaction, le rédacteur a l'impression que ses §§1 et 2 (qui, en tout ce qui concerne les anneaux avec diviseurs de zéro, sont essentiellement un état 1) devraient pouvoir être améliorés, et les recommande tout particulièrement à l'attention du Congrès qui les examinera.

7) En vue de la discussion en Congrès, il est recommandé de se munir de la rédaction précédente (et aussi, si possible, des rédactions ultérieures), ainsi que de la Tribu (Congrès du Pelvoux).

SPECIALISATIONS et VALUATIONS.

Dans ce chapitre, on entendra toujours par "anneau" un anneau commutatif avec élément unité ; par "homomorphisme d'anneau" un homomorphisme d'un tel anneau A dans un tel anneau A' qui applique l'élément unité de A sur celui de A'. En conséquence, si (a_ι) est une famille d'éléments d'un anneau A , on dira "le sous-anneau de A engendré par la famille (a_ι)" au lieu de "le sous-anneau de A engendré par la famille (a_ι) et l'élément unité". On notera qu'avec ce langage, si $\mathfrak{a}$ est un idéal d'un anneau A , le quotient $A/\mathfrak{a}$ n'est un anneau, et on n'a le droit de parler de l'homomorphisme canonique de A sur $A/\mathfrak{a}$, que si $\mathfrak{a} \neq A$.

[N.B : Le rédacteur s'est aperçu à ce propos, avec stupéfaction, que la prop.5 du Chap.I, p. 144 est <u>fausse</u> : en effet, suivant les définitions de ce chapitre, un anneau d'intégrité peut être réduit à l'élément 0, tandis que ce n'est pas possible pour un corps].

On notera toujours par A^* le monoide multiplicatif des éléments $\neq 0$ d'un anneau A (cette notation ne sert guère d'ailleurs que dans les anneaux d'intégrité).

§ 1. Anneaux de fractions.

Soient A un anneau, et S une partie non vide de A , stable pour la multiplication, ne contenant pas 0 . La réunion $\mathfrak{U}_S$ des annulateurs des éléments de S (Chap.I, § 8, n°5) est alors un idéal de A , autre que A ; en effet, on a $1 \notin \mathfrak{U}_S$; si $a \in A$, $s \in S$, et $as = 0$, on a $(a_1 a)s = 0$ quel que soit $a_1 \in A$, donc $A\mathfrak{U}_S \subset \mathfrak{U}_S$; et, si $a' \in A$, $s' \in S$, $a's' = 0$, on a $(a+a')ss' = 0$, $ss' \in S$, donc $\mathfrak{U}_S + \mathfrak{U}_S = \mathfrak{U}_S$.

Soit φ l'homomorphisme canonique de A sur $A/\mathfrak{U}_S$; dans l'anneau $\varphi(A) = A/\mathfrak{U}_S$, l'annulateur de tout élément de $\varphi(S)$ est réduit à $\{0\}$; autrement dit, aucun élément de $\varphi(S)$ n'est diviseur de 0 dans $\varphi(A)$, ou encore tous les éléments de $\varphi(S)$ sont réguliers pour la multiplication dans $\varphi(A)$. Soit R l'anneau des fractions de $\varphi(A)$ (Chap.I, § 9, n°4, déf.2) ; dans R , tous les éléments de $\varphi(S)$ sont inversibles.

Soit A_S l'ensemble $\varphi(A)\varphi(S)^{-1}$, c'est-à-dire l'ensemble des éléments de R de la forme $\varphi(a)/\varphi(s)$, avec $a \in A$, $s \in S$; comme $\varphi(a) = \varphi(as)/\varphi(s)$, on a $A_S \supset \varphi(A)$, et on vérifie immédiatement que A_S est un sous-anneau de R , à savoir celui qui est engendré par $\varphi(A)$ et par $\varphi(S)^{-1}$.

Définition 1. Soient A un anneau et S une partie non vide de A, stable pour la multiplication, ne contenant pas 0. L'anneau A_S défini plus haut s'appelle l'anneau de fractions dérivé de A au moyen de S ; l'homomorphisme φ défini plus haut s'appelle l'homomorphisme canonique de A dans A_S.

Remarque.- L'anneau des fractions de A, tel qu'il a été défini au Chap.I, §9, n°4, déf.2, n'est évidemment autre que l'anneau dérivé de A au moyen de l'ensemble de tous les éléments de A qui ne sont pas diviseurs de 0 dans A.

Proposition 1.- Soient A un anneau et S une partie non vide de A, stable pour la multiplication, ne contenant pas 0. Soient A_S l'anneau des fractions dérivé de A au moyen de S, et φ l'homomorphisme canonique de A dans A_S. Alors φ a pour noyau la réunion $\mathfrak{n}_S$ des annulateurs des éléments de S dans A ; tout élément de $\varphi(S)$ est inversible dans A_S ; et on a $A_S = \varphi(A)\varphi(S)^{-1}$. Si aucun élément de S n'est diviseur de 0 dans A, A est un sous-anneau de A_S, et φ est l'isomorphisme identique de A dans A_S ; si tout élément de S est inversible dans A, on a $A_S=A$, et φ est l'isomorphisme identique de A sur A. Si A est anneau d'intégrité, A_S est un anneau d'intégrité, sous-anneau du corps des fractions de A.

Ce sont là des conséquences immédiates de ce qui précède.

Proposition 2.- Soient A un anneau et S une partie non vide de A, stable pour la multiplication, ne contenant pas 0 ; soient A_S l'anneau des fractions dérivé de A au moyen de S, et φ l'homomorphisme canonique de A dans A_S. Soit f un homomorphisme de A dans un anneau B, tel que $0 \notin T = f(S)$; soit ψ l'homomorphisme canonique de B dans l'anneau des fractions B_T dérivé de B au moyen de T. Alors il existe un homomorphisme g et un seul de A_S dans B_T, tel que $g\circ\varphi = \psi\circ f$; on a $g(A_S) = \psi[f(A)]\psi[f(S)]^{-1}$; si $\mathfrak{a}$ est le noyau de f, le noyau $\bar{\mathfrak{a}} = \overset{-1}{\psi}(\mathfrak{a})$ de $f\circ\psi$ est l'ensemble des $a \in A$ tels que $aS \cap \mathfrak{a} \neq \emptyset$, et le noyau de g est $\varphi(\bar{\mathfrak{a}})\varphi(S)^{-1}$.

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "\varphi"'] & B \arrow[d, "\psi"] \\ A_S \arrow[r, "g"'] & B_T \end{tikzcd}$$

Supposons g construit ; alors, si $\varphi(a)/\varphi(s)$ est un élément quelconque de A_S, avec $a \in A$, $s \in S$, on aura $g[\varphi(a)/\varphi(s)] = \psi[f(a)] / \psi[f(x)]$ ce qui montre que g est unique ; réciproquement, il est immédiat que cette formule définit un homomorphisme g de A_S dans B_T. De plus, la relation $g[\varphi(a)/\varphi(s)] = 0$ équivaut à $\psi[f(a)]=0$, donc (puisque le noyau de ψ est la réunion des annulateurs des éléments de $f(S)$ dans B) à l'existence de $s \in S$ tel que $f(a)f(s) = f(as) = 0$ ou encore tel que $as \in \mathfrak{a}$, c'est-à-dire à $aS \cap \mathfrak{a} \neq \emptyset$; l'ensemble de ces éléments est donc bien le noyau $\bar{\mathfrak{a}}$ de $f \circ \psi$, et le noyau de g est $\varphi(\bar{\mathfrak{a}})\varphi(S)^{-1}$.

Remarque.- Si S est l'ensemble des éléments réguliers de A, et si les éléments de $f(S)$ sont inversibles dans B, on retrouve la deuxième partie de la prop.4 du Chap.I, § 9,n°4.

Corollaire 1. *Avec les notations ci-dessus, si f est un isomorphisme de A dans B, g est un isomorphisme de A_S dans B_T.*

En effet, en ce cas, on a $\bar{\mathfrak{a}} = \mathfrak{n}_S$, donc le noyau de g est (0).

En vertu de ce corollaire, *si A est un sous-anneau de B*, et qu'on prenne pour f l'isomorphisme identique, il y a un isomorphisme g, canoniquement défini, de A_S dans B_S au moyen duquel *on peut identifier A_S avec le sous-anneau* $A.S^{-1}$ de B_S ; le plus souvent, on conviendra de faire cette identification.

Corollaire 2.- *A, S, A_S et φ étant comme dans la prop.1, soit $\mathfrak{a}'$ un idéal de A_S ; soit $\mathfrak{a} = \overset{-1}{\varphi}(\mathfrak{a}')$; alors on a $\mathfrak{a}' = \varphi(\mathfrak{a})\varphi(S)^{-1}$; si $a \in A$, $aS \cap \mathfrak{a} \neq \emptyset$ entraîne $a \in \mathfrak{a}$; et ces relations déterminent une correspondance biunivoque entre les idéaux $\mathfrak{a}'$ de A_S, et les idéaux $\mathfrak{a}$ de A tels que $aS \cap \mathfrak{a} \neq \emptyset$ entraîne $a \in \mathfrak{a}$. De plus, si $\mathfrak{a}$ et $\mathfrak{a}'$ se correspondent ainsi et que $\mathfrak{a} \neq A$, et si $T = f(S)$ est l'image de S par l'homomorphisme canonique f de A sur $B = A/\mathfrak{a}$, B est sous-anneau de B_T, et il y a un homomorphisme g de A_S sur B_T, de noyau $\mathfrak{a}'$, tel que $f = g \circ \varphi$; enfin,*

<u>si</u> $A/\mathfrak{a}$ <u>est un anneau d'intégrité, il en est de même de</u> $A_S/\mathfrak{a}'$.

Si $\mathfrak{a}' = A_S$, on a $\mathfrak{a} = A$, et $\mathfrak{a}$, $\mathfrak{a}'$ ont bien les propriétés indiquées. Soit donc $\mathfrak{a}' \neq A_S$; alors $B' = A_S/\mathfrak{a}'$ est un anneau ; soit g l'homorphisme canonique de A_S sur B' ; soit $f = g\circ\varphi$. Les éléments de $\varphi(S)$ étant inversibles dans A_S, ceux de $T = f(S) = g[\varphi(S)]$ le sont dans B' ; d'après la prop.1, on a donc $B'_T = B'$, et l'homomorphisme canonique de B' dans B'_T est l'isomorphisme identique de B' sur B' ; appliquant la prop.2 à A, S, f et B', on voit qu'alors le noyau $\mathfrak{a} = \overset{-1}{\varphi}(\mathfrak{a}')$ de f est identique à l'ensemble $\overline{\mathfrak{a}}$ des $a \in A$ tels que $aS \cap \mathfrak{a} \neq \emptyset$, et que le noyau $\mathfrak{a}'$ de g est $\varphi(\mathfrak{a})\varphi(S)^{-1}$. Soit maintenant $\mathfrak{a}$ un idéal de A autre que A, tel que $aS \cap \mathfrak{a} \neq \emptyset$ entraîne $a \in \mathfrak{a}$; soit f l'homomorphisme canonique de A sur $B = A/\mathfrak{a}$; l'hypothèse faite sur $\mathfrak{a}$ équivaut à dire qu'aucun élément de $T = f(S)$ n'est 0 ni un diviseur de 0 dans B ; d'après la prop.1, B est donc sous-anneau de B_T, et, avec les notations de la prop.2, ψ est l'isomorphisme identique de B dans B_T, et on a $\overline{\mathfrak{a}} = \mathfrak{a}$. Le reste de notre corollaire découle immédiatement de là.

<u>Corollaire 3.</u> <u>Soient</u> A <u>un anneau, et</u> S <u>une partie non vide de</u> A, <u>multiplicativement stable, dont aucun élément n'est</u> 0 <u>ni un diviseur de</u> 0. <u>Alors les relations</u> $\mathfrak{a} = A \cap \mathfrak{a}'$, $\mathfrak{a}' = \mathfrak{a}S^{-1} = \mathfrak{a}A_S$ <u>déterminent une correspondance biunivoque entre les idéaux</u> $\mathfrak{a}'$ <u>de</u> A_S <u>et les idéaux</u> $\mathfrak{a}$ <u>de</u> A <u>tels que</u> $aS \cap \mathfrak{a} \neq \emptyset$ <u>entraîne</u> $a \in \mathfrak{a}$. <u>De plus, si</u> $\mathfrak{a}$ <u>et</u> $\mathfrak{a}'$ <u>se correspondent ainsi et que</u> $\mathfrak{a} \neq A$, <u>et si</u> $T = f(S)$ <u>est l'image de</u> S <u>par l'homomorphisme canonique</u> f <u>de</u> A <u>sur</u> $B = A/\mathfrak{a}$, B <u>est sous-anneau de</u> B_T, <u>et</u> f <u>se prolonge à un homomorphisme de noyau</u> $\mathfrak{a}'$ de A_S <u>sur</u> B_T ; <u>enfin, si</u> $A/\mathfrak{a}$ <u>est anneau d'intégrité, il en est de même de</u> $A_S/\mathfrak{a}'$.

C'est là un cas particulier du coroll.2. On observera que, puisque $\mathfrak{a} = \mathfrak{a}A$, $\mathfrak{a}' = \mathfrak{a}S^{-1}$ entraîne $\mathfrak{a}' = \mathfrak{a}(AS^{-1}) = \mathfrak{a}A_S$.

2. Spécialisations.

1. *Spécialisations finies.*

Définition 1. On appelle spécialisation finie d'un anneau A *tout homomorphisme de* A *sur un anneau d'intégrité.*

Remarque. Cette définition apparaîtra bientôt comme un cas particulier de deux autres qui seront données plus loin (spécialisation finie d'une partie de A , puis plus généralement spécialisation d'une partie de A).

Comme tout anneau d'intégrité peut être considéré comme plongé dans son corps des fractions, et que tout sous-anneau d'un corps est un anneau d'intégrité, la première partie de la déf.1 revient à dire qu'une *spécialisation finie d'un anneau* A *est un homomorphisme de* A *dans un corps*. Quant à la deuxième partie, on voit, par passage au quotient, *que deux spécialisations finies* f, f' *de l'anneau* A *sont équivalentes s'il existe un isomorphisme* g *de* $f(A)$ *sur* $f'(A)$ *tel que* $f' = g \circ f$; en ce cas, il résulte de la prop.4 du chap.I, § 9, n°4, que g *peut, d'une manière et d'une seule, être prolongé à un isomorphisme du corps des fractions de* $f(A)$ *sur celui de* $f'(A)$.

Définition 2. Un idéal $\mathfrak{p}$ *d'un anneau* A *est dit premier si c'est le noyau d'une spécialisation de* A .

Il revient au même de dire que $\mathfrak{p}$ *est premier si* $A/\mathfrak{p}$ *est anneau d'intégrité*, ou encore *si* $\mathfrak{p} \neq A$ *et si* $x \in A$, $y \in A$, $xy \in \mathfrak{p}$ *entraîne* $x \in \mathfrak{p}$ *ou* $y \in \mathfrak{p}$, ou encore *si* $C(\mathfrak{p}) = A - \mathfrak{p}$ *est non vide et stable pour la multiplication*.

Remarque. Il résulte de là qu'on peut, conformément aux définitions du § 1, former l'anneau $A_{C(\mathfrak{p})}$ des fractions dérivé de A au moyen de $C(\mathfrak{p})$; les anneaux de fractions ainsi formés sont particulièrement importants. Il arrive souvent, lorsqu'on a à considérer fréquemment des anneaux de fractions de cette espèce, et qu'on n'a pas à ...

considérer d'autres, qu'on simplifie la notation et le langage en écrivant $A_{\mathfrak{p}}$ au lieu de $A_{C(\mathfrak{p})}$, et en disant que c'est là l'anneau des fractions dérivé de A au moyen de $\mathfrak{p}$; comme $0 \in \mathfrak{p}$, les définitions du § 1 n'attribuent aucun sens à cette dernière expression ni au symbole $A_{\mathfrak{p}}$, de sorte qu'aucune confusion n'est possible.

Exemples. 1) Si A est l'anneau des polynomes à n indéterminées $X_1,\dots,X_n$ sur un corps k, et si $(a)=(a_1,\dots,a_n)$ est une suite de n éléments d'une extension K de k, l'application f qui, à tout polynome $P(X_1,\dots,X_n)\in A$, fait correspondre sa valeur $P(a_1,\dots,a_n)$ est une spécialisation de A dans le corps K.

2) Z étant l'anneau des entiers rationnels, les seuls idéaux premiers de Z autres que (0) sont les idéaux (p), où p est un nombre premier ; l'homomorphisme canonique de Z sur $Z/(p)$ est une spécialisation de Z sur le corps fini à p éléments. Plus généralement, dans un anneau principal A, les idéaux premiers sont (0) et les idéaux de la forme (p), où p est élément extrémal de A.

3) Tout idéal maximal $\mathfrak{m}$ d'un anneau A est premier, car $A/\mathfrak{m}$ est un corps (Chap. I, § 9, n°3, th. 2) ; la réciproque n'est pas vraie, car, dans l'anneau $k[X,Y]$ des polynomes à deux indéterminées X, Y sur un corps k, les idéaux (X) et (Y) sont premiers, et tous deux strictement contenus dans l'idéal maximal (X, Y).

4) Soit $\mathfrak{a}$ l'anneau des applications f d'un ensemble E dans un anneau d'intégrité A, ou bien un sous-anneau de cet anneau (par ex. l'anneau des applications continues d'un espace topologique dans R ou dans C) ; alors, si $x\in E$, l'application $f \to f(x)$ est une spécialisation finie de $\mathfrak{a}$.

5) Soit A l'anneau des séries formelles à n indéterminées sur un corps ; l'application qui, à toute série formelle, fait correspondre son terme constant est une spécialisation de A , dont le noyau est l'idéal maximal de A .

Soit $\mathfrak{a} = (a_\iota)_{\iota \in I}$ une famille d'éléments d'un anneau R ; d'après le th.1 du Chap.IV, § 2,n°1, et la Remarque 1, p.20, du Chap.IV, §2,n°1 , le sous-anneau A de R engendré par les a_ι n'est autre que l'ensemble $Z[\mathfrak{a}]$ des éléments $P(\mathfrak{a})$ quand P décrit l'anneau $Z[X]$ des polynomes sur Z à indéterminées $(X_\iota)_{\iota \in I}$; et A est isomorphe à $Z[X]/\mathfrak{A}$ où $\mathfrak{A}$ est l'idéal des relations algèbriques à coefficients dans Z entre les x_ι , c'est-à-dire l'ensemble des $P \in Z[X]$ tels que $P(\mathfrak{a})=0$.

Proposition 1.- Soit $\mathfrak{a} = (a_\iota)_{\iota \in I}$ une famille d'éléments d'un anneau R ; soit $\alpha = (\alpha_\iota)_{\iota \in I}$ une famille d'éléments d'un corps k , ayant même ensemble d'indices que $\mathfrak{a}$. Pour qu'il existe une spécialisation finie f dans k de l'anneau $Z[\mathfrak{a}]$ engendré par $\mathfrak{a}$ dans R , telle que $f(a_\iota) = \alpha_\iota$ quel que soit ι , il faut et il suffit que α soit un zéro de l'idéal $\mathfrak{A}$ des relations algèbriques à coefficients dans Z entre les α_ι , c'est-à-dire que $P \in Z[X]$, $P(\mathfrak{a})=0$ entraîne $P(\alpha)=0$; et, quand il en est ainsi, f est déterminée d'une manière unique.

En effet, si φ est l'homomorphisme $P \to P(\mathfrak{a})$, de noyau $\mathfrak{A}$, de $Z[X]$ sur $Z[\mathfrak{a}]$, et si f est une spécialisation finie de $Z[\mathfrak{a}]$ dans k , $g = f \circ \varphi$ en est une de $Z[X]$ dans k ; si $f(a_\iota) = \alpha_\iota$, on a $g(X_\iota) = \alpha_\iota$, d'où $g(P) = f[P(\mathfrak{a})] = P(\alpha)$ quel que soit $P \in Z[X]$, et en particulier $0 = P(\alpha)$ pour $P(\mathfrak{a}) = 0$. Réciproquement, si $P(\mathfrak{a})=0$ entraîne $P(\alpha)=0$, et qu'on pose $g(P) = P(\alpha)$ quel que soit $P \in Z[X]$, g est un homomorphisme de $Z[X]$ dans k qui s'annule sur $\mathfrak{A}$, et détermine donc, par passage au quotient, un homomorphisme f de $Z[\mathfrak{a}]$ dans k tel que $g = f \circ \varphi$, donc en particulier $\alpha_\iota = f(a_\iota)$.

On démontre exactement de même la proposition suivante :

Proposition 2.- Soient R un anneau, k un corps, et A un sous-anneau de R qui soit en même temps sous-anneau de k . Soient $\mathfrak{a} = (a_\iota)$, $\alpha = (\alpha_\iota)$ une famille d'éléments de R et une famille d'éléments de k ayant même ensemble d'indices. Pour qu'il existe une spécialisation finie f dans k de l'anneau $A[\mathfrak{a}]$ engendré par A et $\mathfrak{a}$ dans R , telle que $f(a_\iota) = \alpha_\iota$ quel que soit ι et que f induise sur A l'automorphisme identique, il faut et il suffit que α soit un zéro de l'idéal des relations algèbriques à coefficients dans A entre les a_ι , c'est-à-dire que $P \in A[(X_\iota)]$, $P(\mathfrak{a})=0$ entraîne $P(\alpha)=0$; et, quand il en est ainsi, f est déterminée d'une manière unique.

Définition 2.- Soient $\mathfrak{a}=(a_\iota)$, $\alpha = (\alpha_\iota)$ une famille d'éléments d'un anneau R , et une famille d'éléments d'un corps k , ayant même ensemble d'indices. On dira que α est une spécialisation finie de $\mathfrak{a}$ dans k si c'est un zéro de l'idéal des relations algèbriques à coefficients dans Z entre les a_ι , c'est-à-dire si $P \in Z[(X_\iota)]$, $P(\mathfrak{a})=0$ entraîne $P(\alpha)=0$.

On notera que, s'il en est ainsi, $a_\iota = a_\kappa$ entraîne $\alpha_\iota = \alpha_\kappa$, donc que $a_\iota \rightarrow \alpha_\iota$ détermine une application dans k de l'ensemble des éléments de la famille $\mathfrak{a}$.

D'après la prop.1, la déf.2 revient à dire que α est une spécialisation finie de $\mathfrak{a}$ s'il existe une spécialisation finie f d'un sous-anneau de R contenant les a_ι , telle que $f(a_\iota)=\alpha_\iota$, quel que soit ι . En particulier, si $\mathfrak{a}$ est une partie de R (considérée comme famille d'éléments de R au moyen de l'application identique de $\mathfrak{a}$ dans R ; cf. Ens.R , § 2,n°14), une spécialisation finie de $\mathfrak{a}$ dans k est une application de $\mathfrak{a}$ dans k qui peut se prolonger à un homomorphisme de $Z[\mathfrak{a}]$ dans k , ce prolongement étant d'ailleurs unique d'après la prop.1. Si $\mathfrak{a}$ est un sous-anneau de R, on a $\mathfrak{a} = Z[\mathfrak{a}]$, et on retrouve, comme il se doit, le contenu de la déf.1

De ce qui précède (ou bien directement de la déf.2) on déduit immédiatement aussi le résulta-t suivant :

Proposition 3. Soient $\mathfrak{a} = (a_\iota)$, $\alpha = (\alpha_\iota)$ une famille d'éléments d'un anneau R et une famille d'éléments d'un corps k , ayant même ensemble d'indices ; soit f un homomorphisme de R dans un anneau R'. Alors, si α est une spécialisation finie de la famille $f(\mathfrak{a})=(f(a_\iota))$ d'éléments de R', c'est une spécialisation finie de $\mathfrak{a}$.

2. Prolongement des spécialisations finies.

Si X est une partie d'un anneau R , f une spécialisation finie de X , et a un élément de R , il n'est pas toujours possible de prolonger f à une spécialisation finie de $X \cup \{a\}$. Par exemple, cela est impossible si $aa'=1$, $a' \in X$ et $f(a')=0$; en effet, si on pouvait prolonger ainsi f , on aurait $f(1) = f(a)f(a')=0$.

Proposition 4. Soient A un sous-anneau d'un anneau R , f une spécialisation finie de A dans un corps k , et $\mathfrak{p}$ le noyau de f . Soit $x \in R$. Alors, pour qu'il existe une extension K de k , et une spécialisation finie g de $A[x]$ dans K prolongeant f , il faut et il suffit qu'on ait $A \cap x\,\mathfrak{p}[x] \subset \mathfrak{p}$, ou autrement dit que x ne satisfasse à aucune relation de la forme $a = p_1x + p_2x^2 + \dots + p_nx^n$ avec $a \in A - \mathfrak{p}$, $p_i \in \mathfrak{p}$ pour $1 \leqslant i \leqslant n$; et, s'il en est ainsi, on peut prendre pour K la clôture algèbrique de k .

Posons $A'=f(A)$; et soit k' le corps des fractions de A', c'est-à-dir le sous-corps $k'=A'.A'^{-1}_*$ de k , où A'_* désigne l'ensemble des éléments non nuls de A'. D'après la prop.1 du Chap.IV, § 1,n°2, indéterminée ; convenons de noter P' le transformé, par f ainsi étendu, d'un polynome $P \in A[X]$, c'est-à-dire le polynome obtenu en appliquant f aux coefficient de P . Posons, quand g existe, $g(x) = \xi$, d'où, quel que soit $P \in A[X]$, $g(P(x)) = P'(\xi)$; si $\mathfrak{a}$ est l'idéal des relations en x à

à coefficients dans A , c'est-à-dire l'ensemble des $P \in A[X]$ tels que $P(x)=0$; l'application $P \to P(x)$ est un homomorphisme φ, de noyau $\mathfrak{a}$, de $A[X]$ sur $A[x]$, et $g\circ\varphi$ est l'homomorphisme $P \to P'(\xi)$ de $A[X]$ dans K ; on a $P'(\xi)=0$ chaque fois que $P(x)=0$ c'est-à-dire pour tout $P \in \mathfrak{a}$; et réciproquement, si $P(x)=0$ entraîne $P'(\xi)=0$, l'homomorphisme $P \to P'(\xi)$ de $A[X]$ dans K détermine, par passage au quotient, un homomorphisme g de $A[x]$ dans K . Si donc on désigne par $\mathfrak{a}'$ l'ensemble des transformés P' par f des polynomes $P \in \mathfrak{a}$, il faut et il suffit, pour que g existe, que les polynomes $P' \in \mathfrak{a}'$ aient un zéro commun ξ dans K .
Mais $\mathfrak{a}'$ est un idéal de $A'[X]$; et, si on pose $\mathfrak{L} = A'^{-1}_{*}\mathfrak{a}'$, $\mathfrak{L}$ est un idéal de $k'[X]$; en effet, tout polynome de $k'[X]$ peut être mis sous la forme $\alpha^{-1}P'$, avec $P' \in A'[X]$ et $\alpha \in A'_{*}$, d'où on conclut aussitôt que $\mathfrak{L}.k'[X] = \mathfrak{L}$; et de même, si $P' \in \mathfrak{a}'$, $P'_1 \in \mathfrak{a}'$, $\alpha \in A'_{*}$, $\alpha_1 \in A'_{*}$, on a $\alpha^{-1}P' + \alpha_1^{-1}P'_1 = (\alpha\alpha_1)^{-1}(\alpha'_1 P' + \alpha P'_1) \in \mathfrak{L}$. Dans ces conditions, on sait que $\mathfrak{L}$ est un idéal principal (Chap...) ; alors, si $\mathfrak{L} = (0)$, on satisfera aux conditions imposées en prenant $K = k$, $\xi=0$; si $\mathfrak{L} \neq (0)$ et $\mathfrak{L} \neq (1)$, $\mathfrak{L}$ est engendré par un polynome $Q \in k'[X]$ de degré $\geqslant 1$, et on satisfera aux mêmes conditions en prenant pour K la clôture algèbrique de k , et pour ξ un zéro de Q dans K . Enfin, supposons qu'on ait $\mathfrak{L} = (1)$, donc $1 \in \mathfrak{L}$, c'est-à-dire qu'il existe dans $\mathfrak{a}'$ un polynome réduit à un terme constant non nul ; alors celui-ci n'a pas de zéro, et g ne peut exister. Mais, par définition de $\mathfrak{a}'$, il faut et il suffit, pour qu'on soit dans ce cas, que x satisfasse à une relation $\sum_{i=0}^{n} a_i x^i = 0$, avec $f(a_0)\neq 0$, $f(a_i)=0$ pour $1 \leqslant i \leqslant n$, c'est-à-dire $a_0 \in A - \mathfrak{p}$, $a_i \in \mathfrak{p}$ pour $1 \leqslant i \leqslant n$; c'est bien ce qu'il fallait démontrer.

Proposition 5. Soient A un sous-anneau d'un anneau R , f une spécialisation finie de A dans un corps k , et $\mathfrak{p}$ le noyau de f ; soit K la clôture algèbrique de k . Soient $x \in R$, $x' \in R$, tels que $xx' \in A - \mathfrak{p}$;

<u>alors on peut prolonger</u> f <u>à une spécialisation finie, soit de</u> $A[x]$, <u>soit de</u> $A[x']$, <u>dans</u> K .

Supposons qu'il n'en soit pas ainsi ; alors, d'après la prop.3, x satisfera au moins à une relation de la forme $a = p_1x + \ldots + p_nx^n$, avec $a \in A - \mathfrak{p}$, $p_i \in \mathfrak{p}$ pour $1 \leqslant i \leqslant n$; parmi toutes les relations de cette forme auxquelles satisfait x , on peut supposer que celle qu'on vient d'écrire est l'une de celles qui sont de plus petit degré en x . Soit de même $a' = p'_1x' + \ldots + p'_mx'^m$ une relation analogue en x', dont le degré en x' soit le plus petit possible. Supposons par exemple qu'on ait $n \geqslant m$ (sinon on échangerait x et x') ; et posons $b = xx' \in A - \mathfrak{p}$. Multiplions la première relation par a', la seconde par p_nx^n , et ajoutons ; on obtient :

$$aa' = (p_1a'x + \ldots + p_{n-1}a'x^{n-1}) + (p_np'_1bx^{n-1} + \ldots + p_np'_mb^mx^{n-m}) .$$

Mais, $\mathfrak{p}$ étant premier, on a $aa' \in A - \mathfrak{p}$; d'autre part, le second membre est un polynome en x de degré $\leqslant n-1$, dont tous les coefficients sont des éléments de $\mathfrak{p}$; si $n > m$, le second membre est sans terme constant, et l'existence de la relation ainsi obtenue contredit l'hypothèse d'après laquelle x ne satisfait à aucune relation de même forme que $a = p_1x + \ldots + p_nx^n$ et de degré $< n$; si $n = m$, il n'y a qu'à faire passer au premier membre le terme constant $p_np'_mb^m$ du second membre pour obtenir de même une contradiction.

3. <u>Spécialisations dans les corps projectifs.</u>

Comme on a vu au n°2, le prolongement d'une spécialisation finie n'est pas toujours possible ; au contraire, le prolongement sera toujours possible si l'on étend la notion de spécialisation comme suit.

Rappelons (Alg.,Chap.IX) que, si k est un corps, on appelle corps projectif k_∞ la réunion de k et d'un ensemble à un seul élément noté ∞ , auquel on étend (partiellement) comme suit les lois de composition de k .

On pose $\alpha \pm \infty = \infty$ quel que soit $\alpha \in k$; $\alpha/0 = \alpha.\infty = \infty$ quel que soit $\alpha \neq 0$ dans k_∞ ; $\alpha/\infty = 0$ quel que soit $\alpha \in k$. Si K est un corps, et k un sous-corps de K (en particulier le corps premier), on convient d'identifier toujours k_∞ avec le sous-ensemble $k \cup \{\infty\}$ de K_∞ .

<u>Définition 3. Soient</u> $\mathfrak{a} = (a_\iota)_{\iota \in I}$, $\alpha = (\alpha_\iota)_{\iota \in I}$ <u>une famille d'éléments d'un anneau</u> R , <u>et une famille d'éléments d'un corps projectif</u> k_∞ , <u>ayant même ensemble d'indice</u> I ; <u>soit</u> L <u>l'ensemble des</u> $\lambda \in I$ <u>tels que</u> $\alpha_\lambda = \infty$; <u>soit</u> $\beta_\iota = \alpha_\iota$ <u>pour</u> $\iota \in C(L)$, $\beta_\lambda = \alpha_\lambda^{-1} = 0$ <u>pour</u> $\lambda \in L$. <u>On dira que</u> α <u>est une spécialisation de</u> $\mathfrak{a}$ <u>dans</u> k_∞ <u>s'il existe un homomorphisme</u> f <u>de</u> R <u>dans un anneau</u> R' <u>tel que</u> $f(a_\lambda)$ <u>soit inversible dans</u> R' <u>quel que soit</u> $\lambda \in L$, <u>et qu'en posant</u> $b_\iota = f(a_\iota)$ <u>pour</u> $\iota \in C(L)$, $b_\lambda = f(a_\lambda)^{-1}$ <u>pour</u> $\lambda \in L$, $\beta = (\beta_\iota)_{\iota \in I}$ <u>soit une spécialisation finie de</u> $\mathfrak{b} = (b_\iota)_{\iota \in I}$.

D'après la prop.3 du n°1, si L est vide, on retombe sur la notion de spécialisation finie ; autrement dit, une spécialisation finie est une spécialisation dont aucun élément n'est ∞ . Il est clair aussi que, si $\mathfrak{a} = (a_\iota)_{\iota \in I}$ est une famille d'éléments de l'anneau R , et si g est un homomorphisme de R dans un anneau R_1 , toute spécialisation de la famille $g(\mathfrak{a}) = (g(a_\iota))_{\iota \in I}$ est une spécialisation de $\mathfrak{a}$.

Comme dans le cas des spécialisations finies, il est immédiat qu'avec les hypothèses et notations de la déf.3, $a_\iota = a_k$ entraîne $\alpha_\iota = \alpha_k$; donc $a_\iota \rightarrow \alpha_\iota$ détermine une application dans k_∞ de l'ensemble des éléments de la famille $\mathfrak{a}$; il n'y a donc pas de distrinction substantielle à établir entre spécialisations d'une famille d'éléments de R et spécialisations d'une partie de R . Enfin, si $\alpha = (\alpha_\iota)_{\iota \in I}$ est comme ci-dessus une spécialisation de $\mathfrak{a} = (a_\iota)_{\iota \in I}$, et si J est une partie de I , $(\alpha_\iota)_{\iota \in J}$ est une spécialisation de la famille partielle $(a_\iota)_{\iota \in J}$;

il revient au même de dire que toute spécialisation d'une partie X d'un anneau R induit, sur toute partie X' de X , une spécialisation de celle-ci.

Supposons que α soit une spécialisation de $\mathfrak{a}$ dans k_∞ , les notations restant celles de la déf.3 ; soit S la plus petite partie de R , stable pour la multiplication, contenant 1 et les a_λ pour $\lambda \in L$, c'est-à-dire l'ensemble des monomes $M((a_\lambda)_{\lambda\in L})$ de degré $\geqslant 0$ dans les a_λ ; tous les éléments de $f(S)$ devant être inversibles dans R', S ne contient pas 0 . Comme au § 1, soit R_S l'anneau des fractions dérivé de R au moyen de S ; soit φ l'homorphisme canonique de R dans R_S ; d'après la prop.2 du § 1, il existe un homomorphisme g et un seul de R_S dans R' tel que $f = g\circ\varphi$. Posons $b'_\iota = a'_\iota = \varphi(a_\iota)$ pour $\iota \notin L$,$a'_\lambda = \varphi(a_\lambda)$ et $b'_\lambda = a'^{-1}_\lambda$ pour $\lambda \in L$, d'où $b_\iota = g(b'_\iota)$ quel que soit ι ; il s'ensuit (prop.3,n°1) que β <u>est une spécialisation finie de</u> $b' = (b'_\iota)_{\iota\in I}$: c'est donc là une condition nécessaire et suffisante pour que α soit une spécialisation de $\mathfrak{a}$. Appliquons la déf.2 ; soit $P = P((Y_\iota)_{\iota\in I}) = P((Y_\iota)_{\iota\in C(L)}, (Y_\lambda)_{\lambda\in L})$ un polynome de l'idéal des relations entre les b'_ι à coefficients dans Z ; on devra avoir $0 = P((\beta_\iota)_{\iota\in I}) = P((\alpha_\iota)_{\iota\in C(L)}, (0)_{\lambda\in L})$. Mais, si P est un polynome quelconque de $Z((Y_\iota)_{\iota\in I})$, on a, d'après la définition de R_S :

$$P((b'_\iota)_{\iota\in I}) = Q((a'_\iota)_{\iota\in I})/M((a'_\lambda)_{\lambda\in L})$$
$$= \varphi\left[Q((a_\iota)_{\iota\in I})\right]/\varphi\left[M((a_\lambda)_{\lambda\in L})\right] ,$$

où $M((X_\lambda)_{\lambda\in L})$ est un monome et $Q((X_\iota)_{\iota\in I})$ un polynome de $Z[(X_\iota)_{\iota\in I}]$ tels que l'on ait :

$$Q((X_\iota)_{\iota\in C(L)}, (X_\lambda)_{\lambda\in L}) = M((X_\lambda)_{\lambda\in L}) P((X_\iota)_{\iota\in C(L)}, (X_\lambda^{-1})_{\lambda\in L}) .$$

Pour que $P((b'_\iota)_{\iota\in I})$ s'annule, il faut et il suffit, avec ces notations, que $Q((a_\iota)_{\iota\in I})$ soit dans le noyau de φ , donc (Prop.1 du § 1) dans l'annulateur d'un monome $M_0((a_\lambda)_{\lambda\in L})$, donc, en posant $Q_1 = M_0 Q$, que

que l'on ait $Q_1((a_\iota)_{\iota\in I})=0$. Remplaçant M , Q par $M_1=M_0M$ et Q_1 , on obtient ainsi le résultat suivant :

Proposition 6. $\mathfrak{a}$, α, I, L étant comme dans la déf.3, soit $\mathcal{A}$ l'ensemble des polynomes $P\in Z[(Y_\iota)_{\iota\in I}]$ ayant la propriété suivante : il existe un monôme $M((X_\lambda)_{\lambda\in L})$ tel que $Q = M((X_\lambda)_{\lambda\in L})P((X_\iota)_{\iota\in C(L)}, (X_\lambda^{-1})_{\lambda\in L})$ soit un polynome dans les X_ι et que $Q((a_\iota)_{\iota\in I})=0$. Alors une condition nécessaire et suffisante pour que α soit une spécialisation de $\mathfrak{a}$ est que l'on ait $0 = P((\beta_\iota)_{\iota\in I}) = P((\alpha_\iota)_{\iota\in C(L)},(0)_{\lambda\in L})$ quel que soit $P\in\mathcal{A}$.

Proposition 7.- Soit f une spécialisation, dans un corps projectif k_∞, d'une partie X d'un anneau R . Alors chacune des relations

$$f(x\pm y) = f(x)\pm f(y)\ ,\quad f(xy) = f(x)f(y),\quad f(x/y) = f(x)/f(y)$$

est satisfaite chaque fois que les deux membres sont définis.

Considérons par exemple la première de ces relations, $f(x+y) = f(x)+f(y)$; notre proposition signifie que cette relation est satisfaite chaque fois que $x\in X$, $y\in X$, $x+y\in X$, et que $f(x)$, $f(y)$ ne sont pas tous deux ∞ . Il en est ainsi, d'après la définition des spécialisations finies, si $f(x)$, $f(y)$, $f(x+y)$ sont tous trois finis ; en examinant les divers cas possibles, on voit que tout revient à démontrer que, s'ils ne sont pas tous trois finis, deux d'entre eux au moins sont ∞ . Supposons donc qu'un seul d'entre eux, par exemple $f(x)$, soit ∞ ; appliquant la déf.3, on se ramène immédiatement au cas où x est inversible dans R ; posons $x'=x^{-1}$, $z=x+y$; alors, par hypothèse, $(0,f(y), f(x+y))$ est une spécialisation finie de (x',y,z) ; mais on a $x'(z-y)=1$,d'où contradiction. Les autres cas, et les autres relations, se traitent de même.

4. **Prolongement des spécialisations.**

Proposition 8. *Soit f une spécialisation finie, dans un corps k, d'un sous-anneau A d'un anneau R. Soit X l'ensemble des éléments x de R qui satisfont à une relation de la forme $ax = b$, où $a \in A$, $b \in A$, et $f(a) \neq 0$ ou $f(b) \neq 0$. Alors f peut être prolongée, d'une manière et d'une seule, à une spécialisation de X dans k_∞.*

L'unicité résulte immédiatement de la prop.7 ; si f' est un tel prolongement, une relation de la forme $ax = b$ entraîne $f(a)f'(x) = f(b)$, ce qui détermine $f'(x)$; on voit que $f'(x)$ est fini sauf si $f(a)=0$, $f(b)\neq 0$. Si $s \in R$ satisfait à deux relations de cette forme, $ax = b$ et $a'x = b'$, on a $x(ab'-a'b)=0$, puis, en multipliant cette dernière relation par a, $b(ab'-a'b)=0$, et de même $b'(ab'-a'b)=0$, d'où $f(b)f(ab-a'b)=0$ et $f(b')f(ab'-a'b)=0$; ou bien donc on a $f(b)=f(b')=0$, ou on a $f(ab'-a'b)=0$ c'est-à-dire $f(a)f(b')=f(a')f(b)$, donc en tout cas, en vertu des hypothèses faites, $f(b)/f(a)= f(b')/f(a')$; si donc on pose $f'(x) = f(b)/f(a)$, f' est une application de X dans k_∞. Soit A' l'ensemble des $x \in X$ tels que $f'(x) \neq \infty$, c'est-à-dire des $x \in R$ satisfaisant à une relation $ax = b$ avec $a \in A$, $b \in A$, $f(a)\neq 0$; si x' est un autre élément de A', satisfaisant à une relation analogue $a'x'=b'x$, on a $(aa')(xx') = bb'$, $(aa')(x+x')=a'b+ab'$, donc A' est un anneau, qui contient évidemment A ; il est immédiat alors que f' induit sur A' un homomorphisme de A' dans k. Soit maintenant S le complémentaire de A' dans X, c'est-à-dire l'ensemble des $s \in R$ satisfaisant à une relation $as = b$ avec $a \in A$, $b \in A$, $f(a)=0$, $f(b)\neq 0$; si S est vide, il ne nous reste rien à démontrer. Sinon, S est multiplicativement stable et ne contient pas 0. Soit x un élément de l'annulateur de $s \in S$; on a $as=b$ avec $a \in A$, $b \in A$, $f(a)=0$, $f(b)\neq 0$, et $sx = 0$, donc $0 = asx = bx$, donc $x \in A'$ et $f'(x)=0$; par suite, la réunion $\mathcal{U}_S$ des annulateurs des éléments de S est contenue dans le noyau de f'. Par passage au quotient,

f' détermine donc un homomorphisme f'' dans k de l'image $\varphi(A')$ de A' par l'homomorphisme canonique φ de R dans l'anneau des fractions R_S dérivé de R au moyen de S, et notre proposition sera démontrée si nous faisons voir que f'' se prolonge en une spécialisation de $\varphi(A') \cup \varphi(S)$ prenant la valeur sur $\varphi(S)$. En remplacant R, A, S, f par R_S, $\varphi(A')$, $\varphi(S)$, f'', on est donc ramené à démontrer ce qui suit : si f est un homomorphisme dans k d'un sous-anneau A d'un anneau R, et si S est une partie de R telle que tout $s \in S$ soit inversible dans R et satisfasse à une relation $as = b$ avec $a \in A$, $b \in A$, $f(a)=0$, $f(b) \neq 0$, alors l'application de $A \cup S$ dans k_∞ qui coïncide avec f sur A et prend la valeur sur S est une spécialisation de A S. Mais, d'après ce qui précède, on peut étendre f à un homomorphisme dans k de l'ensemble A' des $x \in R$ tels que $ax = b$, $a \in A$, $b \in A$, $f(a) \neq 0$, $f(b)=0$; il est clair d'ailleurs que S^{-1} est contenu dans A', et plus précisément dans le noyau de cet homomorphisme. D'après la déf.3, cela achève la démonstration.

<u>Proposition 9</u>.- <u>Soit</u> f <u>une spécialisation d'une partie</u> X <u>d'un anneau</u> R <u>dans un corps projectif</u> k_∞ ; <u>soit</u> K <u>la clôture algèbrique de</u> k. <u>Alors, quel que soit</u> $x \in R$, f <u>peut se prolonger à une spécialisation de</u> $X \cup \{x\}$ <u>dans</u> K_∞.

Soit $Z = \overset{-1}{f}(\infty)$ la partie de X sur laquelle f prend la valeur ∞, et $Y = \overset{-1}{f}(k)$ son complémentaire dans X. En vertu de la déf.3, il y a un homomorphisme g de R dans un anneau R', tel que tous les éléments de $g(Z)$ soient inversibles dans R', et une spécialisation finie f' de la partie $X' = g(Y) \cup g(Z)^{-1}$ de R', prenant la valeur 0 sur $g(Z)^{-1}$ et telle que f coïncide avec $f' \circ g$ sur Y. Il suffit, dans ces conditions, de montrer que f' peut être prolongée à une spécialisation (finie ou non f'' de $X' \cup \{g(x)\}$; s'il en est ainsi, en effet, la fonction égale à f'' sur ce dernier ensemble, et à ∞ sur $g(Z)$, est une spécialisation de

$X' \cup \{g(x)\} \cup g(Z) = g(X \cup \{x\}) \cup g(Z)^{-1}$, et induit sur $g(X \cup \{x\})$ une spécialisation de ce dernier ensemble qui, composée avec g, donne bien le prolongement cherché pour f. Remplaçant alors X, x, f par X', f', $g(x)$, on voit qu'on est ramené au cas où f est une spécialisation finie de X dans k. Par définition des spécialisations finies, f peut alors se prolonger en tout cas au sous-anneau engendré par X dans R ; tout revient donc à démontrer que, si A est un sous-anneau de R, et si $x \in R$, toute spécialisation finie f de A dans k peut être prolongée à une spécialisation finie ou non de $A \cup \{x\}$ dans K_∞. Appliquant la prop.4 du n°2, on voit que tout revient à démontrer ce qui suit : soient f un homomorphisme de A dans k, $\mathfrak{P}$ son noyau, x un élément de R satisfaisant à une relation de la forme $a = p_1x + \dots + p_nx^n$, avec $a \in A - \mathfrak{P}$, $p_i \in \mathfrak{P}$ pour $1 \leqslant i \leqslant n$; alors f peut être prolongée à une spécialisation (nécessairement non finie) de $A \cup \{x\}$ dans k_∞. Posons en effet $x' = p_1 + \dots + p_nx^{n-1}$, d'où $xx' = a$; d'après les prop.4 et 5, f se prolonge à une spécialisation finie f' de $A' = A[x']$; et, d'après la prop.8, f' se prolonge à une spécialisation de l'ensemble de tous les éléments u de R satisfaisant à une relation $a'u = b'$, avec $a' \in A'$, $b' \in A'$, $f'(a') \neq 0$ ou $f'(b') \neq 0$; comme on a $x' \in A'$, $a \in A'$, $f'(a) = f(a) \neq 0$, x appartient à cet ensemble, ce qui achève la démonstration.

<u>Définition 4</u>. <u>Soient</u> R <u>un anneau</u>, k_∞ <u>un corps projectif</u> ; <u>on appelle place de</u> R, <u>à valeurs dans</u> k_∞, <u>toute spécialisation de</u> R <u>dans</u> k_∞ ; <u>si</u> π <u>est une telle place, l'image</u> $x(\pi)$, <u>par</u> π, <u>de</u> $x \in R$ <u>dans</u> k_∞ <u>s'appellera la valeur de</u> x <u>en</u> π.

Ce langage et cette notation sont suggérés par des exemples tels que les suivants :

Exemples.- 1) Soit $k(X)$ le corps des fractions rationnelles à une indéterminée X sur un corps k ; c'est le corps des fractions de l'anneau $k[X]$ des polynomes en X sur k. Soit ξ un élément d'une extension K de k ; comme on a vu (n°1, ex.1), l'application $P \rightarrow P(\xi)$ est une spécialisation finie de $k[X]$ dans K. Mais tout $R \in k(X)$ peut être mis sous la forme $R = P/Q$, où P, Q sont premiers entre eux dans $k[X]$ et par conséquent $P(\xi) \neq 0$ ou $Q(\xi) \neq 0$; il résulte alors de la prop.8 qu'en posant dans ces conditions $R(\xi) = P(\xi)/Q(\xi)$, on définit une place $R \rightarrow R(\xi)$ du corps $k(X)$, à valeurs dans K_∞.

2)* Soient D un domaine (ensemble ouvert connexe) du plan de la variable complexe, a un point de D, M le corps des fonctions méromorphes dans D ; $f \rightarrow f(a)$ est une place de M à valeurs dans C_∞.*

Théorème 1. Soient R un anneau, K un corps algèbriquement clos ; toute spécialisation d'une partie X de R, à valeurs dans K_∞, peut être prolongée à une place de R à valeurs dans K_∞.

Ordonnons en effet les spécialisations de parties de R dans K_∞ par la relation "f prolonge f'" ; il est immédiat qu'elles forment un ensemble inductif ; donc, en vertu du th. de Zorn, toute spécialisation admet un prolongement maximal. Mais, d'après la prop.9, une spécialisation maximale à valeurs dans K_∞ est nécessairement définie sur R tout entier ; autrement dit, c'est une place de R.

5. Spécialisations des anneaux d'intégrité. Comme on est convenu de considérer une fois pour toutes tout anneau d'intégrité comme plongé dans son corps des fractions, il n'y a pas de distinction à établir entre spécialisations d'une famille d'éléments d'un anneau d'intégrité et spécialisations d'une famille d'éléments d'un corps. Nous étendrons comme suit la notion de spécialisation aux parties et familles d'éléments des corps projectifs :

Définition 5. Soient $\mathfrak{a} = (a_\iota)_{\iota\in I}$, $\alpha = (\alpha_\iota)_{\iota\in I}$ deux familles d'éléments ayant même ensemble d'indices, appartenant respectivement à deux corps projectifs K_∞ , k_∞ ; soit J l'ensemble des $\iota \in I$ tels que $a_\iota \neq \infty$. On dira que α est une spécialisation de $\mathfrak{a}$ si $(\alpha_\iota)_{\iota\in J}$ est une spécialisation de $(a_\iota)_{\iota\in J}$ et si $\alpha_\iota = \infty$ pour tout $\iota \in C(J)$.

Autrement dit, une application f d'une partie X d'un corps projectif K_∞ dans un corps projectif k_∞ est une spécialisation si elle induit une spécialisation sur l'ensemble des éléments de X autres que ∞ , et si $f(\infty) = \infty$ pour $\infty \in X$. Dans ces conditions, le contenu de la prop.7 subsiste :

Proposition 10.- Soit f une spécialisation d'une partie d'un corps projectif K_∞ dans un corps projectif k_∞ . Alors chacune des relations

$$f(x\pm y) = f(x) \pm f(y) \ , \quad f(xy) = f(x)f(y) \ , \quad f(x/y) = f(x)/f(y)$$

est satisfaite chaque fois que les deux membres sont définis.

Soient $\mathfrak{a} = (a_\iota)_{\iota\in I}$, $\alpha = (\alpha_\iota)_{\iota\in I}$ deux familles d'éléments, ayant même ensemble d'indices, appartenant respectivement à deux corps projectifs K_∞ , k_∞ ; soit L l'ensemble des $\lambda \in I$ tels que $\alpha_\lambda = \infty$. Tenant compte des déf.2 (n°1), 3 (n°3) et des remarques qui suivent celle-ci, on voit que α sera une spécialisation de $\mathfrak{a}$ s'il existe un homomorphisme f dans k du sous-anneau de K engendré par les a_ι pour $\iota \in C(L)$ et par les a_λ^{-1} pour $\lambda \in L$, tel que $f(a_\iota)=\alpha_\iota$ pour $\iota \in C(L)$ et $f(a_\lambda^{-1}) = \alpha_\lambda^{-1} = 0$ pour $\lambda \in L$. Supposons maintenant que les familles $\mathfrak{a}$, α soient spécialisations l'une de l'autre ; alors, non seulement $a_\iota = \infty$ entraîne $\alpha_\iota = \infty$, mais $\alpha_\iota = \infty$ entraîne $a_\iota = \infty$; L est donc aussi l'ensemble des K tels que $a_K = \infty$; et il existe un homomorphisme g dans K de l'anneau engendré par les α_ι pour $\iota \in C(L)$, tel que $g(\alpha_\iota)=a_\iota$, pour tout $\iota \in C(L)$. Il s'ensuit que $g\circ f$ et $f\circ g$ sont les automorphismes identiques des sous-anneaux de K et de k engendrés par les a_ι et par les α_ι , respectivement, pour $\iota \in C(L)$, donc que f, g sont deux isomorphismes, réciproques l'un de l'autre, de ces anneaux l'un sur l'autre. Comme ces isomorphismes peuvent alors être étendus aux corps des fractions K', k' de ces anneaux, puis aux corps projectifs K'_∞ , k'_∞ , on en conclut :

Proposition 11. Soient $(a_\iota)_{\iota \in I}$, $(\alpha_\iota)_{\iota \in I}$ deux familles d'éléments, ayant même ensemble d'indices, de deux corps projectifs K_∞ , k_∞ . Pour que ces familles soient spécialisations l'une de l'autre, il faut et il suffit qu'il y ait un sous-corps projectif K'_∞ de K_∞ , et un isomorphisme f de K'_∞ sur un sous-corps projectif k'_∞ de k_∞ , tels que $a_\iota \in K'_\infty$ et $f(a_\iota)=\alpha_\iota$ quel que soit $\iota \in I$.

Définition 6. Si deux familles d'éléments $(a_\iota)_{\iota \in I}$, $(\alpha_\iota)_{\iota \in I}$ de deux corps projectifs K_∞ , k_∞ , ayant même ensemble d'indices, sont spécialisations l'une de l'autre, elles sont dites spécialisations génériques l'une de l'autre.

D'après la prop.11, il est clair que toute spécialisation générique d'une famille d'éléments $\mathfrak{a}$ d'un anneau ou bien d'un corps projectif est encore une spécialisation de $\mathfrak{a}$.

Définition 7. Deux spécialisations α , α' d'une famille $\mathfrak{a}$ d'éléments d'un anneau ou bien d'un corps projectif seront dites équivalentes si elles sont spécialisations génériques l'une de l'autre.

En particulier, deux spécialisations finies f , f' d'un anneau A seront équivalentes s'il existe un isomorphisme g de $f(A)$ sur $f'(A)$ tel que $f'=g\circ f$; pour qu'il en soit ainsi, il faut et il suffit, comme on sait, qu'elles aient même noyau.

Plus généralement, on a le principe suivant, dit de "transitivité des spécialisations " :

<u>Théorème 2. Toute spécialisation d'une spécialisation d'une famille $\mathfrak{a}$ d'éléments d'un anneau R est une spécialisation de $\mathfrak{a}$</u>.

Soit α une spécialisation de $\mathfrak{a} = (a_\iota)_{\iota \in I}$ dans un corps projectif k_∞ ; définissons L, f, R', $\mathfrak{b}$, β comme dans la déf.3 . Soit α' une spécialisation de α dans un corps projectif k'_∞ ; posons $\beta'_\iota = \alpha'_\iota$ pour $\iota \in C(L)$, $\beta'_\lambda = \alpha'^{-1}_\lambda$ pour $\lambda \in L$; comme $\alpha_\lambda = \infty$ entraîne $\alpha'_\lambda = \infty$, on a $\beta'_\lambda = 0$ pour $\lambda \in L$. Dans ces conditions, $\beta' = (\beta'_\iota)_{\iota \in I}$ est une spécialisation de β ; comme β est une spécialisation finie de $\mathfrak{b}$, il résulte de la prop.6 du n°3 , et de la déf.2 du n°1, que β' est une spécialisation de $\mathfrak{b}$; si donc M désigne l'ensemble des $\mu \in I$ tels que $\beta'_\mu = \infty$, il y a un homomorphisme g de R' dans un anneau R'' tel que $g(b_\mu)$ soit inversible dans R'' quel que soit $\mu \in M$ et qu'en posant $c_\iota = g(b_\iota)$ et $\gamma'_\iota = \beta'_\iota$ pour $\iota \in C(M)$, $c_\mu = g(b_\mu)^{-1}$ et $\gamma'_\mu = 0$ pour $\mu \in M$, γ' soit une spécialisation finie de $c = (c_\iota)_{\iota \in I}$. Mais dans ces conditions $L \cup M$ est l'ensemble des ι tels que $\alpha'_\iota = \infty$, et on a $\gamma'_\iota = \alpha'_\iota$ pour $\iota \in C(L \cup M)$, $\gamma'_\iota = 0$ pour $\iota \in L \cup M$; $h = g \circ f$ est un homomorphisme de R dans R'', et on a $c_\iota = h(a_\iota)$ pour $\iota \in C(L \cup M)$, $c_\iota = h(a_\iota)^{-1}$ pour $\iota \in L \cup M$. D'après la déf.3 du n°3, cela démontre le théorème.

Lorsqu'il s'agit d'une famille d'éléments d'un corps, la définition d'une spécialisation donnée précédemment peut êtr présentée d'une manière plus simple, en raison du fait que tout élément d'un corps est inversible. En combinant les déf.2 (n°1), (n°3) et 5 , et les remarques qui suivent la déf.3, on obtient le résultat suivant :

Proposition 12. *Soient* $\mathfrak{a} = (a_\iota)_{\iota \in I}$, $\alpha = (\alpha_\iota)_{\iota \in I}$ *deux familles d'éléments, ayant même ensemble d'indices, de deux corps projectifs* K_∞ , k_∞ ; *soit* L *l'ensemble des* $\lambda \in I$ *tels que* $\alpha_\lambda = \infty$. *Alors, pour que* α *soit une spécialisation de* $\mathfrak{a}$, *il faut et il suffit que* $a_\iota \neq \infty$ *pour* $\iota \in C(L)$, $a_\lambda^{-1} \neq \infty$ pour $\lambda \in L$, *et qu'il y ait un homomorphisme* f *dans* k *du sous-anneau de* K *engendré par les* a_ι *pour* $\iota \in C(L)$ *et par les* a_λ^{-1} *pour* $\lambda \in L$, *tel que* $f(a_\iota)=\alpha_\iota$ *pour* $\iota \in C(L)$ *et* $f(a_\lambda^{-1}) = \alpha_\lambda^{-1} = 0$ *pour* $\lambda \in L$.

Par suite, se donner une spécialisation d'une famille d'éléments d'un corps projectif K_∞ revient à se donner une spécialisation finie d'un sous-anneau de K , donc d'un anneau d'intégrité. Nous allons maintenant appliquer la prop.8 du n°4 aux spécialisations de cette sorte.

Définition 8. *Soit* f *un homomorphisme d'un anneau d'intégrité* A *dans un corps* k ; *soit* K *le corps des fractions de* A . *Alors l'ensemble* D *des* $x \in K_\infty$ *de la forme* $x = b/a$ *avec* $a \in A$, $b \in A$, *et* $f(a) \neq 0$ ou $f(b) \neq 0$, *s'appellera le domaine de la spécialisation finie* f *de* A ; *l'application* $b/a \to f'(b/a) = f(b)/f(a)$ *de* D *dans* k_∞ *s'appellera le prolongement canonique de* f .

Il résulte de la prop.8 que ce prolongement est bien défini sur l'ensemble des éléments de D autres que ∞ , et que c'est une spécialisation de cet ensemble ; et, pour $b/a = \infty$, on a nécessairement $a = 0$, donc $f(a)=0$, $f(b) \neq 0$, de sorte que $f'(\infty)$ est bien défini et a la valeur ∞ ; f' est donc une spécialisation de D .

Soit $\mathfrak{p} = \overset{-1}{f}(0)$ le noyau de f ; soit A' l'ensemble des $x \in D$ tels que $f'(x) \neq \infty$, c'est-à-dire l'ensemble des $x \in K$ de la forme $x = b/a$ avec $a \in A - \mathfrak{p}$, $b \in A$; alors, d'après la déf.1 du § 1, A' est l'anneau des fractions dérivé de A au moyen de l'ensemble (non vide, multiplicativement stable) $A - \mathfrak{p}$; conformément à la remarque qui suit la déf.2 du n°1, nous noterons désormais cet anneau par $A_{\mathfrak{p}}$. Dans ces conditions, f' induit sur $A'=A_{\mathfrak{p}}$ un homomorphisme de cet anneau dans k , qui n'est autre évidemment que celui dont l'existence résulte de la prop.2 du § 1, appliquée à A, f, $S = A-\mathfrak{p}$, $A_S = A'$, $B = B_T = k$, φ étant l'isomorphisme identique de A dans A' et ψ celui de k sur k ; alors f' induit g sur A' ; il s'ensuit que le noyau $\mathfrak{p}' = \overset{-1}{f'}(0)$ de f' est donné par $\mathfrak{p}' = \mathfrak{p}S^{-1} = \mathfrak{p}A_{\mathfrak{p}}$. Comme d'ailleurs f' induit f sur A , on a $\mathfrak{p} = A \cap \mathfrak{p}'$. Enfin, si $x \in D$, on a $x^{-1} \in D$, et $f'(x^{-1}) = f'(x)^{-1}$; en particulier, $A'-\mathfrak{p}'$ est l'ensemble des éléments inversibles de A', d'où résulte que $A'_{\mathfrak{p}'} = A'$; et $D-A' = \mathfrak{p}'^{-1}$, d'où $D = A' \cup \mathfrak{p}'^{-1} = A' \cup A'^{-1}$. Il s'ensuit que le domaine de la spécialisation finie induite ~~xxxxx~~ par f' sur A' est D , et que son prolongement canonique est f'.

Avec les notations ci-dessus, pour qu'on ait $A'=A$, c'est-à-dire $A_{\mathfrak{p}} = A$, il faut et il suffit que tout élément de $A-\mathfrak{p}$ soit inversible dans A ; comme d'ailleurs aucun élément de $\mathfrak{p}$ ne peut être inversible dans A (sinon on aurait $\mathfrak{p} = A$), $\mathfrak{p}$ est l'ensemble des éléments non inversibles de A . Comme un idéal de A ne peut contenir d'élément inversible s'il est $\neq A$, tout idéal de A autre que A est alors contenu dans $\mathfrak{p}$, et $\mathfrak{p}$ est idéal maximal dans A (Chap.I, § 8, n°7, déf.7) et est l'unique idéal maximal de A ; $A/\mathfrak{p}$ est alors un corps (Chap.I, § 9, n°3, th.2).

<u>Définition 9</u>.- <u>On dit qu'un anneau</u> A (commutatif, avec élément unité) <u>est un anneau local si l'ensemble</u> $\mathfrak{p}$ <u>des éléments non inversibles de</u> A <u>est un idéal de</u> A ; $\mathfrak{p}$ <u>est alors l'idéal maximal de</u> A , <u>et</u> $A/\mathfrak{p}$ <u>s'appellera le corps des restes de</u> A .

<u>Remarque</u>.- Certains auteurs modernes réservent le nom "d'anneau local" aux anneaux <u>noethériens</u> qui satisfont à la déf.9 .

Définition 10.- Soient f une spécialisation finie d'un anneau d'intégrité A, $\mathfrak{p} = \overset{-1}{f}(0)$ son noyau, K le corps des fractions de A. Alors l'anneau $A_{\mathfrak{p}}$ est appelé l'anneau local de la spécialisation f, et son idéal maximal $\mathfrak{p}A_{\mathfrak{p}}$ est appelé l'idéal de spécialisation de f.

Nous pouvons alors résumer et complèter comme suit les résultats obtenus.

Théorème 3. Soient f un homomorphisme d'un anneau d'intégrité A dans un corps k, $\mathfrak{p} = \overset{-1}{f}(0)$ le noyau de f, K le corps des fractions de A. Alors f peut, d'une manière unique, être prolongée à un homomorphisme g dans k de l'anneau local $A_{\mathfrak{p}}$ de f, c'est-à-dire de l'anneau des fractions dérivé de A au moyen de $A-\mathfrak{p}$; le noyau de g est $\mathfrak{p}A_{\mathfrak{p}}$; c'est l'unique idéal maximal de $A_{\mathfrak{p}}$, et on a $\mathfrak{p} = A \cap (\mathfrak{p}A_{\mathfrak{p}})$. Le domaine D de f est $D = A_{\mathfrak{p}} \cup A_{\mathfrak{p}}^{-1}$; le prolongement canonique de f est l'application de D dans k_∞ égale à g sur $A_{\mathfrak{p}}$ et à ∞ sur $D-A_{\mathfrak{p}} = (\mathfrak{p}A_{\mathfrak{p}})^{-1}$. L'image $g(A_{\mathfrak{p}})$ de $A_{\mathfrak{p}}$ par g est le corps des fractions de l'image $f(A)$ de A par f dans k. Enfin, les relations $\mathfrak{q} = A \cap \mathfrak{q}'$, $\mathfrak{q}' = \mathfrak{q}A_{\mathfrak{p}}$ établissent une correspondance biunovique entre les idéaux premiers $\mathfrak{q}'$ de $A_{\mathfrak{p}}$ et les idéaux premiers $\mathfrak{q}$ de A contenus dans $\mathfrak{p}$.

Sauf les deux dernières assertions, tout cela a été démontré plus haut. Le fait que $g(A_{\mathfrak{p}})$ soit le corps des fractions de $f(A)$ résulte de la prop.2 du §1. Si $S = A-\mathfrak{p}$, et si $\mathfrak{a}$ est un idéal de A tel que $aS \cap \mathfrak{a} \neq \emptyset$ entraîne $a \in \mathfrak{a}$, $S \cap \mathfrak{a} \neq \emptyset$ entraîne $1 \in \mathfrak{a}$, donc on a $\mathfrak{a} = A$ ou $\mathfrak{a} \subset \mathfrak{p}$; réciproquement, si $\mathfrak{a} \subset \mathfrak{p}$, et si de plus $\mathfrak{a}$ est premier dans A, une relation $au \in \mathfrak{a}$, où $a \in A$, $u \in A-\mathfrak{p} \subset A-\mathfrak{a}$ entraîne $a \in \mathfrak{a}$. Supposons alors que $aS \cap \mathfrak{a} \neq \emptyset$ entraîne $a \in \mathfrak{a}$ et que $\mathfrak{a} \neq A$, donc que $\mathfrak{a} \subset \mathfrak{p}$. D'après le coroll.2 de la prop.2 du §1, $A/\mathfrak{a}$ peut être identifié avec un sous-anneau de $A_{\mathfrak{p}}/\mathfrak{a}'$,

$A_{\mathfrak{p}}/\mathfrak{a}'$ étant alors l'anneau des fractions dérivé de $A/\mathfrak{a}$ au moyen de l'image de S dans $A/\mathfrak{a}$. Si donc l'un de ces anneaux est un anneau d'intégrité, il en est de même de l'autre ; donc, si l'un des idéaux $\mathfrak{a}$, $\mathfrak{a}'$ est premier, l'autre l'est aussi.

Exemples.- 1) Si p est un nombre premier, et f l'homomorphisme canonique de Z sur Z/(p), l'anneau local de f est l'ensemble des nombres rationnels de la forme b/a avec $a \in Z$, $b \in Z$, $a \not\equiv 0$ mod.p ; le domaine de f est Q_{∞} .

2) Dans l'ann'au $A = k[[X_1,\ldots,X_n]]$ des séries formelles à n indéterminées $X_1,\ldots,X_n$ sur un corps k , toute série à terme constant non nul est inversible (Alg...) ; si donc f est la spécialisation de A qui à toute série fait correspondre son terme constant (exemple 5 du n°1), l'anneau local de f est A ; l'idéal maximal de A, qui est le noyau de f , est engendré par $X_1,\ldots,X_n$.

Enfin, nous donnerons quelques conditions nécessaires et suffisantes pour qu'un anneau soit un anneau local :

Proposition 13. Soient A un anneau, et M l'ensemble des éléments non inversibles de A . Alors M est réunion des idéaux de A autres que A , réunion des idéaux principaux de A autres que A , et réunion des idéaux maximaux de A ; on a $MA = M$; et les propriétés suivantes sont équivalentes :

a) M est un idéal, ou autrement dit A est anneau local ;

b) il n'y a dans A qu'un idéal maximal ;

c) on a $M+M \subset M$;

d) $x \in M$ entraîne $1+x \notin M$.

En effet, $x \in M$ équivaut à $1 \notin xA$, donc à $xA \neq A$. Si $\mathfrak{a}$ est un idéal autre que A, et si $x \in \mathfrak{a}$, on a $xA \subset \mathfrak{a}$, donc $xA \neq A$ et $x \in M$. Donc tout idéal autre que $\mathfrak{a}$ est contenu dans M , et tout élément de M appartient à un idéal principal autre que A et même engendre un tel idéal.

Comme tout idéal autre que A est contenu dans un idéal maximal (th.2, Alg., Chap.I, §8, n°7), cela démontre la première partie de la proposition et l'équivalence de a) et b). Comme $\mathfrak{M}$ est réunion d'idéaux, on a $\mathfrak{M}A \subset \mathfrak{M}$, donc $\mathfrak{M}A = \mathfrak{M}$ puisque $1 \in A$; donc a) et c) sont équivalentes. Si c) est vérifiée, et on avait $x \in \mathfrak{M}$, $1+x \in \mathfrak{M}$, on aurait $-x \in \mathfrak{M}$, puis $1 = (1+x)+(-x) \in \mathfrak{M}$; donc c) entraîne d). Si c) n'est pas véifiée, soient $a \in \mathfrak{M}$, $b \in \mathfrak{M}$ tels que $a+b \notin \mathfrak{M}$; $a+b$ est donc inversible. Soient alors $x = -(a+b)^{-1}a$, $y = (a+b)^{-1}b$; comme $\mathfrak{M}A = \mathfrak{M}$, on a $x \in \mathfrak{M}$ et $1+x = y \in \mathfrak{M}$, donc d) n'est pas vérifiée.

§ 3. Valuations.

1. Places d'un corps et valuations.

Soit π une place d'un corps K ; d'après la prop.10 du §2, n°5, l'ensemble A des $x \in K$ tels que $x(\pi) \neq \infty$ est un sous-anneau de K, sur lequel π induit une spécialisation finie ; soit $\mathfrak{p}$ le noyau de celle-ci, c'est-à-dire l'ensemble des $x \in K$ tels que $x(\pi)=0$. Si $x \in A-\mathfrak{p}$, on a $x(\pi) \neq 0$, donc $x^{-1}(\pi) \neq \infty$ et $x^{-1} \in A$; A est donc un anneau local, et $\mathfrak{p}$ est son idéal maximal. Si $x \in K-A$, on a $x(\pi) = \infty$, donc $x^{-1}(\pi)=0$ et $x^{-1} \in \mathfrak{p}$; donc le domaine de la spécialisation induite par π sur A est $K_\infty = A \cup \mathfrak{p}^{-1} = A \cup A^{-1}$. Par abus de langage, on ne distinguera pas entre la place π, la spécialisation finie induite par π sur A, et le prolongement canonique de celle-ci à K_∞ ; et l'anneau local A de π sera dit plus brièvement l'anneau de la place π.

On désignera par K^* le groupe multiplicatif des éléments $\neq 0$ du corps K ; rappelons que la relation de divisibilité dans K, relativement à un anneau A, munit K^* d'une structure de groupe préordonné, et que le groupe ordonné canoniquement associé à celui-ci est isomorphe au groupe P^* des idéaux principaux fractionnaires xA de K pour $x \in K^*$, ordonné par inclusion.

Si $K_\infty = A \cup A^{-1}$, ce groupe est totalement ordonné ; en effet, si $x \in K^*$, $y \in K^*$, on a, soit $x/y \in A$, soit $x/y \in A^{-1}$, donc soit $x \in yA$ d'où $xA \subset yA$, soit $y \in xA$ d'où $yA \subset xA$. Réciproquement, supposons que K soit le corps des fractions d'un anneau A et que l'ensemble des idéaux principaux de A soit totalement ordonné par inclusion ; alors, si b/a est un élément quelconque de K^*, avec $a \in A$, $b \in A$, $a \neq 0$, $b \neq 0$, on a, soit $aA \subsetneq bA$ d'où $a \in bA$, $a/b \in A$, $b/a \in A^{-1}$, soit $bA \subset aA$, d'où $b \in aA$, $b/a \in A$; on a donc $K^* \subset A \cup A^{-1}$, d'où $K_\infty = A \cup A^{-1}$. D'ailleurs, la réunion d'une partie, totalement ordonnée par inclusion, de l'ensemble des idéaux d'un anneau est un idéal (cf. la démonstration du th.2 du Chap.I, § 8, n°7) ; d'après la prop.13 du § 2, n°5, il s'ensuit que tout anneau A tel que $K_\infty = A \cup A^{-1}$ est anneau local ; si $\mathfrak{p}$ est son idéal maximal, on en conclut, d'après le th.3 du § 2, n°5, que le prolongement canonique de l'homomorphisme canonique de A sur $A/\mathfrak{p}$ est une place π de K, et que A est l'anneau de π ; la place π est dite canoniquement associée à A.

D'une manière générale, si A est un sous-anneau quelconque d'un corps K, et si φ désigne l'application $x \to xA$ du groupe K^* sur le groupe P^* ordonné par inclusion, φ est un homomorphisme dont le noyau est le groupe multiplicatif des éléments inversibles de A ; on a donc $\varphi(xy) = \varphi(x)\,\varphi(y)$; et, si $x, y, x+y$, z sont dans K^*, les relations $\varphi(x) \geqslant \varphi(z)$, $\varphi(y) \geqslant \varphi(z)$ entraînent $\varphi(x+y) \geqslant \varphi(z)$, car ces relations sont respectivement équivalentes à $x \in zA$, $y \in zA$, $x+y \in zA$.

Si le groupe P^* est réticulé, et en particulier s'il est totalement ordonné, on a donc, pour $x, y, x+y$ dans K^*, $\varphi(x+y) \geqslant \inf[\varphi(x), \varphi(y)]$. Pour des raisons de commodité (le groupe P^* se trouvant être isomorphe au groupe <u>additif</u> Z dans beaucoup de cas importants), nous conviendrons d'employer en général, pour le groupe des valeurs d'une fonction telle que φ, la notation additive; et nous poserons la définition suivante :

Définition 1. On appelle valuation d'un corps K une application ω de K^* dans un groupe totalement ordonné Γ qui satisfasse aux conditions suivantes :

(V_I) $\omega(xy) = \omega(x)+\omega(y)$ pour $x \in K^*$, $y \in K^*$.

(V_{II}) $\omega(x+y) \geqslant \min[\omega(x), \omega(y)]$ pour $x, y, x+y$ dans K^* ;

pour $x \in K^*$, $\omega(x)$ s'appelle l'ordre de x pour la valuation ω. Deux valuations ω, ω' de K seront dites équivalentes s'il existe un isomorphisme φ du groupe ordonné $\omega(K^*)$ sur le groupe ordonné $\omega'(K^*)$, tel que $\omega' = \varphi \circ \omega$.

La condition (V_I) exprime que ω est un homomorphisme. On conviendra une fois pour toutes, dans ces conditions, d'adjoindre à Γ un ensemble de deux éléments notés $-\infty$, $+\infty$, d'étendre à l'ensemble obtenu la relation d'ordre et la loi de composition de Γ en posant $-\infty < \gamma < +\infty$, $\gamma+(+\infty) = \gamma-(-\infty) = +\infty$, $\gamma+(-\infty) = \gamma-(+\infty) = -\infty$ quel que soit $\gamma \in \Gamma$, et de prolonger la valuation ω à K_∞ en posant $\omega(0) = +\infty$, $\omega(\infty) = -\infty$; on vérifie aussitôt que, dans ces conditions, les relations (V_I), (V_{II}) sont satisfaites toutes les fois que les deux membres ont un sens.

Ce qui précède montre que, si A est un sous-anneau de K, si l'on a $K_\infty = A \cup A^{-1}$, et si $U(A) = A \cap A^{-1}$ désigne le groupe des éléments inversibles de A, l'homomorphisme canonique de K^* sur le groupe $K^*/U(A)$ noté additivement est une valuation ω de K, dite canoniquement associée à A ; par définition de ω, $\omega(x) \geqslant 0$, pour $x \in K_\infty$, est équivalent à $x \in A$, donc aussi à $x(\pi) \neq \infty$ si π est une place de K dont l'anneau est A ; la relation $\omega(x) = 0$ est équivalente à $x \in U(A) = A \cap A^{-1}$ et à $x(\pi) \neq 0$, $x(\pi) \neq \infty$; par suite, $\mathfrak{p} = A - U(A)$ désignant comme toujours l'idéal maximal de A, $\omega(x) > 0$ est équivalente à $x \in \mathfrak{p}$ et à $x(\pi) = 0$.

Réciproquement, soit ω une valuation quelconque d'un corps K ; il est immédiat que l'ensemble des $x \in K_{\infty}$ tels que $\omega(x) \geqslant 0$ est un sous-anneau A de K , dont les éléments inversibles sont ceux pour lesquels $\omega(x)=0$, et que les x tels que $\omega(x) > 0$ forment un idéal $\mathfrak{p}$ de A , qui est donc l'idéal maximal de A . Comme Γ est totalement ordonné, on a $K_{\infty} = A \cup A^{-1}$. Le groupe ordonné $\omega(K^{*})$ est, dans ces conditions, isomorphe au groupe $K^{*}/U(A)$ ordonné comme il a été dit ci-dessus ; autrement dit, ω est équivalente à la valuation canoniquement associée à A.

Définition 2. Si ω est une valuation d'un corps K , l'ensemble A des $x \in K$ tels que $\omega(x) \geqslant 0$, et l'ensemble $\mathfrak{p}$ des $x \in K$ tels que $\omega(x) > 0$, s'appelleront respectivement l'anneau de la valuation et l'idéal de la valuation. Un anneau d'intégrité A s'appellera un anneau de valuation d'un corps K si c'est l'anneau d'une valuation de K ; il sera dit anneau de valuation si c'est l'anneau d'une valuation de son corps des fractions.

On peut résumer comme suit les résultats obtenus :

Théorème 1. Soient A un anneau d'intégrité, K son corps des fractions. Alors les propriétés suivantes sont équivalentes :

a) l'ensemble des idéaux principaux de A est totalement ordonné par inclusion ;

b) l'ensemble des idéaux principaux fractionnaires dans K relativement à A est totalement ordonné par inclusion ;

c) $K_{\infty} = A \cup A^{-1}$;

d) A est l'anneau d'une place π de K , c'est-à-dire l'anneau des $x \in K$ tels que $x(\pi) \neq \infty$;

e) A est l'anneau d'une valuation ω de K , c'est-à-dire l'anneau des $x \in K$ tels que $\omega(x) \geqslant 0$.

 34

Lorsqu'il en est ainsi, A est un anneau local ; si π est une place, et ω une valuation, dont l'anneau soit A , l'idéal maximal $\mathfrak{p}$ de A est le noyau de π c'est-à-dire l'ensemble des x tels que $x(\pi)=0$, et est aussi l'ensemble des x tels que $\omega(x)>0$. Enfin, si A est donné, la place π et la valuation ω sont déterminées d'une manière unique à une équivalence près ; l'image de A par π est un corps isomorphe à $A/\mathfrak{p}$.

On dira qu'une place π et une valuation ω ayant le même anneau A sont associées l'une à l'autre et associées à A ; par abus de langage, on transportera parfois aux valuations la terminologie relative aux places, et réciproquement ; c'est ainsi que, si A' est un sous-anneau de A , l'idéal premier $A'\cap\mathfrak{p}$ de A', qui est le noyau de la spécialisation finie induite par π sur A', s'appellera, soit le noyau de π sur A', soit le noyau de ω sur A' ; comme ω n'induit pas un homomorphisme sur A', cet abus de langage ne peut en général causer aucune confusion. L'image de A par π, ou encore l'image de K par π qui est le corps projectif déduit de l'image de A par π par adjonction de ∞ , s'appelleront souvent, par abus de langage, le corps des valeurs de π . L'image de K^* par ω , ou encore, par abus de langage, l'image de K par ω qui se déduit de $\omega(K^*)$ par adjonction de $+\infty$ et de $-\infty$, s'appelleront le groupe des ordres de ω . Le corps des valeurs d'une place associée à A est isomorphe au corps des restes $A/\mathfrak{p}$ de A , et le corps des valeurs de la place canoniquement associée à A est ce corps des restes. Le groupe des ordres d'une valuation associée à A est isomorphe au groupe $K^*/U(A)$ écrit additivement.

Il est clair que, non seulement $\omega(x)>0$, mais toute relation $\omega(x)>\gamma$ ou $\omega(x)\geqslant\gamma$, avec $\gamma\in\Gamma$, détermine un idéal fractionnaire de A , et un idéal de A si $\gamma\geqslant 0$. Plus généralement, soit M un sous-A-module de K ; soient $\Gamma'=\omega(M)$, $\Gamma''=\omega(C(M))$. Si $x\in M$, $y\in C(M)$, on ne peut avoir $y \in xA$, donc on a $\omega(y) < \omega(x)$; donc $\omega(x) = \omega(y)$ entraîne que x, y sont à la fois dans M ou à la fois dans $C(M)$, et par suite on a $M = \overset{-1}{\omega}(\Gamma')$; et on a $\gamma'' < \gamma'$ quels que soient $\gamma' \in \Gamma'$, $\gamma'' \in \Gamma''$. Rappelons qu'on appelle coupure d'un ensemble totalement ordonné X une partition $X = X' \cup X''$ de X en deux parties non vides X', X'' telles que $x' \in X'$, $x'' \in X''$ entraîne $x'' < x'$. Il est immédiat que réciproquement, si $\omega(K_{\infty}) = \Gamma' \cup \Gamma''$ est une coupure de $\omega(K_{\infty})$, $M = \overset{-1}{\omega}(\Gamma')$ est un sous-A-module de K ; il y a donc correspondance biunivoque entre ces coupures et ces A-modules. Les cas $M = \{0\}$, $M = K$ correspondent respectivement à $\Gamma' = \{+\infty\}$ et à $\Gamma'' = \{-\infty\}$; en tout autre cas, il y a $z \in K$ tel que $\omega(z) \in \Gamma''$, et alors on a $M \subset zA$, donc M est idéal fractionnaire ; M est un idéal de A si tout élément de Γ' est $\geqslant 0$.

L'application du théorème de prolongement des spécialisations (th.1 du §2, n°4) donne ici ce qui suit :

Théorème 2. *Soient A un sous-anneau d'un corps K , et $\mathfrak{a}$ un idéal de A autre que A_1. Alors il existe une place π et une valuation ω de K dont l'anneau contienne A et dont le noyau contienne $\mathfrak{a}$, et même, si $\mathfrak{a}$ est un idéal premier de A , une place π et une valuation ω de K dont l'anneau contienne A et dont le noyau sur A soit $\mathfrak{a}$.*

Si $\mathfrak{a}$ est premier, posons $\mathfrak{p} = \mathfrak{a}$; sinon, prenons pour $\mathfrak{p}$ un idéal maximal de A contenant $\mathfrak{a}$. On prendra alors pour π une place de K prolongeant l'homomorphisme canonique de A sur $A/\mathfrak{p}$, et pour ω une valuation associée à π .

Théorème 3. *Si L est une extension d'un corps K , toute valuation de K peut être prolongée à une valuation de L .*

Il suffit en effet de prolonger à une place de L une place associée à la valuation donnée sur K , et de prendre une valuation associée à la place de L ainsi obtenue. Bien entendu, le groupe des ordres de la valuation prolongée sera en général distinct du groupe des ordres de la valuation dont on est parti (qui en est un sous-groupe ordonné) ; le prolongement ne serait pas toujours possible si on voulait que le groupe des ordres restât le même.

Exemples. 1) Tout corps K est un anneau de valuation. Une place associée à cet anneau est un isomorphisme de K dans un corps ; en particulier, la place canoniquement associée à cet anneau est l'automorphisme identique de K . Une valuation associée à cet anneau prend sur K^* la valeur constante 0 . Ces places et cette valuation de K sont dites triviales.

2) Soient p un nombre premier, f l'homomorphisme canonique de Z sur le corps fini $F = Z/(p)$ à p éléments. Le domaine de f étant Z (cf. exemple 1, § 2, n°5), le prolongement canonique de f est une place π de Q , à savoir la place canoniquement associée à l'anneau local A de f . Si, pour tout $x \in Q^*$, on définit $\omega(x)$ comme l'exposant de p dans la décomposition de x en facteurs premiers (Alg...), on vérifie aussitôt que ω est une valuation de Q ; on l'appelle la valuation p-adique de Q . L'anneau de ω n'étant autre que l'anneau local A de f, ω et la place π sont associées.

3) L'exemple 2) se généralise aussitôt au corps des fractions de tout anneau principal (Alg...). Considérons en particulier le corps k(X) des fractions rationnelles à une indéterminée X sur un corps k . Si ξ est un élément d'une extension K de k, on a vu (exemple 1 du § 2, n°4) que $R \rightarrow R(\xi)$ est une place de k(X), dont l'anneau est l'ensemble A des fractions $R = P/Q$, où $P \in k[X]$, $Q \in k[X]$, et $Q(\xi) \neq 0$.

Si ξ est transcendant sur k, on a donc $A = k(X)$, et ξ définit une place triviale de $k(X)$. Si au contraire ξ est algèbrique sur k, soit F son polynome minimal sur k ; et, pour tout $R \in k(X)$, soit $\omega(R)$ l'exposant de F dans l'expression de R comme produit de puissances de polynomes irréductibles de $k[X]$. Alors ω est une valuation de $k(X)$ dont l'anneau est A.

4) Soit $K = k((X))$ le corps des fractions de l'anneau $A = k[[X]]$ des séries formelles à une indéterminée X sur le corps k ; rappelons (Alg...) que K est le corps des séries formelles $x = \sum_{\nu=n}^{\infty} a_\nu X^\nu$ où n est un entier positif ou négatif, et les a_ν sont dans k ; si, pour un tel élément x, on désigne par $\omega(x)$ le plus petit entier ν tel que $a_\nu \neq 0$, ω est une valuation de k, dont l'anneau est A. Si f est la spécialisation qui, à tout $x \in A$, fait correspondre son terme constant, le domaine de f est K_∞, et son prolongement canonique est une place de K dont l'anneau est A.

5) Au contraire, l'anneau $k[[X_1, \dots, X_n]]$ des séries formelles à n indéterminées n'est pas un anneau de valuation si $n > 1$.

6) Considérons le corps $K = k(X,Y)$ des fractions rationnelles à deux indéterminées X,Y sur un corps k. Si on pose $k'=k(X)$, on a $K = k'(Y)$, et on peut donc appliquer à K tout ce qu'on a fait dans l'exemple 2) ci-dessus ; on obtient ainsi des valuations dont le groupe des ordres est isomorphe à Z, et des places dont le corps des valeurs est isomorphe à une extension algèbrique de $k'=k(X)$. On peut opèrer de même en échangeant X et Y. Nous allons maintenant définir des valuations et places d'un autre type ; nous nous bornerons à considérer des places qui induisent sur l'anneau $k[X,Y]$ la spécialisation $P(X,Y) \to P(0,0)$, et des valuations associées à de telles places.

a) Dans l'anneau $k[[T]]$ des séries formelles à une indéterminée T, soient x,y deux séries algèbriquement indépendantes, à terme constant nul (si k est de caractéristique 0, on peut prendre p.ex. $x = T$, $y = \sum_{n=1}^{\infty} T^n/n!$) ; l'application $R \to R(x,y)$ de $k(X,Y)$ dans $k((T))$ est un isomorphisme. Si ω désigne la valuation de $k((T))$, à valeurs dans Z, définie dans l'exemple 3) ci-dessus, $R \to \omega(R(x,y))$ est une valuation de $k(X,Y)$, dont le groupe des ordres est Z.

b) Soit α un nombre réel irrationnel >0. Un polynome $P \in k[X,Y]$ étant écrit sous la forme $P = \sum_i a_i X^{m_i} Y^{n_i}$, avec $a_i \in k$ et $a_i \neq 0$ pour tout i, posons $v(P) = \min_i (m_i + \alpha n_i)$; on notera que, pour $i \neq j$, on a $m_i + \alpha n_i \neq m_j + \alpha n_j$ puisque α est irrationnel. Dans ces ces conditions, on vérifie immédiatement que v satisfait, sur l'anneau $k[X,Y]$, aux conditions (V_I), (V_{II}) des valuations, d'où on conclut (cf. prop.2 du n°2 ci-dessous) que v se prolonge à une valuation de $k(X,Y)$ par la formule $v(P/Q) = v(P) - v(Q)$. Le groupe des ordres de v est le sous-groupe $Z + \alpha Z$ de R, avec l'ordre induit par celui de R.

c) Ordonnons cette fois le groupe $Z \times Z$ lexicographiquement ; rappelons que, pour cet ordre, on a $(m,n) < (m',n')$ si $m < m'$ ou si $m = m'$, $n \leq n'$; $Z \times Z$ est ainsi totalement ordonné. Un polynome P étant toujours écrit comme $P = \sum_i a_i X^{m_i} Y^{n_i}$, posons cette fois $w(P) = \min_i((m_i, n_i))$, min étant pris au sens de l'ordre lexicographique. On vérifie à nouveau (V_I), (V_{II}), puisque w se prolonge au moyen de $w(P/Q) = w(P) - w(Q)$ à une valuation de $k(X,Y)$; le groupe des ordres est ici $Z \times Z$. On vérifie facilement que l'anneau A de w se compose des $R = P/Q$ tels que l'on ait, soit $P(0,Y) = 0$ et $Q(0,Y) \neq 0$, soit $P(0,Y) = Y^n P_1(Y)$, $Q(0,Y) = Y^n Q_1(Y)$ et $Q_1(0) \neq 0$, P, Q, P_1 et Q_1 étant des polynomes. Mais posons $k'' = k(Y)$, d'où $K = k''(X)$; soit φ la place de K, à valeurs dans k''_∞, qui, à tout $R = \Phi(X) \in k''(X) = K$, fait correspondre $\varphi(R) = \Phi(0) \in k''_{\infty}$; soit ψ la place de k'', à valeurs dans k_{∞}, qui, à tout $S(Y) \in k'' = k(Y)$, fait correspondre $\psi(S) = S(0)$; comme toujours, on prend $\psi(\infty) = \infty$. Alors $\psi\circ\varphi$ est une place de K à valeurs dans k_{∞} ; et on vérifie que l'anneau de cette place n'est autre que l'anneau A de la valuation w.

[Note du rédacteur : Il serait peut être préférable de rédiger les exemples a),b),c) ci-dessus pour les séries formelles à deux variables (corps des quotients de l'anneau $k[[X,Y]]$) plutôt que pour les fractions rationnelles ; le fait qu'on a affaire à des fractions rationnelles tend à détourner l'attention de ce qui est essentiel dans ces exemples. On peut se demander, d'autre part, s'ils sont bien à leur place ici ; en particulier, c) se comprend mieux après la discussion générale des valuations composées ; et il ne convient pas de séparer b) de c). Le plus simple, et peut-être le mieux, serait de les mettre en exercice, avec un renvoi approprié dans le texte].

2. Propriétés élémentaires des valuations.

Proposition 1. Soit ω une valuation d'un corps K. On a $\omega(\pm 1)=0$, et même $\omega(\zeta)=0$ pour toute racine de l'unité ζ dans K ; $\omega(-x)=\omega(x)$ pour $x\in K$; et, quels que soient les $x_i \in K$, on a

$$\omega\Big(\sum_{i=1}^{m} x_i\Big) \geqslant \min_i(\omega(x_i)) \quad ; \tag{1}$$

de plus, dans cette dernière relation, les deux membres sont égaux s'il n'y a qu'un seul indice i tel que $\omega(x_i) = \min_i(\omega(x_i))$.

Soit A l'anneau de ω. Soit $\zeta^n = 1$; on a $\zeta \in A$ ou $\zeta^{-1} \in A$; donc, en vertu de $\zeta^{-1} = \zeta^{n-1}$, $\zeta = (\zeta^{-1})^{n-1}$, ζ et ζ^{-1} sont dans A, donc $\omega(\zeta)=0$; par suite, $\omega(\zeta x) = \omega(x)$ pour tout x, et en particulier $\omega(-x) = \omega(x)$. La relation (1) est triviale pour $m=1$, n'est autre que (V_{II}) (déf.1 du n°1) pour $m=2$, et se démontre aussitôt à partir de là, par récurrence, pour m quelconque. Enfin, si $\omega(x_j) > \omega(x_i)$ pour tout $j \neq i$, et qu'on pose $y = \sum_{j\neq i} x_j$, on aura $\omega(y) \geqslant \min_{j\neq i}(\omega(x_j)) > \omega(x_i)$; on a aussi, dans ces conditions, $\omega(x_i) = \omega((x_i+y)+(-y)) \geqslant \min(\omega(x_i+y), \omega(y))$; ces relations entraînent $\omega(x_i) \geqslant \omega(x_i+y)$; comme (1) s'écrit $\omega(x_i+y) \geqslant \omega(x_i$

il y a donc bien égalité entre les deux membres de (1).

Corollaire 1. Si $x\in K$, $y\in K$, et $\omega(x)\neq\omega(y)$, on a $\omega(x+y)=\min(\omega(x),\omega(y))$.

Ceci est la dernière assertion de la prop.1 pour $m=2$.

Corollaire 2. Si les x_i sont dans K et satisfont à $\sum_{i=1}^{m} x_i=0$, $m>1$, il y a au moins deux indices distincts i, j tels que $\omega(x_i)=\omega(x_j)=\min_{1\leqslant k\leqslant m}(\omega(x_k))$.

Cela est évident si tous les x_i sont nuls. Sinon on a $\omega(\sum x_i)=+\infty>\min_k(\omega(x_k))$, d'où le résultat en vertu de la dernière assertion de la prop.1 .

Corollaire 3. Un corps fini n'admet pas de valuation non triviale.

En effet, dans un corps fini, tout élément $\neq 0$ est racine de l'unité.

Proposition 2. Soient A un anneau d'intégrité, et ω une application de l'ensemble A^* des éléments $\neq 0$ de A dans un ~~xxxx~~ groupe totalement ordonné Γ, telle que l'on ait $\omega(xy)=\omega(x)+\omega(y)$ pour $x\in A^*$, $y\in A^*$, et $\omega(x+y)\geqslant\min(\omega(x),\omega(y))$ pour $x\in A^*$, $y\in A^*$, $x+y\in A^*$. On peut alors, d'une manière et d'une seule, prolonger ω à une valuation du corps des fractions K de A , dont le groupe des ordres est le sous-groupe engendré par $\omega(A^*)$ dans Γ .

En effet, on peut, d'une manière et d'une seule, prolonger ω à un homomorphisme de K^* dans Γ (Alg.,Chap.I...) ; reste à vérifier (V_{II}). Soient donc $x=b/a$, $y=b'/a'$ des éléments de K^* tels que $x+y\in K^*$, où a,b,a',b' sont dans A^* ; on a alors $\omega(x)=\omega(a'b)-\omega(aa')$, $\omega(y)=\omega(ab')-\omega(aa')$, $\omega(x+y)=\omega(a'b+ab')-\omega(aa')$, et, par hypothèse, $\omega(a'b+ab')\geqslant\min(\omega(a'b),\omega(ab'))$, d'où le résultat.

Proposition 3. Soient A un anneau principal, K son corps des fractions ; alors, si (p) est un idéal maximal de A, $A_{(p)}$ est un anneau de valuation de K , et il n'y a pas d'autre anneau de valuation de K , contenant A ,

<u>que K et les $A_{(p)}$. La place de K canoniquement associée à $A_{(p)}$ est le prolongement canonique de l'homomorphisme canonique de A sur $A/(p)$; une valuation associée à $A_{(p)}$ est celle où l'ordre de tout $x \in K^*$ est l'exposant de p dans la décomposition de x en facteurs premiers relative à A</u> .

En effet, si π est une place dont l'anneau contienne A, son noyau sur A est un idéal premier, donc (0) ou de la forme (p) ; l'anneau local de la spécialisation induite par π sur A est K dans le premier cas, $(A_{(p)}$ dans le second, et en tout cas son domaine est K_∞ ; car, si $v_p(x)$ est, pour $x \in K^*$, l'exposant de p dans la décomposition de x en facteurs premiers, il est immédiat que $x \in A_{(p)}^*$ équivaut à $v_p(x) \geqslant 0$, donc que $x \notin A_{(p)}$ entraîne $x^{-1} \in A_{(p)}$. La place π est donc le prolongement canonique de la spécialisation qu'elle induit sur A , et son anneau est $A_{(p)}$; et on vérifie immédiatement que v_p est une valuation.

<u>Corollaire 1. Toute valuation non triviale du corps Q des nombres rationnels est équivalente à l'une des valuations</u> v_p (dites "p-adiques", cf. exemple 2 du n°1) <u>associées aux nombres premiers</u> p .

En effet, tout sous-anneau de Q contient 1, donc Z ; il n'y a donc qu'à appliquer la prop.3 à Z et Q .

<u>Corollaire 2. Soit $K = k(X)$ le corps des fractions rationnelles à une indéterminée X sur un corps k . Alors toute valuation de K , non triviale sur K , triviale sur K , est équivalente à l'une des suivantes</u> :

a) F <u>étant un polynome irréductible dans $k[X]$, on prend pour</u> $v_F(R)$, <u>quel que soit $R \in K^*$, l'exposant de F dans la décomposition de R en polynomes irréductibles de</u> $k[X]$;

b) <u>pour</u> $R = P/Q$, $P \in k[X]$, $Q \in k[X]$, $P \neq 0$, $Q \neq 0$, <u>on prend</u> $v_\infty(R) = \deg P - \deg Q$.

Soit A un anneau de valuation de K , contenant k et autre que K . Si $X \in A$, on a $A \supset k[X]$; alors la prop.3, appliquée à $k[X]$ et K , montre que A est l'anneau d'une des valuations v_P. Sinon, on a $1/X \in A$, donc $A \supset k[X']$ avec $X' = 1/X$; de plus, comme $X \notin A$, $X' = 1/X$ est dans l'idéal maximal de A, donc dans le noyau sur $k[X']$ de toute place d'anneau A ; ce noyau contient donc l'idéal (X') de $k[X']$, et par suite n'est autre que (X') puisque c'est là un idéal maximal. La valuation v associée à A est alors (à une équivalence près) celle où $v(R)$ est l'exposant de X' dans la décomposition de R en polynomes irréductibles de $k[X']$; on vérifie immédiatement que cet exposant n'est autre que v_∞.

3. Indépendance des valuations. Dans ce qui va suivre, il sera commode (mais non indispensable) de pouvoir utiliser un langage topologique. Si ω est une valuation d'un corps K, les parties de K définies par une inégalité de la forme $\omega(x) > \gamma$, où $\gamma \in \omega(K^*)$, forment un système fondamental de voisinages de 0 sur le groupe additif de K, et définissent donc sur K une topologie compatible avec sa structure de groupe additif. Si ω est triviale, on obtient ainsi la topologie discrète de K ; dans le cas contraire, si A est l'anneau de ω, il suit des résultats donnés au n°1 qu'on définit la même topologie sur K en prenant pour système fondamental de voisinages de 0 tous les idéaux de A autres que (0), ou encore tous les sous-A-modules de K autres que $\{0\}$.

On vérifie alors sans difficulté qu'on définit une topologie séparée sur K_∞ en prenant de plus, pour système fondamental de voisinages de ∞, les parties de K_∞ définies par une inégalité $\omega(x) < \gamma$, où $\gamma \in \omega(K^*)$. On vérifie aussi que, pour cette topologie, la fonction $1/x$ est partout continue (c'est donc un homéomorphisme de K_∞ sur lui-même), et les fonctions $x \pm y$ et xy sont continues en tout point de $K_\infty \times K_\infty$ où elles sont définies ; ce sont là des conséquences faciles de (V_{II}) et du coroll.1 de la prop.3, n°2. En particulier, K est un corps topologique pour la topologie en question ; et, si R est une fraction rationnelle à une indéterminée X sur K, l'application $x \to R(x)$ de K_∞ dans K_∞

est continue (cf. Top.Géné., Chap.VI, § 3, n°4).

Nous allons appliquer ces notions à l'étude simultanée de plusieurs valuations d'un même corps K.

Remarquons d'abord que, si A est un anneau de valuation du corps K, et R une partie multiplicativement stable de K, contenant 1, $A'=AR$ est l'anneau engendré par $A\cup R$; en effet, si $a\in A$, $b\in A$, $r\in R$, $s\in R$, on a, soit $r/s\in A$, soit $s/r\in A$; si par exemple $r/s\in A$, on a $ar+bs = s[a(r/s)+b]s\in AR$; de plus, comme $A'\supset A$ et $A\cup A^{-1}=K_\infty$, on a $A'\cup A'^{-1}=K_\infty$, donc A' est anneau de valuation.

Proposition 4. Soient ω, ω' deux valuations non triviales d'un corps K, et A, A' leurs anneaux. Alors AA' est l'anneau engendré par $A\cup A'$, et est anneau de valuation de K ; et les propriétés suivantes sont équivalentes :

a) $AA'=K$;

b) quels que soient $\gamma\in\omega(K^*)$, $\gamma'\in\omega'(K^*)$, il existe $x\in K^*$ tel que $\omega(x)\geqslant\gamma$, $\omega'(x)\leqslant\gamma'$;

c) si V est un voisinage de $a\in K_\infty$ pour la topologie définie par ω, et V' un voisinage de $a'\in K_\infty$ pour la topologie définie par ω', on a $V\cap V'\neq\emptyset$.

c) entraîne b) qui en est un cas particulier (pour $a=0$, $a'=\infty$) ; b) entraîne a), car, si $z\in K^*$ et si on prend, dans b), $\gamma=0$ et $\gamma'=\omega'(z)$, on aura $x\in A$ et $z/x\in A'$, donc $z=x(z/x)\in AA'$. Réciproquement, a) entraîne b) ; prenons en effet $\gamma=\omega(y)$, $\gamma'=\omega'(y')$; a) étant vérifiée, on a $y'/y=aa'$ avec $a\in A$, $a'\in A'$, d'où, en prenant $x=ya=y'/a'$, $\omega(x)\geqslant\gamma$ et $\omega'(x)\leqslant\gamma'$. Enfin, puisque ω et ω' ne sont pas triviales et que par conséquent $\omega(K^*)$ et $\omega'(K^*)$ sont des groupes ordonnés non réduits à $\{0\}$, donc n'ont ni élément minimal ni élément maximal, b) entraîne que c) est vérifiée pour $a=0$, $a'=\infty$. Pour $a\neq a'$, $x\to(x-a)/(x-a')$

est un homéomorphisme de K_∞ sur K_∞ qui applique a sur 0 et a' sur ∞ ; donc c) est encore vérifiée dans ce cas ; et c) est vérifiée trivialement pour $a = a'$.

<u>Définition 3.</u> <u>On dit que deux valuations non triviales</u> ω, ω' <u>d'un corps</u> K , <u>d'anneaux</u> A,A', <u>sont étrangères si</u> $AA' = K$.

<u>Proposition 5.</u> <u>Soient</u> ω_i $(0 \leqslant i \leqslant n)$ <u>des valuations non triviales d'un corps</u> K , <u>telles que</u> ω_0 <u>et</u> ω_j <u>soient étrangères pour</u> $1 \leqslant j \leqslant n$. <u>Soient</u> a,a' <u>deux éléments distincts de</u> K_∞ ; <u>soit</u> V_0 <u>un voisinage de</u> a <u>pour la topologie définie par</u> ω_0, <u>et, pour</u> $1 \leqslant j \leqslant n$, <u>soit</u> V_j <u>un voisinage de</u> a' <u>pour la topologie définie par</u> ω_j. <u>Alors</u> $V_0, V_1, \ldots, V_n$ <u>ont au moins un élément commun</u>.

Comme ci-dessus, au moyen de l'homéomorphisme $x \to (x-a)/(x-a')$, on se ramène au cas $a=0$, $a'=\infty$; le résultat étant vrai pour $n=1$ d'après la prop.4, on procédera par récurrence. En remplacant V_0 et les V_j par des voisinages plus petits, on peut supposer qu'ils sont définis respectivement par $\omega_0(x) > \gamma_0$, $\omega_j(x) < -\gamma_j$, avec $\gamma_i \in \omega_i(K^*)$ et $\gamma_i > 0$ pour $0 \leqslant i \leqslant n$. D'après l'hypothèse de récurrence, il existe y tel que $\omega_0(y) > \gamma_0$ et $\omega_h(y) < -\gamma_h$ pour $1 \leqslant h \leqslant n-1$, et z tel que $\omega_0(z) > \gamma_0$ et $\omega_k(z) < -\gamma_k$ pour $2 \leqslant k \leqslant n$. On distinguera quatre cas :

a) si $\omega_n(y) \leqslant 0$, $\omega_1(z) \leqslant 0$, on prendra $x = yz$;

b) si $\omega_n(y) \leqslant 0$ et $\omega_1(z) > 0$, on prendra $x = yz+y = y(1+z)$.

En effet, on a alors $\omega_k(1+z) = \omega_k(z)$ et $\omega_k(y) \leqslant 0$, donc $\omega_k(x) \leqslant \omega_k(z)$, pour $2 \leqslant k \leqslant n$, et $\omega_1(1+z)=0$, donc $\omega_1(x) = \omega_1(y)$.

c) de même, si $\omega_n(y) > 0$, $\omega_1(z) \leqslant 0$, on prendra $x = yz+z$.

d) si $\omega_n(y) > 0$, $\omega_1(z) > 0$, on prendra $x = yz+y+z = (1+y)(1+z)-1$.

En effet, on a alors $\omega_\ell(1+y) = \omega_\ell(y)$, $\omega_\ell(1+z) = \omega_\ell(z)$, d'où $\omega_\ell(x) = \omega_\ell(yz)$ pour $2 \leqslant \ell \leqslant n-1$; $\omega_1(1+y) = \omega_1(y)$, $\omega_1(1+z)=0$, d'où $\omega_1(x) = \omega_1(y)$, et de même $\omega_n(x) = \omega_n(z)$.

Théorème 4 ("théorème d'approximation"). Soient $\omega_1,\dots,\omega_n$ des valuations non triviales, deux à deux étrangères, d'un corps K ; pour $1\leq i\leq n$, soit $a_i\in K_\infty$, et soit V_i un voisinage de a_i pour la topologie définie par ω_i ; alors les V_i ont au moins un élément commun.

D'après le coroll.3 de la prop.1 du n°2, K est un corps infini ; il y a donc un $b\in K$ distinct de tous les a_i , et, au moyen de l'homéomorphisme $x\to 1/(x-b)$, on se ramène au cas où tous les a_i sont finis. On a donc à démontrer le résultat suivant :

Théorème 4'. K et les ω_i étant comme dans le th.4, soit, pour $1\leq i\leq n$, $a_i\in K$ et $\gamma_i\in\omega_i(K^*)$. Alors il existe $x\in K$ tel que $\omega_i(x-a_i)>\gamma_i$ pour $1\leq i\leq n$.

Prenons $x=\sum_i t_ia_i$, d'où $x-a_i=(t_i-1)a_i+\sum_{j\neq i} t_ja_j$; x satisfera aux conditions imposées si l'on a

$\omega_i(t_i-1)>\gamma_i-\omega_i(a_i)$, $\omega_i(t_j)>\gamma_i-\omega_j(a_j)$ quels que soient i,j .

Autrement dit, t_i est assujetti à être dans un voisinage donné de 1 pour la topologie ω_i , et dans un voisinage donné de 0 pour chacune des topologies ω_j avec $j\neq i$. Comme il existe de tels t_i d'après la prop.5, cela démontre le théorème.

4. Places et valuations composées. Soient A,A' deux anneaux de valuation d'un corps K , tels que $A'\subset A$; leurs idéaux maximaux sont alors $\mathfrak{p}=C(A^{-1})$, $\mathfrak{p}'=C(A'^{-1})$, les complémentaires étant pris dans K_∞ ; on a donc $\mathfrak{p}\subset\mathfrak{p}'\subset A'\subset A$. Soit φ une place de K_∞ associée à A , donc une spécialisation de K_∞ sur un corps projectif L_∞ ; soit φ' une place de K_∞ associée à A'. Sur A', φ' induit un homomorphisme de A' sur $\varphi'(A')$, dont le noyau $\mathfrak{p}'$ contient le noyau $\mathfrak{p}$ de l'homomorphisme induit par φ sur A' ; donc, par passage au quotient, φ' détermine un homomorphisme

ψ de $B = \varphi(A')$ sur $\varphi'(A')$, tel que l'on ait, sur A', $\varphi' = \psi \circ \varphi$.

Si $y \in L_\infty - B$, on a $y = \varphi(x)$ avec $x \in K_\infty - A'$, donc $x^{-1} \in \mathfrak{P}'$, et par suite $y^{-1} = \varphi(x^{-1})$ est alors dans le noyau $\mathfrak{Q} = \varphi(\mathfrak{P}')$ de ψ ; il s'ensuit que le domaine de la spécialisation finie ψ de B est L_∞ , et que le prolongement canonique de ψ à ce domaine, qu'on notera encore ψ , est une place de L_∞ . Il est immédiat qu'on a alors $\varphi' = \psi \circ \varphi$, non seulement sur A', mais sur K_∞ tout entier. Réciproquement, soit φ une place de K_∞ , appliquant K_∞ sur un corps projectif L_∞ ; soit ψ une place de L_∞ ; $\varphi' = \psi \circ \varphi$ est alors une place de K_∞ ; et, si A, A', B sont les anneaux des places φ, φ', ψ , il est clair qu'on a $A' = \overset{-1}{\varphi}(B) \subset A$.

Examinons maintenant la structure de valuations ω, ω' respectivement associées aux anneaux A, A' considérés ci-dessus. Soient $U = A - \mathfrak{P}$, $U' = A' - \mathfrak{P}'$, $V = B - \mathfrak{Q}$ les groupes des éléments inversibles de A , de A' et de B , respectivement ; on a $U' \subset U$. Soient $\Gamma = \omega(K^*)$, $\Gamma' = \omega'(K^*)$; ω est un homomorphisme de K^* sur Γ , de noyau U , et ω' un homomorphisme de K^* sur Γ' , de noyau U' ; puisque $U' \subset U$, ω définit par passage au quotient un homomorphisme θ de Γ' sur Γ , tel que $\omega = \theta \circ \omega'$. De plus, comme la relation de divisibilité $y \in xA'$ dans K^* relativement à A' implique la relation analogue $y \in xA$ relative à A , on voit que θ est un homomorphisme croissant, c'est-à-dire que $\gamma' \geqslant 0$ implique $\theta(\gamma') \geqslant 0$. Autrement dit, si P est l'ensemble des éléments positifs de Γ , et P' celui de Γ' , on a $P \supset \theta(P')$.

On va montrer qu'on a $P = \theta(P')$, ou encore, d'après la définition de θ, que P est l'image de A'^* par l'homomorphisme canonique de K^* sur K^*/U , ou autrement dit que $A = A'U$. Mais, d'après la remarque qui précède immédiatement la prop.4 du n°3, $A'U$ est l'anneau engendré par $A' \cup U$; et, d'après la prop.13 du § 2, n°5, appliquée à A , tout élément de A est, soit dans U, soit de la forme u^{-1} avec $u \in U$; on a donc $A \subset A'U$; comme $A \supset A'U$, on a bien $A = A'U$.

Pour énoncer commodément les résultats obtenus, nous poserons une définition et démontrerons un lemme sur les groupes ordonnés :

<u>Définition 4.</u> <u>Un sous-groupe</u> H <u>d'un groupe ordonné</u> G <u>sera dit isolé si</u> $x \geqslant 0$, $y \geqslant 0$, $x+y \in H$ <u>entraîne</u> $x \in H$ <u>et</u> $y \in H$.

<u>Lemme 1.</u> <u>Soient</u> G <u>un groupe ordonné</u>, f <u>un homomorphisme de</u> G <u>sur un groupe</u> G', H <u>le noyau de</u> f ; <u>soient</u> P <u>l'ensemble des éléments positifs de</u> G , <u>et</u> $P'=f(P)$ <u>son image par</u> f . <u>Alors, pour que</u> P' <u>soit l'ensemble des éléments positifs d'un ordre sur</u> G' <u>compatible avec sa structure de groupe, il faut et il suffit que</u> H <u>soit un sous-groupe isolé de</u> G .

On a en tout cas $P'+P'=P'$; nous devons donc montrer que $P' \cap (-P')=\{0\}$ équivaut à dire que H est isolé. En effet, cette relation signifie que, si $x \geqslant 0$, $y \geqslant 0$, et $f(x)=f(-y)$, on a $f(x) = 0$.

Revenons aux groupes Γ , Γ' ; on voit que le noyau Δ de θ est un sous-groupe isolé de Γ' . Réciproquement, si Δ est n'importe quel sous-groupe isolé de Γ' , soit θ l'homomorphisme canonique de Γ' sur Γ'/Δ ; ordonnons ce dernier groupe en prenant $\theta(P)$ pour ensemble d'éléments positifs ; il est immédiat alors que $\dot{\omega} = \theta\circ\omega$ est une valuation de K .

Enfin, supposons de nouveau les places φ, φ', ψ définies comme alors φ induit sur U un homomorphisme de U sur L^* , dont le noyau est $\overset{-1}{\varphi}(1)$. Mais $\varphi(u)=1$ entraîne $\varphi'(u)=1$, donc $\omega'(u)=0$; par suite ω' induit sur U un homomorphisme de U dans Γ' dont le noyau contient $\overset{-1}{\varphi}(1)$, et détermine donc, par passage au quotient, un homomorphisme η de L^* dans Γ' tel que $\omega' = \eta\circ\varphi$ sur U ; et on a $\eta(L^*)=\omega'(U) = \Delta$. On vérifie immédiatement que η est une valuation de L .

On peut résumer comme suit les résultats obtenus :

Théorème 5. Soient A un anneau de valuation d'un corps K , et $\mathfrak{p}$ son idéal maximal ; soient φ une place et ω une valuation de K , d'anneau A , $\varphi(K_\infty)=L_\infty$, et $\omega(K^*)=\Gamma$. Alors, si A' est un anneau de valuation de K contenu dans A , $\mathfrak{p}'$ son idéal maximal, φ' une place et ω' une valuation de K d'anneau A', on a $A \supset A' \supset \mathfrak{p}' \supset \mathfrak{p}$; il y a une place ψ et une valuation η de L , d'anneau $B=\varphi(A')$, telles que $\varphi'=\psi\circ\varphi$ et $\omega'=\eta\circ\varphi$. Réciproquement, la donnée d'un anneau de valuation B de L , et d'une place ψ et d'une valuation η de L d'anneau B détermine, au moyen de ces formules et de $A'=\overset{-1}{\varphi}(B)$, un anneau de valuation A' de K contenu dans A , et une place φ' et une valuation ω' de K d'anneau A'.

Soient de plus $\Gamma'=\omega'(K^*)$ et $\Delta=\eta(L^*)$; alors Δ est un sous-groupe isolé de Γ'; il y a un homomorphisme θ de Γ' sur Γ , de noyau Δ , appliquant l'ensemble des éléments positifs de Γ' sur celui de Γ , et tel que $\omega=\theta\circ\omega'$. Réciproquement, étant donnés A', ω' et un sous-groupe isolé Δ de $\Gamma'=\omega'(K^*)$, les propriétés précédentes déterminent θ et une valuation ω de K , dont l'anneau A contient A'.

Corollaire. Si ω, ω' sont des valuations non triviales d'un corps K , d'anneaux A,A', et si $A' \subset A$, elles définissent la même topologie sur K.

En effet, un système fondamental de voisinages de 0 pour ω est donné par les ensembles xA , où $x\in K^*$, et un autre est donné par les $x\mathfrak{p}$, où $x\in K^*$; il en est de même pour ω' ; notre conclusion résulte alors de $A\supset A'\supset \mathfrak{p}'\supset\mathfrak{p}$.

[N-B. C'est sans doute pour cela que La Tribu (n°25, p.21, dernière ligne) prescrit de mettre "plus fine", "moins fine", pour les valuations en accord avec la topologie ! . Dans la présente rédaction, les dénominations "valuations plus (moins) fines" ont été supprimées pour cette raison].

Exemple.- La place $\psi\circ\varphi$ du corps $k(X,Y)$, définie dans l'exemple 5c) du n°1, est du type décrit ci-dessus ; Γ' est en ce cas le groupe $Z \times Z$ ordonné lexicographiquement, et Δ est le sous-groupe $\{0\} \times Z$ de celui-ci.

Proposition 6.- Soit B un sous-anneau d'un corps K ; soient $\mathfrak{q}$, $\mathfrak{q}'$ deux idéaux premiers de B tels que $\mathfrak{q}' \supset \mathfrak{q}$. Alors il existe un anneau de valuation A de K, d'idéal maximal $\mathfrak{p}$, tel que $A \supset B$ et $\mathfrak{q} = B \cap \mathfrak{p}$; et, étant donné un tel anneau A, il existe un anneau de valuation A' de K, d'idéal maximal $\mathfrak{p}'$, tel que $A \supset A' \supset B$ et que $\mathfrak{q}' = B \cap \mathfrak{p}'$.

La première assertion n'est autre que le contenu du th.2 du n°1.

Soit alors φ une place d'anneau A, appliquant A sur un corps L ; alors $\varphi(B)$ est un sous-anneau de L, et $\varphi(\mathfrak{q}')$ est un idéal premier de $\varphi(B)$, auxquels on peut appliquer à nouveau le même théorème ; si ψ est une place de L dont l'anneau contienne $\varphi(B)$ et dont le noyau sur $\varphi(B)$ soit $\varphi(\mathfrak{q}')$, $\psi\circ\varphi$ sera une place de K dont l'anneau A' répond à la question.

5. Valuations dans les extensions de dimension finie.

Définition 5. On dira qu'un corps K est de rang fini s'il est de dimension finie n sur le corps premier contenu dans K ; on dira alors qu'il est de rang n+1 s'il est de caractéristique 0, de rang n dans le cas contraire.

Nous démontrerons ensemble les deux théorèmes suivants :

Théorème 6. Soit K une extension d'un corps k, de dimension finie n sur k ; soit φ une place de K, triviale sur k, et soit L le corps des valeurs de φ. Alors la dimension de L sur le corps $\varphi(k)$ est $\leqslant n$; et elle est $\leqslant n-1$ si φ n'est pas triviale sur K.

Théorème 6'. Soit K un corps de rang fini n ; soient φ une place de K, et L le corps des valeurs de φ. Alors le rang de L est $\leqslant n$, et est $\leqslant n-1$ si φ n'est pas triviale ; de plus, ou bien K et L ont même caractéristique, ou bien K est de caractéristique 0 et L de caractéristique $\neq 0$.

Dans le cas du th.6', l'anneau de φ contient l'anneau engendré par 1, donc Z si K est de caractéristique 0, et le corps premier dans le cas contraire. Dans le second cas, φ est donc triviale sur le corps premier, et le th.6' se réduit à un cas particulier du th.6 ; il en est de même dans le premier cas si le noyau de φ sur Z est (0), car alors φ induit un isomorphisme sur Z., donc aussi sur Q d'après la prop.8 du §2,n°4 ; enfin, si le noyau de φ sur Z n'est pas (0), c'est un idéal premier (p), et l'image $\varphi(Z)$ dans L est le corps premier $F = Z/(p)$ à p éléments. Nous n'avons donc qu'à démontrer le th.6 et à traiter le cas d'"inégale caractéristique" du th.6'.

Soient $y_i = \varphi(x_i)$ $(1 \leqslant i \leqslant m)$ des éléments de L algèbriquement indépendants sur le corps $\varphi(k)$ (resp. sur le corps premier $F = (Z) = Z/(p)$). Alors φ induit une spécialisation finie sur l'ensemble $k \cup \{x_1,\ldots,x_m\}$ (resp. sur $Z \cup \{x_1,\ldots,x_m\}$). Si les x_i n'étaient pas algèbriquement indépendants sur k (resp. sur Q), ils satisferaient à une relation $P(x_1,\ldots,x_m)=0$, où P est un polynome à coefficients dans k (resp. un polynome à coefficients dans Z de p.g.c.d. égal à 1 et par suite non tous multiples de p). D'après la définition d'une spécialisation finie (déf.2 du §2,n°1), cela entraînerait une relation analogue, à coefficients non tous nuls dans $\varphi(k)$ (resp. dans $F = Z/(p)$) entre les y_i, ce qui est contraire à l'hypothèse. Donc les x_i sont algèbriquement indépendants sur k (resp. sur Q), et par suite $m \leqslant n$. Cela complète la démonstration de la première partie du th.6'. Pour achever celle du th.6, observons que, ~~xxx~~ les x_i étant comme ci-dessus, φ induit un isomorphisme sur $k[x_1,\ldots,x_m]$, donc aussi sur le corps $k(x_1,\ldots,x_m)$ en vertu de la prop.8 du §2, n°4 ; ce corps est donc contenu dans l'anneau A de φ. Supposons alors que $m = n$, donc que A contienne le corps $K_0 = k(x_1,\ldots,x_n)$; K, ayant même dimension n que K_0 sur k, en est une

une extension algèbrique ; donc si $x \in K$, et en particulier si $x \in A$, $K_0[x]$ est un corps (Alg., Chap. V, § 3, n°1, th. 1) ; A est donc réunion de corps, donc est un corps. On a alors $K_\infty = A \cup A^{-1} = A_\infty$, donc $A=K$; autrement dit, φ est triviale sur K .

Corollaire 1. *Si K est une extension algèbrique d'un corps k , toute place de K , triviale sur k , l'est aussi sur K .*

Pour formules commodément le coroll. 2, nous conviendrons, si K est une extension d'un corps k , et X une partie de K_∞ , de désigner par k(X) le sous-corps de K engendré par k et l'ensemble des éléments de X autres que ∞ .

Corollaire 2. *Soient K une extension d'un corps k , et X une partie de K_∞ telle que k(X) soit de dimension finie sur k . Soit f une spécialisation de $k \cup X$ dans un corps projectif L_∞ qui induise sur k un isomorphisme de k sur un corps k' . Alors la dimension de k'(f(X)) sur k' est $\leqslant n$; et, si cette dimension est n , la spécialisation f est générique.*

Soit en effet K' une clôture algèbrique de k'(f(X)) ; d'après le th. 1 du § 2, n°4, f peut être prolongée à une place φ de k(X) à valeurs dans K' ; le corps des valeurs de φ contient k'(f(X)) et est contenu dans K', donc a même dimension sur k' que k'(f(X)). La conclusion s'ensuit en appliquant à φ le th. 6 .

Remarque - On peut aussi donner du coroll. 2 une démonstration directe ne faisant pas usage du théorème de prolongement (v. exerc.).

Nous allons maintenant considérer les suites finies d'anneaux de valuations A_i d'un corps K dont chacun est contenu dans le précédent, c'est-à-dire tels que $K \supset A_1 \supset A_2 \supset \dots \supset A_m$. D'après le th. 5 du n°4, il revient au même de se donner une telle suite ou bien une suite de corps $K_0=K$,

$K_1,\dots,K_m$, et, pour $1 \leqslant i \leqslant m$, une place φ_i de K_{i-1} dont le corps des valeurs soit K_i ; en effet, de telles places étant données, on définira par récurrence des places θ_i de K en posant $\theta_1 = \varphi_1$, $\theta_{i+1} = \varphi_{i+1} \circ \theta_i$ pour $1 \leqslant i \leqslant m-1$, et on prendra pour A_i l'anneau de θ_i ; réciproquement, les A_i étant donnés, et les θ_i étant des places d'anneaux respectifs A_i , ces formules définissent bien, d'après le th.5, des places φ_i ayant les propriétés indiquées. On dira qu'une telle suite d'anneaux, ou une telle suite de corps et de places, est <u>normale</u> si l'on a $K \neq A_1$ et $A_i \neq A_{i+1}$ pour $1 \leqslant i \leqslant m-1$, c'est-à-dire si la suite $(K, A_1, \dots, A_m)$ est strictement décroissante par inclusion, ou, ce qui revient au même, si aucune des places φ_i n'est triviale. Enfin, si k est un sous-corps de K , on dira qu'une telle suite est <u>normale relativement à</u> k si tous les anneaux A_i contiennent k ; on peut alors supposer que chacune des places φ_i induit sur k l'automorphisme identique.

<u>Proposition 7</u>. <u>Soit</u> K <u>un corps de rang fini</u> n (resp. <u>une extension de dimension finie</u> n <u>d'un corps</u> k). <u>Soit</u> $(A_i)_{1 \leqslant i \leqslant m}$ <u>une suite normale</u> (resp. <u>une suite normale relativement à</u> k), <u>c'est-à-dire une suite, strictement décroissante par inclusion</u>, <u>d'anneaux de valuation de</u> K , <u>autres que</u> K (resp. <u>autres que</u> K <u>et contenant</u> k). <u>Alors la longueur</u> m <u>de cette suite est</u> $\leqslant n$; <u>et il existe de telles suites de longueur</u> n .

Considérons une suite de corps K_i et de places φ_i associée comme il a été dit à la suite (A_i). D'après le th.6' (resp. le th.6), les rangs des corps K_i (resp. les dimensions des K_i sur k) forment pour $0 \leqslant i \leqslant m$, une suite strictement décroissante d'entiers $\geqslant 0$, dont le premier est n ; donc on a $m \leqslant n$. Quant à la dernière assertion, on procédera par récurrence. Prenons d'abord $n=1$; si K est de rang 1 et de caractéristique 0 , c'est une extension algèbrique de Q ; soit $F = Z/(p)$, où p

est un nombre premier, et soit $\overline{F}$ une clôture algèbrique de F ; prolongeons à une place φ_1 de K , à valeurs dans $\overline{F}_\infty$, l'homomorphisme canonique de Z sur Z/(p) (th. du § 2, n°4). Si K est une extension de k de dimension 1, soit x un élément de K transcendant sur k ; soit $\overline{k}$ une clôture algèbrique de k ; prolongeons à une place φ_1 de K , à valeurs dans $\overline{k}_\infty$, l'homomorohisme $P(x) \longrightarrow P(0)$ de $k[x]$ sur k , où P désigne un polynome quelconque à coefficients dans k . Enfin, si K est de rang 1 et de caractéristique $\neq 0$, procédons de même en prenant pour k le corps premier contenu dans K . Dans tous les cas, φ_1 et son corps des valeurs K_1 déterminent a-vec $K_0=K$ une suite normale. Pour n quelconque, soit k' un sous-corps de K sur lequel K soit de dimension 1 (resp. un tel sous-corps, contenant k) ; la construction qu'on vient d'indiquer donne une place φ_1 de K dont le corps des valeurs K_1 est une extension algèbrique de k', donc un corps de rang n-1 (resp. une extension de k de dimension n-1). La conclusion s'ensuit en appliquant à K_1 l'hypothèse de récurrence.

[N-B : C'est ici que le rédacteur comptait placer la prop.13,p.22, de la rédaction précédente, démontrée, suivant les indications de La Tribu, n°25, p.22, 1.3-5, comme conséquence (immédiate !) du coroll.1 du th.6, ci-dessus, et du théorème de prolongement (th.1 du § 2,n°4). A la réflexio (et à moins que le précédent rédacteur n'ait eu des raisons profondes pour l'insèrer dans le texte) il lui semble que cela mérite à peine un exercice] .

6. Rang d'une valuation.

Ce qui précède permet de déterminer la structure des valuations des corps de rang fini. Nous donnerons d'abord quelques résultats auxiliaires sur les groupes ordonnés.

Proposition 8;- Si G est un groupe totalement ordonné, les trois propriétés suivantes sont équivalentes :

a) G <u>n'admet pas de sous-groupe isolé autre que</u> G <u>et</u> $\{0\}$;

b) <u>quels que soient</u> $x>0$ <u>et</u> $x'>0$ <u>dans</u> G , <u>il y a un entier</u> $n>0$ <u>tel que</u> $nx \geqslant x'$;

c) G <u>est isomorphe à un sous-groupe du groupe additif</u> R <u>des nombres réels</u>.

a) entraîne b) ; en effet, si $x>0$ dans G , l'ensemble des $x' \in G$ tels qu'il existe un entier $n>0$ pour lequel $|x'| \leqslant nx$ est un sous-groupe isolé de G , donc n'est autre que G si a) est vérifiée. Réciproquement, si b) est vérifiée, soit x un élément >0 d'un sous-groupe isolé H de G , et $x'>0$ dans G ; il y a $n>0$ tel que $nx-x' \geqslant 0$, d'où on conclut $x' \in H$ puisque $nx = x'+(nx-x') \in H$; on a donc $H = G$. Mais b) n'est pas autre chose que l'"axiome d'Archimède" ((GR_{IV}) de <u>Top.Géné.</u>, Chap.V, §2) ; et, si P est l'ensemble des éléments $\geqslant 0$ de G , la prop.1 de <u>Top.Géné.</u>, Chap.V, § 2 s'applique à $E = I = P$, $\omega = 0$, pourvu que $P-\{0\}$ n'ait pas de plus petit élément, et montre que dans ce cas G est isomorphe à un sous-groupe partout dense de R . Si au contraire $P-\{0\}$ a un plus petit élément <u>a</u> , et si $x \in P$, soit n le plus petit entier tel que $na>x$; on a alors $(n-1)a \leqslant x$, donc $0 \leqslant x-(n-1)a<a$ et par suite $x=(n-1)a$; G est donc alors isomorphe à Z .

<u>Remarque</u>. b) étant l'"axiome d'Archimède", un groupe G satisfaisant aux conditions de la prop.8 est souvent dit archimédien.

En vertu du th.5 du n°4, la prop.8 admet une application immédiate aux anneaux de valuation. On dira, par abus de langage, qu'un sous-anneau A d'un corps K est <u>maximal</u> si A n'est pas un corps et s'il n'existe pas de sous-anneau B de K , autre que K ou A , tel que $K \supset B \supset A$. On déduit alors de la prop.8 le corollaire suivant :

Corollaire. Pour qu'un sous-anneau d'un corps K soit maximal, il faut et il suffit que ce soit l'anneau d'une valuation non triviale de K dont le groupe des ordres soit un sous-groupe de R .

Soit A un tel anneau ; comme ce n'est pas un corps, il y a dans A un élément x non inversible ; d'après le th.2 du n°1, A est donc contenu dans l'anneau A' d'une place dont le noyau sur A contient l'idéal xA ; cette place n'est donc pas triviale, et, comme A est maximal, on a A=A' . Soit ω une valuation de K d'anneau A ; d'après le th.5 du n°4, il faut et il suffit, pour que A soit maximal, que le groupe des ordres de ω n'admette pas de sous-groupe isolé ; la conclusion s'ensuit d'après la prop.8 .

Proposition 9. Si G est un groupe totalement ordonné, l'ensemble des sous-groupes isolés de G est totalement ordonné par inclusion.

Soient H, H' deux sous-groupes isolés de G ; supposons que $H'\not\subset H$, donc qu'il existe un $x' > 0$ dans $H' \cap C(H)$; soit x un élément > 0 de H ; on a $x \leqslant x'$, car dans le cas contraire on aurait $x = x'+(x-x') \in H$, $x' \in 0$, $x-x' \in 0$, donc $x' \in H$. Mais alors les relations $x'=x+(x'-x) \in H'$, $x > 0$, $x'-x \geqslant 0$ montrent que $x \in H'$. Donc on a $H \subset H'$.

Corollaire 1. Si A est un anneau de valuation d'un corps K , les sous-anneaux de K qui contiennent A forment un ensemble totalement ordonné par inclusion.

En effet, d'après le th.5 du n°4, ils sont en correspondance biunivoque (préservant la relation d'inclusion) avec les sous-groupes isolés du groupe des ordres d'une valuation associée à l'anneau A .

Corollaire 2. Si les sous-groupes isolés d'un groupe totalement ordonné G sont en nombre fini, ils forment une suite $H_0 = G \supset H_1 \supset \dots \supset H_m = \{0\}$ telle que chacun des groupes $G_i = H_{i-1}/H_i$ $(1 \leqslant i \leqslant m)$ soit isomorphe à un sous-groupe de R .

La première assertion résulte de la prop.9. Si G_i n'était pas isomorphe à un sous-groupe de R , il aurait, d'après la prop.8, un sous-groupe isolé autre que G_i et $\{0\}$; alors l'image réciproque de ce sous-groupe, pour l'homomorphisme canonique de H_{i-1} sur G_i , serait un sous-groupe isolé de H_{i-1} , donc de G , distinct de tous les H_j .

Définition 6. On dira qu'un groupe totalement ordonné G est de rang m si ses sous-groupes isolés (y compris G et $\{0\}$) sont au nombre de $m+1$. On dira qu'une valuation d'un corps K est de rang m si son groupe des ordres est de rang m .

Un groupe de rang 1 est donc un groupe isomorphe à un sous-groupe de R non réduit à $\{0\}$; et une valuation de rang 1 est une valuation dont le groupe des ordres est un tel groupe.

Remarque. Une valuation de rang 1 est quelquefois dite archimédienne.

[N-B : Cette dénomination est à proscrire, en raison de la confusion avec les "valuations archimédiennes" de la théorie des nombres, qui ne sont même pas des valuations au sens de ce chapitre (ce sont des valeurs absolues)] .

Proposition 10. Un corps K de rang $n > 0$ admet des valuations de rang n , et n'admet que des valuations de rang $\leq n$; il en est de même pour une extension K de dimension n d'un corps k si l'on ne considère que les valuations de K triviales sur k .

C'est une conséquence immédiate du coroll.2 de la prop.9, de la prop.7 du n°5, et du th.5 du n°4 .

7. Valuations de rang 1 .

Quand il s'agira désormais d'une valuation de rang 1, on supposera toujours qu'elle prend ses valeurs dans R ; comme toute valuation de rang 1 est équivalente à une valuation prenant ses valeurs dans R , cela ne restreint pas la généralité des raisonnements. Le groupe des ordres d'une valuation de rang 1 est alors, soit un sous-groupe partout dense de R, soit un sous-groupe discret de R qui est donc isomorphe à Z.

Définition 7. Une valuation sera dite discrète de rang 1 (ou, par abus de langage, discrète) si son groupe des ordres est isomorphe à Z ; une telle valuation sera dite normée si son groupe des ordres est Z .

Dans toute la suite de ce chapitre, nous dirons toujours "valuation discrète" pour "valuation discrète de rang 1 ".

Toute valuation discrète est équivalente à une valuation discrète normée et à une seule. Si ω est une valuation discrète d'un corps K , la restriction de ω à un sous-corps de K est, soit triviale, soit discrète ; dans ce dernier cas, ω peut être normée sans que sa restriction le soit.

Soit A l'anneau d'une valuation discrète normée ω d'un corps K ; on peut lui appliquer ce qui a été dit au n°1 sur les sous-A-modules de K . On voit ainsi qu'en dehors de K et de $\{0\}$, ces A-modules sont les ensembles déterminés par une relation $\omega(x) \geqslant n$, où $n \in Z$. Si p est un élément de K tel que $\omega(p)=1$, ces ensembles ne sont autres que les idéaux principaux fractionnaires $p^n A$; on dit souvent que p est une "uniformisante locale" de K pour A , ou pour ω , ou pour une place de K d'anneau A . En particulier, A est un anneau principal.

Remarque. On peut montrer que, réciproquement, tout anneau d'intégrité qui est à la fois local et principal est l'anneau d'une valuation discrète de son corps des fractions (v. exercice du § 5).

[N-B : Comme en effet un tel anneau est un anneau normal de Dedekind, donc que tout idéal premier y est maximal et qu'il n'a donc qu'un seul idéal premier, donc une seule valuation essentielle, le résultat en question est une conséquence triviale du §5, où il trouverait sa place tout naturellement si on tenait à le conserver dans le texte (dans la rédaction précédente, c'était la prop.7, p.25). Un exercice, et la remarque ci-dessu dans le texte, semblent suffisants au rédacteur (à moins que son prédécesseur n'en connaisse des applications intéressantes). Le rédacteur propose, à plus forte raison, de faire un exercice (à placer où ?) de la remarque p.26, 1.12-14, de la précédente rédaction (que La Tribu demandait de placer dans le texte)] .

Proposition 11. Deux valuations de rang 1 d'un corps K sont, soit équivalentes, soit étrangères.

En effet, leurs anneaux A, A' sont des anneaux maximaux d'après le coroll. de la prop.8 du n°6, donc on a $AA' = A = A'$ ou $AA' = K$.

Ce résultat permet d'appliquer le "théorème d'approximation" du n°3 chaque fois qu'on a affaire à un nombre fini de valuations de rang 1 .

Nous allons examiner en particulier le prolongement d'une valuation de rang 1 d'un corps K à une extension algèbrique de K . Nous poserons les définitions suivantes :

Définition 8. Soient ω une valuation d'un corps K, et K_0 un sous-corps de K ; soient $\Gamma = \omega(K^*)$ le groupe des ordres de ω , et $\Gamma_0 = \omega(K_0^*)$ celui de la valuation induite par ω sur K_0 . Si Γ_0 est un sous-groupe de Γ d'indice fini e , on dira que e est l'indice de ramification de ω par rapport à K_0, ou que ω est ramifiée d'indice e sur K_0 ; sinon, on dira que ω est ramifiée d'indice infini sur K_0 .

Si, dans ces conditions, φ est une place de K associée à ω , on dira aussi que φ est ramifiée d'indice e (resp. d'indice infini).

Définition 9. Soient φ une place d'un corps K , et K_0 un sous-corps de K ; soient k le corps des valeurs de φ , et k_0 celui de la place induite par φ sur K_0 (c'est-à-dire qu'on a $k_\infty = \varphi(K_\infty)$, $(k_0)_\infty = \varphi[(K_0)_\infty]$) . Si k est une extension algèbrique de k_0 de degré fini d , on dira que d est le degré local de K sur K_0 en φ , ou que φ a le degré local d sur K ; sinon on dira que K est de degré local infini sur K_0 en φ .

Si, dans ces conditions, ω est une valuation de K associée à φ, on dira que d est le degré local de K sur K_0 par rapport à ω, ou que ω a le degré local d sur K_0 ; de même dans le cas infini.

Bien entendu, les notions ci-dessus se conservent si on remplace la valuation ω, ou la place φ, par d'autres équivalentes, et ne dépendent donc que de l'anneau A de ω et de φ ; e est l'indice $[K^*:UK_0^*]$, où U est le groupe des éléments inversibles de A ; d'autre part, si $\mathfrak{p}$ est l'idéal maximal de A, et si $A_0=K_0\cap A$, $\mathfrak{p}_0=K_0\cap\mathfrak{p}$, d est le nombre d'éléments d'un système maximal $x_1,\dots,x_d$ d'éléments de A dont les images dans $A/\mathfrak{p}$ sont linéairement indépendantes sur $A_0/\mathfrak{p}_0$, c'est-à-dire tels que la relation $\sum_i t_i x_i \equiv 0$ mod. $\mathfrak{p}$, avec $t_i\in A_0$ $(1\leq i\leq d)$ entraîne $t_i\in\mathfrak{p}_0$ quel que soit i.

<u>Théorème 7</u>. <u>Soit</u> L <u>une extension algébrique de degré fini</u> n <u>d'un corps</u> K ; <u>soit</u> ω <u>une valuation de rang</u> 1 <u>de</u> K. <u>Alors les valuations de</u> L <u>qui prolongent</u> ω <u>sont de rang</u> 1, <u>sont en nombre fini</u>, <u>et sont de degré local et d'indice de ramifications finis par rapport à</u> K ; <u>si ces valuations sont</u> $\omega'_1,\dots,\omega'_h$, <u>et si</u> e_i <u>est l'indice de ramification de</u> ω'_i <u>sur</u> K, <u>et</u> d_i <u>son degré local</u>, <u>on a</u> $\sum_i d_i e_i \leq n$. <u>Si de plus</u> ω <u>est discrète</u>, <u>il en est de même des</u> ω'_i.

Soient A l'anneau de ω, Γ le groupe des ordres de ω. Soient $\omega'_1,\dots,\omega'_m$ des prolongements de ω à L en nombre fini, deux à deux inéquivalents. Pour chaque i, soient $x_{i,1},\dots,x_{i,m_i}$ des éléments de K^* dont les ordres $\omega'_i(x_{i,\mu})$ pour ω'_i appartiennent à des classes distinctes dans le groupe des ordres de ω'_i modulo Γ ; l'existence de tels éléments implique naturellement que l'indice de ramification de ω'_i est $\geq m_i$. Soient de même, pour chaque i, $y_{i,1},\dots,y_{i,r_i}$ des éléments de l'anneau de ω'_i tels que la relation $\omega'_i(\sum_\rho t_\rho y_{i,\rho})>0$, avec $t_\rho\in A$, implique $\omega(t_\rho)>0$ pour tout ρ ; leur existence implique que le degré local de ω' est $\geq r_i$.

On aura alors $\omega_i'(y_{i,\rho}) = 0$ pour tout ρ . Posons $\gamma_i = \max_\mu \omega_i'(x_{i,\mu})$. D'après le th.4' du n°4, il y aura des $x'_{i,\mu}$ tels que $\omega_i'(x'_{i,\mu}-x_{i,\mu}) > \gamma_i$, donc $\omega_i'(x'_{i,\mu}) = \omega_i'(x_{i,\mu})$, et que $\omega_j'(x'_{i,\mu}) > \gamma_j$ pour $j \neq i$; et il y aura des $y'_{i,\rho}$ tels que $\omega_i'(y'_{i,\rho}-y_{i,\rho}) > 0$, et $\omega_j'(y'_{i,\rho}) \geqslant 0$ pour $j \neq i$. Alors les $x'_{i,\mu}$, $y'_{i,\rho}$ auront les mêmes propriétés que les $x_{i,\mu}$, $y_{i,\rho}$; en remplaçant ceux-ci par ceux-là, on aura alors $\omega_i'(x_{j,\nu}) > \gamma_i$ et $\omega_i'(y_{j,\rho}) \geqslant 0$ chaque fois que $i \neq j$. On va montrer que, dans ces conditions, les $x_{i,\mu}y_{i,\rho}$ sont linéairement indépendants sur K ; cela impliquera que l'on a $\sum_i m_i r_i \leqslant n$, donc que les valuations inéquivalentes de L prolongeant ω sont en nombre $\leqslant n$ et satisfont à l'inégalité de notre théorème. En effet, supposons qu'on ait une relation

$$(1) \qquad \sum_i \sum_\mu \sum_\rho a_{i\mu\rho} x_{i,\mu} y_{i,\rho} = 0 ,$$

avec des $a_{i\mu\rho} \in K$ et non tous nuls ; et supposons par exemple que, parmi les $a_{i\mu\rho}$ pour lesquels $\omega(a_{i\mu\rho})$ est le plus petit possible, il y en ait un pour lequel $i=1$; en divisant la relation (1) par celui-là, on aura une relation analogue où cette fois tous les $a_{i\mu\rho}$ seront dans A et l'un des $a_{1\mu\rho}$ sera égal à 1 . Dans ces conditions, l'un au moins des termes de (1) pour lesquels $i=1$ aura pour ω_1' un ordre $\leqslant \gamma_1$; et tous les termes de (1) pour lesquels $i\neq 1$ auront pour ω_1' un ordre $> \gamma_1$; si donc γ est le plus petit des ordres, pour ω_1' , des termes de (1), les termes de (1) d'ordre γ seront tous relatifs à $i=1$. Supposons par exemple que l'un de ces termes soit $a_{111}x_{1,1}y_{1,1}$; si $a_{1\mu\rho}x_{1,\mu}y_{1,\rho}$ en est un autre, on aura $\omega_1'(x_{1,\mu})-\omega_1'(x_{1,1}) = \omega(a_{111}/a_{1\mu\rho}) \in \Gamma$, ce qui n'est possible, par définition des $x_{1,\mu}$, que si $\mu=1$; donc tous les termes de (1) d'ordre γ seront obtenus pour $i = \mu = 1$. En divisant (1) par $a_{111}x_{1,1}$, on aura donc une relation de la forme : $\sum_\rho b_\rho y_{1,\rho} + w = 0$, où w est une somme de termes dont les ordres pour ω'_1 sont tous >0 , où l'on a $b_\rho \in K$ et $\omega'_1(b_\rho y_{1,\rho}) \geqslant 0$, donc $\omega(b_\rho) \geqslant 0$, quel que soit ρ , et $b_1=1$. Mais cela est contraire à la définition des $y_{1,\rho}$. Il résulte en particulier de ce qui précède que l'indice de ramification e de tout prolongement ω' de ω à L est fini ; alors $\delta \rightarrow e\,\delta$ est un isomorphisme dans Γ du groupe ordonné Γ' des ordres de ω' ; donc ω' est de rang 1 , et discrète si ω est discrète ; de plus, si on suppose comme d'habitude que Γ est un sous-groupe de R (et non pas seulement isomorphe à un tel sous-groupe), il y a une valuation et une seule, équivalente à ω', prenant ses valeurs dans R , et qui prolonge ω , à savoir la valuation $f\circ\omega'$, où f est l'isomorphisme de Γ' dans R déterminé par $f(\delta) = (e\delta)/e$. Donc les ω' qui prolongent ω sont en nombre fini, et deux à deux inéquivalentes si on les assujettit à prendre leurs valeurs dans R .

Corollaire. Si L est une extension algèbrique d'un corps K , et ω une valuation de rang 1 de K , tout prolongement de ω à L est de rang 1 .

En effet, une telle valuation induit une valuation de rang 1 sur toute extension de K de degré fini contenue dans L ; il est immédiat dans ces conditions que son groupe des ordres satisfait à l'axiome d'Archimède (condition b de la prop.8, n°6).

Remarque. Dans les conditions du corollaire, ω peut être discrète sans que son prolongement à L le soit, si L est de degré infini.

8. <u>Topologies déterminées par les valuations de rang 1</u> .

Soit ω une valuation de rang 1 d'un corps K ; soit a un nombre réel >1 ; on posera, pour $x \in K^*$, $|x| = a^{-\omega(x)}$, et $|0| = 0$, $|\infty| = +\infty$. Alors l'application $x \to |x|$ de K dans R_+ est une <u>valeur absolue</u>, dont la donnée fait de K un <u>corps valué</u> (<u>Top.Géné.</u>,Chap.IX, §3, n°2) ; la topologie définie sur K par cette valeur absolue (loc.cit.) est identique à celle que nous avons associée à ω au début du n°3 ci-dessus. Réciproquement, pour qu'une valeur absolue $|x|$ sur un corps K détermine, au moyen de la formule $\omega(x) = -c \log|x|$ (où c est un nombre >0 quelconque), une valuation de K , il faut et il suffit évidemment qu'elle satisfasse à la condition :

(VM_{III}') $|x+y| \leqslant \sup(|x|,|y|)$ <u>quels que soient</u> x,y <u>dans</u> K .

Dans ce cas, $\omega(x)$ est une valuation de rang 1, bien définie à une équivalence près.

Il s'ensuit que tout corps K peut être complété par rapport à une valuation de rang 1, celle-ci se prolongeant par continuité, d'une manièr et d'une seule, au complété de K (prop.6 de <u>Top.Géné.</u>, Chap.IX, §3,n°2). On dira qu'un corps est <u>complet</u> par rapport à une valuation de rang 1 s'il l'est pour la valeur absolue correspondante.

<u>Remarque</u>. On dit parfois qu'une valeur absolue est "archimédienne" si elle ne satisfait pas à (VM_{III}'), "non-archimédienne" si elle y satisfait.

Une valuation de rang 1 est complètement déterminée par la donnée de la topologie qui lui est associée (ce qui, d'après le coroll. du th.5, n°4, n'est pas le cas pour les valuations quelconques). En effet :

<u>Proposition 12. Soit</u> A <u>l'anneau d'une valuation</u> ω <u>de rang</u> 1 <u>d'un corps</u> K <u>Alors, pour que</u> $x \notin A$, <u>il faut et il suffit que l'on ait</u> $\lim_{n \to +\infty} x^{-n} = 0$ <u>pour la topologie associée à</u> ω .

En effet, si $x \notin A$, on a $|x| > 1$, donc $\lim_{n \to +\infty} |x|^{-n} = 0$; si $x \in A$, on a $|x| \leqslant 1$, donc $\lim_{n \to +\infty} |x|^{-n}$ est 1 ou $+\infty$, et les x^{-n} ne peuvent tendre vers 0 .

Théorème 8. Soit K un corps complet par rapport à une valuation ω de rang 1 de K . Alors ω peut être prolongée d'une manière et d'une seule à toute extension algébrique L de K ; ce prolongement ω' est de rang 1 ; et, si le corps L est de degré fini sur K , il est complet par rapport à ω'.

Le prolongement est en tout cas possible, d'après le th.3 du n°1 ; pour en démontrer l'unicité, on peut supposer que L est de degré fini n sur K , puisqu'en tout cas L est réunion d'extensions de K de degré fini. Soit ω' un prolongement de ω à L ; d'après le th.7, il est de rang 1 . Pour éviter toute confusion, convenons de désigner par K_ω le corps K muni de sa structure de corps valué au moyen de ω , tandis que K désignera le même corps muni de sa seule structure algèbrique ; et définissons de même $L_{\omega'}$ et L . La valeur absolue définie par ω' sur L détermine sur L une structure d'espace vectoriel normé de dimension n sur K_ω , dont la structure topologique et la structure uniforme ne sont autres que celles de $L_{\omega'}$. Mais on sait (Esp. Vect.Topo...) qu'un tel espace, en tant qu'espa-ce vectoriel topologique sur K_ω , est isomorphe à K_ω^n ; si donc $x_1,\dots,x_n$ est une base de L sur K, l'application $(t_1,\dots,t_n) \to \sum t_i x_i$ de K_ω^n sur $L_{\omega'}$ est un isomorphisme au sens de la structure topologique et même au sens de la structure uniforme de ces espaces. La topologie de $L_{\omega'}$ est déterminée par là d'une manière unique à partir de la donnée de L et de ω ; d'après la prop.12, cela démontre l'unicité de ω' . Comme de plus K_ω^n est complet, il en est de même de $L_{\omega'}$.

[N.B : Le th.8 est essentiellement le lemme de Hensel ; joint au th.7, il permet de faire toute la théorie de la ramification. Pour la "relation des degrés" $\sum d_i e_i = n$ sous certaines hypothèses (p.ex. séparabilité), le rédacteur est partisant de la méthode qui utilise la théorie des algèbres commutatives : L étant extension de K de degré n, on considère L comme algèbre commutative sur K, et on étend le corps de base au complété K_ω de K par rapport à ω ; on obtient ainsi une algèbre commutative sur K_ω ; si elle est semi-simple, elle se décompose en somme directe de corps qui ne sont autres que les complétés $L_{\omega'_i}$ de L par rapport aux prolongements ω'_i de ω à L ; alors on a à démontrer que $[L_{\omega'_i} : K_\omega] = d_i e_i$, ce qui est le premier pas dans la théorie de la ramification strictement locale. Le rédacteur verrait volontiers celle-ci poussée assez loin, soit ici même, soit au Chap.III. Comme il est persuadé que tout cela a déjà été rédigé dans une rédaction ultérieure (Principe dit de Dieudonné), il renonce à pousser plus loin ses efforts sur la question, d'autant plus qu'il ne sait pas au juste ce qu'on a ici le droit de supposer acquis sur les algèbres commutatives. Sur la méthode en question, cf. les Algebraic Functions de Chevalley] .

§ 4. Eléments entiers sur un anneau.

Soit R un anneau, soumis comme toujours aux restrictions générales énoncées au début du Chap., mais qu'on ne suppose pas être anneau d'intégrité. Soient A un sous-anneau de R , et x un élément de R . Alors l'ensemble des $a \in A$ tels que $ax \in A$ est évidemment un idéal de A , qu'on conviendra une fois pour toutes (dans le reste de ce chapitre) de noter $\vartheta_A(x)$. D'autre part, $\mathfrak{A}$ l'idéal des relations algèbriques en x à coefficients dans A ; considérons, pour chaque polynome P de cet idéal, le coefficient dominant a_o ; l'ensemble des a_o, ou autrement dit l'ensemble des coefficients dominants a_o des relations $a_o x^n + a_1 x^{n-1} + \dots + a_n = 0$ $(a_i \in A)$ auxquelles satisfait x , est un idéal de A , qu'on notera $\Delta_A(x)$; en effet, si $b \in A$, le produit de cette relation par b est une relation analogue de coefficient dominant $a_o b$; et, si on a deux telles relations, de coefficients dominants a_o, b_o et de degrés respectifs n, m, en les multipliant respectivement par x^m et x^n et les ajoutant, on obtient une relation de degré $n+m$ et de coefficient dominant $a_o + b_o$. On a évidemment $\vartheta_A(x) \subset \Delta_A(x)$. Quand il n'y a pas de confusion possible, on écrira $\vartheta(x)$, $\Delta(x)$ au lieu de $\vartheta_A(x)$, $\Delta_A(x)$.

<u>Remarque</u>. Quand R est un anneau d'intégrité, les éléments non nul de $\vartheta_A(x)$ sont les $a \in A$ tels que x soit de la forme $x = b/a$ avec $b \in A$; aussi $\vartheta_A(x)$ s'appelle-t-il quelquefois alors (par abus de langage) l'idéal des dénominateurs de x relativement à A .

<u>Théorème 1</u>. <u>Soient</u> R <u>un anneau</u>, A <u>un sous-anneau de</u> R , x <u>un élément de</u> R . <u>Alors les propriétés suivantes sont équivalentes</u> :

a) $\Delta_A(x) = A$, <u>ou autrement dit</u> x <u>est racine d'un polynome unitaire</u> $x^n + a_1 x^{n-1} + \dots + a_n = 0$ <u>à coefficients</u> $a_i \in A$;

b) <u>l'anneau</u> $A[x]$ <u>est un module de type fini sur</u> A ;

c) <u>l'anneau</u> $A[x]$ <u>est contenu dans un sous-anneau</u> B <u>de</u> R <u>qui est un module de type fini sur</u> A ;

d) <u>il n'y a pas de spécialisation de</u> $A \cup \{x\}$ <u>qui soit finie sur</u> A <u>et non en</u> x ;

e) <u>on a</u> $x(\pi) \neq \infty$ <u>pour toute place</u> π <u>de</u> R <u>qui induit une spécialisation finie sur</u> A.

<u>Si de plus</u> R <u>est un corps, les propriétés ci-dessus sont équivalentes aux suivantes</u> :

f) <u>on a</u> $\omega(x) \geqslant 0$ <u>pour toute valuation</u> ω <u>de</u> R <u>qui est</u> $\geqslant 0$ <u>sur</u> A ;

g) x <u>est dans l'intersection des anneaux de valuation de</u> R <u>qui contiennent</u> A.

Si a) est vérifiée, on a $x^{n+p} = -a_1 x^{n+p-1} - \dots - a_n x^p$ pour tout $p \geqslant 0$, donc x^{n+p} appartient au A-module engendré par $\{1, x, \dots, x^{n+p-1}\}$; on voit alors, par récurrence sur p, que, pour $p \geqslant 0$, x^{n+p} appartient au module $M = A + Ax + \dots + Ax^{n-1}$, donc que $A[x] = M$; b) est donc vérifiée, ce qui entraîne c). Si c) est vérifiée, soit $A[x] \subset B = \sum_{i=1}^{m} Ab_i$; alors, pour $1 \leqslant i \leqslant m$, xb_i est dans B, donc de la forme $xb_i = \sum_{j=1}^{m} a_{ij} b_j$ $(a_{ij} \in A)$; c'est là un système de m équations linéaires et homogènes entre les b_i ; soit $D = \det(a_{ij} - \delta_{ij} x)$ le déterminant de ce système. On a alors $Db_i = 0$ pour tout i (Alg., Chap. III, §6, n°5, formule (22), donc $Db = 0$ quel que soit $b \in B$, d'où $D = 0$ puisque B est un anneau et que par suite $1 \in B$. Mais $\det(a_{ij} - \delta_{ij} x)$ est, au signe près, un polynome unitaire de degré m en x, à coefficients dans A. Dond c) entraîne a). Soit maintenant f une spécialisation finie de A ; étendons f à $A \cup \{x\}$ en prenant $f(x) = \infty$. Pour que ce soit là une spécialisation de $A \cup \{x\}$, il faut et il suffit, d'après la prop.6 du § 2, n°3, que, si (a_ι) est une famille d'éléments de A, et si les $P_i((X_\iota))$ sont des polynomes à coefficients dans Z, toute relation $P_0((a_\iota))x^n+P_1((a_\iota))x^{n-1}+\ldots+P_n((a_\iota)) = 0$ entraîne $P_0((f(a_\iota))) = 0$, ou, ce qui revient au même, $f[P((a_\iota))] = 0$. Il revient au même de dire que toute relation $a_0x^n+a_1x^{n-1}+\ldots+a_n = 0$ doit entraîner $f(a_0)=0$, ou encore que le noyau de f contient $\Delta_A(x)$. Il n'existe donc pas de telle spécialisation f si $\Delta_A(x) = A$, c'est-à-dire que a) entraîne d) ; si au contraire $\Delta_A(x) \neq A$, on obtient une telle spécialisation en prenant pour f l'homomorphisme canonique de A sur $A/\mathfrak{p}$, où $\mathfrak{p}$ est un idéal maximal de A contenant $\Delta_A(x)$. Donc d) entraîne a). L'équivalence de d) et e) résulte du théorème de prolongement (th.1 du § 2, n°4) ; l'équivalence de e) avec f) et g) quand R est un corps résulte du th.1 du § 3, n°1.

Définition 1. Les hypothèses et notations étant celles du th.1, x est dit entier sur A s'il vérifie a) ; en ce cas, une relation $x^n+a_1x^{n-1}+\ldots+a_n=0$ à laquelle satisfait x, à coefficients dans A, est dite une équation de dépendance intégrale pour x sur A.

Proposition 1. Soient R un anneau, A un sous-anneau de R ; l'ensemble B des éléments de R entiers sur A est un sous-anneau de R qui contient A. Si R est un corps, B est l'intersection des anneaux de valuation de R qui contiennent A.

La première assertion résulte immédiatement de l'équivalence de a) et e) du th.1, et de la prop.7 du § 2, n°3. La seconde résulte de l'équivalence de a) et g) du th.1.

NBR 060 68

Définition 2. Les hypothèses et notations étant celles de la prop.1, B s'appelle la fermeture intégrale de A dans R ; si $A = B$, A est dit intégralement fermé dans R ; si $B = R$, R est dit entier sur A.

Si A est anneau d'intégrité, la fermeture intégrale C de A dans son corps des fractions s'appelle la clôture intégrale de A ; si $A = C$, A est dit intégralement clos.

D'après la prop.1, pour qu'un anneau d'intégrité soit intégralement clos, il faut et il suffit qu'il soit intersection d'anneaux de valuation de son corps des fractions.

S Remarque : Une intersection d'anneaux de valuation d'un corps K n'est pas nécessairement un anneau ayant K pour corps des fractions. Par exemple, les anneaux de valuation de $k(X)$ qui contiennent le corps k ont une intersection réduite à k (exemple 3 du §3, n°1).

Exemples. [ici, prière de transcrire les exemples 1) et 2) de la rédaction précédente, p. 38-39].

Proposition 2 ("transitivité"). Soient A, B deux sous-anneaux d'un anneau R, tel que tout élément de B soit entier sur A. Alors tout élément de R entier sur B est entier sur A.

C'est immédiat en vertu de l'équivalence de a) et e) du th.1.

Proposition 3. Soient R, B, A trois anneaux tels que $R \supset B \supset A$; soit S une partie non vide de A, multiplicativement stable, ne contenant pas 0. Alors, si B est entier sur A, B_S est entier sur A_S ; si B est la fermeture intégrale de A dans R, B_S est celle de A_S dans R_S.

Rappelons, pour justifier cet énoncé, qu'on a convenu d'identifier A_S, B_S avec des sous-anneaux de R_S (v. la remarque qui suit le coroll.1 de la prop.2, §1) ; si φ est l'homomorphisme canonique de R dans R_S, on a $A_S = \varphi(A)\,\varphi(S)^{-1}$, $B_S = \varphi(B)\,\varphi(S)^{-1}$. Supposons B entier sur A ;

soit $\varphi(b)/\varphi(s)$ un élément de B_S, avec $b \in B$, $s \in S$; appliquant φ à une équation de dépendance intégrale pour b sur A, et divisant par $\varphi(s)^n$ si n est le degré de cette équation, on obtient une équation de dépendance intégrale pour $\varphi(b)/\varphi(s)$ sur A_S. Supposons que B soit la fermeture intégrale de A dans R ; soit $\varphi(x)/\varphi(s)$ un élément de R_S entier sur A_S, avec $x \in R$, $s \in S$; une équation de dépendance intégrale pour cet élément sur A_S sera de la forme :

$$\frac{\varphi(x)^n}{\varphi(s)^n} + \frac{\varphi(a_1)}{\varphi(s_1)} \frac{\varphi(x)^{n-1}}{\varphi(s)^{n-1}} + \dots + \frac{\varphi(a_n)}{\varphi(s_n)} = 0$$

avec $a_i \in A$, $s_i \in S$. En multipliant par $\varphi(s^n s_1 s_2 \dots s_n)$, on obtient une relation de la forme $\varphi(u)=0$, avec $u = s_o x^n + a'_1 x^{n-1} + \dots + a'_n$, $s_o \in S$, $a'_i \in A$; u est donc dans le noyau de φ, c'est-à-dire dans l'annulateur d'un élément s' de S ; on a donc $s'u = 0$, c'est-à-dire une relation de la forme $s''x^n + a''_1 x^{n-1} + \dots + a''_n = 0$ avec $s'' \in S$, $a''_i \in A$; en multipliant cette relation par s''^{n-1}, on obtient une équation de dépendance intégrale pour $s''x$ sur A, ce qui donne $b = s''x \in B$, et par suite $\varphi(x)/\varphi(s) = \varphi(b)/\varphi(ss'') \in B_S$.

Corollaire. <u>Soient</u> A <u>un anneau d'intégrité intégralement clos</u>, K <u>son corps des fractions</u>, S <u>une partie non vide de</u> A, <u>multiplicativement stable, ne contenant pas</u> 0. <u>Alors</u> A_S <u>est intégralement clos, et est l'intersection des anneaux des valuations de</u> K <u>qui sont</u> $\geqslant 0$ <u>sur</u> A <u>et</u> 0 <u>sur</u> S.

En prenant, dans la prop.3, $K = R = R_S$ et $B = A$, on voit que A_S est intégralement clos, donc intersection d'anneaux de valuation. Comme A_S est engendré par A et S^{-1}, il faut et il suffit, pour qu'une valuation de K soit $\geqslant 0$ sur A_S, quelle soit $\geqslant 0$ sur A et $\leqslant 0$ sur S, donc 0 sur S.

<u>Proposition 4. Soit</u> B <u>un anneau, entier sur un sous-anneau</u> A <u>de</u> B ; <u>alors, si</u> f <u>est un homomorphisme de</u> B <u>dans un anneau,</u> f(B) <u>est entier sur</u> f(A).

C'est immédiat par application de f à une équation de dépendance intégrale pour un élément quelconque de B sur l'anneau A .

<u>Corollaire. Soit</u> B <u>un anneau entier sur un sous-anneau</u> A ; <u>soient</u> $\mathfrak{q}$, $\mathfrak{q}'$ <u>deux idéaux premiers distincts de</u> B <u>tels que</u> $\mathfrak{q} \supset \mathfrak{q}'$. <u>Alors on a</u> $A \cap \mathfrak{q} \neq A \cap \mathfrak{q}'$.

Appliquant à B l'homomorphisme canonique de B sur $B/\mathfrak{q}'$, et tenant compte de la prop.4, on se ramène au cas où $\mathfrak{q}' = (0)$ et où B est un anneau d'intégrité. Soient K, L les corps des fractions de A et B ; tout élément de B est entier sur A , donc algèbrique sur K , donc L est algèbrique sur K . Soit π une place de L, finie et de noyau $\mathfrak{q}$ sur B ; si son noyau $A \cap \mathfrak{q}$ sur A était (0), elle serait triviale sur K , donc sur L d'après le coroll.1 du th.6, §3,n°5, et on aurait donc $\mathfrak{q} = (0)$.

<u>Proposition 5. Soit</u> A <u>un anneau d'intégrité intégralement clos ; soit</u> K <u>son corps des fractions. Alors, si</u> x <u>est un élément, entier sur</u> A , <u>d'un surcorps de</u> K , <u>le polynome minimal de</u> x <u>sur</u> K <u>a ses coefficients dans</u> A (et est donc le premier membre d'une équation de dépendance intégrale pour x sur A).

Remplaçant le surcorps en question par une extension convenable, on peut supposer qu'il contient,,non seulement x , mais toutes les racines x, x', x",... de son polynome minimal ; ce dernier est alors de la forme $[(X-x)(X-x)(X-x'')\dots]^q$, où q est une puissance de l'exposant caractéristique de K ; ses coefficients sont donc dans l'anneau engendré par x, x', x",... Mais x,x',x",... sont tous racines d'une équation de dépendance intégrale pour x sur A , et sont donc tous entiers sur A ; d'près la prop.1,il en est donc de même des coefficients du polynome minimal.

Corollaire 1. Soient A un anneau d'intégrité intégralement clos, K son corps des fractions, L une extension algèbrique séparable de K de degré fini. Alors, si x est un élément de L, entier sur A, la trace $Tr_{L/K}(x)$ et la norme $N_{L/K}(x)$ de x sur K sont dans A.

C'est immédiat d'après la prop.5, et le coroll.2 de la prop.9, Alg., Chap.V, § 10, n°6, ou bien en vertu de la définition de la norme et de la trace et d'un raisonnement analogue à celui de la démonstration de la prop.5.

Corollaire 2. Soient A un anneau d'intégrité, K son corps des fractions, L une extension algèbrique de K. Supposons que A soit intersection des des anneaux d'un ensemble Ω de valuations de rang 1 de K. Alors la fermeture intégrale B de A dans L est l'intersection des anneaux des valuations de L qui prolongent celles de Ω.

D'après la prop.1, B est en tout cas contenue dans cette intersection ; soit donc x un élément de celle-ci ; soit $x^n + c_1x^{n-1} + \dots + c_n = 0$ le polynome minimal de x sur K. Soit R l'anneau d'une valuation $\omega \in \Omega$; puisque ω est de rang 1, R est un sous-anneau maximal de K (coroll. de la prop.8, § 3, n°6). Soit ω' une valuation non triviale de L qui soit $\geqslant 0$ sur R ; d'après le coroll.1 du th.6, § 3, n°5, la valuation ω_1 qu'elle induit sur K est non triviale, donc l'anneau de ω_1 est $\neq K$, et, comme cet anneau contient R, c'est R, c'est-à-dire que ω_1 est équivalente à ω il s'ensuit que ω' est elle-même équivalente à un prolongement de ω à L, de sorte qu'on a $\omega'(x) \geqslant 0$ d'après l'hypothèse faite sur x. D'après la prop.1, il s'ensuit que x est entier sur R, donc, d'après la prop.5, que $c_i \in R$, c'est-à-dire $\omega(c_i) \geqslant 0$, pour $1 \leqslant i \leqslant n$. Comme il en est ainsi quel que soit $\omega \in \Omega$, on a donc $c_i \in A$ pour $1 \leqslant i \leqslant n$, et par suite $x \in B$.

<u>Remarque</u>. L'hypothèse du coroll.2 peut s'exprimer plus brièvement en disant que A est intersection de sous-anneaux maximaux de son corps des fractions.

[<u>N-B</u> : Le rédacteur présume que le coroll.2 cesse d'être vrai si on ne suppose pas que les valuations de Ω soient de rang 1, mais se trouve trop abruti pour s'en assurer. Il suggère qu'on insère une remarque sur ce point, avec éventuellement un contre-exemple, soit dans le corps de la remarque, soit en exercice].

[<u>N-B</u> : Conformément aux décisions du Congrès, les théorèmes "de Cohen-Seidenberg" sont à renvoyer en exercices. D'ailleurs le premier (prop.4, p.40 de la précédente rédaction) est <u>vachement trivial</u>, ainsi que son corollaire. On aimerait, par raison de symétrie, pouvoir dire que le second est vachement astucieux, mais ce serait excessif. Pour éclairer la lanterne du rédacteur ultérieur, il est à noter que, si on omet de la prop.8 (p.42-43, rédaction précédente) les hypothèses "A int.clos, A' entier sur A", alors $S \cap QA' = \emptyset$ est une condition nécessaire et suffisante pour qu'il existe un Q' tel qu'il est dit dans la proposition (en effet : $S \cap QA' = \emptyset$ équivaut à dire que l'idéal engendré par Q dans A'_S est $= (1)$; cela est nécessaire et suffisant pour qu'il existe une spécialisation finie f de A'_S nulle sur Q ; comme $S \supset A - Q$, le noyau de f sur A est exactement Q ; comme $S \supset A' - P'$, le noyau de f sur A' est contenu dans P')] .

[N-B : Voici encore un exerc. que le rédacteur vient de retrouver dans ses papiers ; il s'agit d'un résultat qui joue un rôle important dans les "Birational Correspondences" de Zariski : Soient R un anneau, A un sous-anneau de R, t un élément inversible de A ; soit x un élément de R entier sur $A[t]$, et tel qu'il existe des $a_i \in A$ pour lesquels $(1 + \sum_{i=1}^{m} a_i t^{-i})x$ soit entier sur $A[t^{-1}]$; alors x est entier sur A (en effet : pour toute place de R, finie sur A, ou bien t est fini, donc aussi x , ou bien t^{-1} devient 0, etc.)] .

§ 5. Anneaux normaux.

Dans toute la suite de ce chapitre, les anneaux qu'on étudiera seront des anneaux d'intégrité ; on désignera en général par A l'anneau qu'on étudie, par K son corps des fractions, par $\mathfrak{p}$ un idéal premier de A .

Par une <u>valuation de</u> A , on entendra toujours dans le reste de ce chapitre (par abus de langage) une valuation ω de K qui est $\geqslant 0$ sur A , c'est-à-dire dont l'anneau contient A ; et on conviendra une fois pour toutes que $\mathfrak{p}(\omega)$ désignera le "noyau" de ω sur A , c'est-à-dire l'ensemble des $x \in A$ tels que $\omega(x) > 0$.

1. <u>Préliminaires</u>. L'idéal $\mathfrak{d}_A(x)$ défini au début du § 4, et qu'en général on notera simplement $\mathfrak{d}(x)$, jouera un grand rôle dans ce qui suit ; sa définition revient à poser $\mathfrak{d}(x) = A \cap x^{-1}A$.

On se servira aussi de la définition suivante (cf. Alg...) :

<u>Définition 1. Etant donnés deux idéaux fractionnaires</u> $\mathfrak{a}$, $\mathfrak{b}$ <u>de</u> K <u>relativement à</u> A , <u>autres que</u> (0), <u>on désignera par</u> $\mathfrak{b} : \mathfrak{a}$ <u>l'ensemble des</u> $x \in K$ <u>tels que</u> $x\mathfrak{a} \subset \mathfrak{b}$.

Il est clair que $\mathfrak{b} : \mathfrak{a}$ est un sous-A-module de K ; de plus, si $a \in \mathfrak{a}$, $x\mathfrak{a} \subset \mathfrak{b}$ entraîne $x \in a^{-1}\mathfrak{b}$, donc $\mathfrak{b} : \mathfrak{a}$ est un idéal fractionnaire de K ; et, si $\mathfrak{a} \subset zA$, on a $z^{-1}\mathfrak{b} \subset \mathfrak{b} : \mathfrak{a}$, donc $\mathfrak{b} : \mathfrak{a} \neq (0)$.

On conviendra d'autre part (par abus de langage) de dire qu'un idéal premier $\mathfrak{p}$ de A est <u>minimal</u> s'il est autre que (0) et ne contient aucun idéal premier de A autre que $\mathfrak{p}$ et (0).

<u>Lemme 1. Soit</u> $\mathfrak{p}$ <u>un idéal premier de</u> A, <u>tel que</u> $A_{\mathfrak{p}}$ <u>soit l'anneau d'une valuation discrète</u> ω <u>de</u> K . <u>Alors</u> $\mathfrak{p}$ <u>est un idéal premier minimal de</u> A ; <u>on a</u> $\mathfrak{p} = \mathfrak{p}(\omega)$; <u>si</u> $\omega(x) < 0$, <u>on a</u> $\mathfrak{d}(x) \subset \mathfrak{p}$; <u>si</u> ω' <u>est une valuation non triviale de</u> A , <u>non équivalente à</u> ω , <u>on a</u> $\mathfrak{p}(\omega') \not\subset \mathfrak{p}$; <u>enfin, si</u> ω <u>est normée, il y a</u> $p \in \mathfrak{p}$ <u>tel que</u> $\omega(p)=1$.

Supposons ω normée, et soit p une "uniformisante locale" (§ 3, n°8) c'est-à-dire un élément de K tel que $\omega(p)=1$; tout idéal de $A_{\mathfrak{p}}$ est alors de la forme $p^n A_{\mathfrak{p}}$ (§ 3, n°8) ; comme le seul de ces idéaux qui soit premier est $pA_{\mathfrak{p}}$, il s'ensuit, d'après le th. 3 du § 2, n°5, que $\mathfrak{p}$ est un idéal premier minimal de A. Le même théorème montre qu'on a $pA_{\mathfrak{p}} = \mathfrak{p} A_{\mathfrak{p}}$ et $\mathfrak{p} = A \cap (\mathfrak{p} A_{\mathfrak{p}})$, que $\mathfrak{p} A_{\mathfrak{p}}$ est l'idéal maximal de $A_{\mathfrak{p}}$, et par suite que $\mathfrak{p} = \mathfrak{p}(\omega)$. On a $p \in A_{\mathfrak{p}}$, donc p est de la forme $p = p'/a$, avec $p' \in A$, $a \in A - \mathfrak{p}$; alors on a $a \in A_{\mathfrak{p}}$ et $a \notin \mathfrak{p} A_{\mathfrak{p}}$, donc $\omega(a)=0$ et $\omega(p')=1$; en remplaçant p par p' on a donc un élément p de $\mathfrak{p}$ tel que $\omega(p)=1$. Si $\omega(x) < 0$ et $ax \in A$ avec $a \in A$, on a $\omega(a) > 0$, donc $a \in A \cap (\mathfrak{p} A_{\mathfrak{p}}) = \mathfrak{p}$. Enfin, soit ω' une valuation non triviale de A telle que $\mathfrak{p}(\omega') \subset \mathfrak{p}$; comme $\mathfrak{p}$ est minimal, on a $\mathfrak{p}(\omega') = \mathfrak{p}$; si donc π est une place de K associée à ω, son noyau sur A est $\mathfrak{p}$; par suite, le domaine de la spécialisation induite par π sur A est K_{∞}, le prolongement canonique de cette spécialisation est π, et l'anneau de π est $A_{\mathfrak{p}}$.

<u>Lemme 2</u>. <u>Supposons que A soit intersection d'une famille (A_ι) de sous-anneaux maximaux A_ι de K ; soit $\mathfrak{p}$ un idéal premier de A. Alors, pour que $A : \mathfrak{p} \neq A$, il faut et il suffit qu'il existe un $z \in K - A$ tel que $\vartheta(z) \supset \mathfrak{p}$; si z est tel, on a $\vartheta(z) = \mathfrak{p}$, et $A_{\mathfrak{p}}$ est l'anneau d'une valuation discrète normée v de K telle que $v(z) = -1$.</u>

Dire que $A : \mathfrak{p} \neq A$ revient à dire qu'il existe $z \in C(A) \cap (A : \mathfrak{p})$, c'est-à-dire $z \in C(A)$ tel que $z\mathfrak{p} \subset A$ ou encore $\mathfrak{p} \subset \vartheta(z)$. Alors il y a un anneau A_ι tel que $z \notin A_\iota$; d'après le coroll. de la prop. 8 du § 3, n°6, A_ι est l'anneau d'une valuation ω de rang 1 ; on a $\omega(z) < 0$, et ω est $\geqslant 0$ sur A ; puisque le groupe des ordres de ω satisfait à l'axiome d'Archimède (condition b) de la prop. 8 du § 3, n°6), il s'ensuit que, si $a \in A^*$, il y a un entier $n > 0$ tel que $\omega(az^n) < 0$, donc tel que $az^n \notin A$. Mais, puisque $z\mathfrak{p} \subset A$, $az^m \in \mathfrak{p}$ entraîne $az^{m+1} \in A$. Si donc, pour $a \in A^*$, on considère la suite $(a, az, az^2, \ldots)$, on voit qu'il existe un $n \geqslant 0$ tel que $az^n \in A - \mathfrak{p}$ et que $az^\nu \in \mathfrak{p}$ pour $0 \leqslant \nu < n$; comme ces conditions déterminent évidemment n d'une manière unique, posons $n = v(a)$. Si de même $b \in A^*$, $v(b)=m$, donc si $bz^m \in A - \mathfrak{p}$ et $bz^\mu \in \mathfrak{p}$ pour $0 \leqslant \mu < m$, on aura $(ab)z^{m+n} \in A - \mathfrak{p}$; si $0 \leqslant \rho < m+n$, peut être mis sous la forme $\rho = \nu + \mu$ avec $0 \leqslant \nu \leqslant n$, $0 \leqslant \mu \leqslant m$, et $\nu < n$ ou $\mu < m$, donc on a $(ab)z^\rho \in \mathfrak{p}$; autrement dit, on a $v(ab)=v(a)+v(b)$. Si d'autre part on a $n \leqslant m$, on aura $(a+b)z^\nu \in \mathfrak{p}$ pour $0 \leqslant \nu < n$, donc $v(a+b) \geqslant n$. Il s'ensuit, d'après la prop. 2 du §3, n°2, que v peut être prolongée à une valuation de K à valeurs dans Z, valuation qu'on désignera encore par v. Par définition, v est 0 sur $A - \mathfrak{p}$, et > 0 sur $\mathfrak{p}$; en particulier, si $a \in A^*$ et $v(a)=n$, on a $v(az^n)=0$; donc $v(z)=-1$; par suite, v est normée. Soit $x=b/a \in K^*$, avec $a \in A^*$, $b \in A^*$, et $v(x) \geqslant 0$; posons $v(a)=n$, $v(b)=m$, donc $m \geqslant n$, d'où $a'=az^n \in A - \mathfrak{p}$, $b'=bz^n \in A$, et $x = b'/a'$; on a donc $x \in A_\mathfrak{p}$; réciproquement, $x \in A_\mathfrak{p}$ entraîne évidemment $v(x) \geqslant 0$. Donc $A_\mathfrak{p}$ est l'anneau de v. Enfin, $a \in \mathfrak{d}(z)$ entraîne $v(a) \geqslant 1$, donc $a \in \mathfrak{p}$; puisque par hypothèse on a $\mathfrak{d}(z) \supset \mathfrak{p}$, on a donc $\mathfrak{d}(z) = \mathfrak{p}$.

2. Anneaux normaux.

Définition 2. Soient A un anneau d'intégrité, et K son corps des fractions. Un ensemble Ω de valuations discrètes normées de K sera dit un ensemble de définition de A si A est l'intersection des anneaux des valuations $\omega \in \Omega$, et si, quel que soit $a \in A^*$, il n'y a qu'un nombre fini de $\omega \in \Omega$ tels que $\omega(a) > 0$. Un anneau qui admet un ensemble de définition sera dit normal.

On notera qu'alors, si $x \in K^*$, il n'y a qu'un nombre fini de $\omega \in \Omega$ tels que $\omega(x) \neq 0$, comme on le voit en écrivant $x = b/a$, $a \in A^*$, $b \in A^*$.

<u>Proposition 1. Soient</u> A <u>un anneau normal</u>, Ω <u>un ensemble de définition de</u> A ; <u>soit</u> $z \in K - A$, <u>et soit</u> $\mathfrak{p}$ <u>un idéal premier de</u> A <u>contenant</u> $\vartheta(z)$. <u>Alors il existe</u> $\omega \in \Omega$ <u>tel que</u> $\omega(z) < 0$ <u>et</u> $\mathfrak{p}(\omega) \subset \mathfrak{p}$.

Par hypothèse, les $\omega \in \Omega$ tels que $\omega(z) < 0$ forment un ensemble fini non vide $\{\omega_1, \ldots, \omega_m\}$. Si on avait $\mathfrak{p}(\omega_i) \not\subset \mathfrak{p}$ pour $1 \leqslant i \leqslant m$, il y aurait, pour $1 \leqslant i \leqslant m$, un $a_i \in \mathfrak{p}(\omega_i)$ tel que $a_i \notin \mathfrak{p}$. Soit $a = a_1 a_2 \ldots a_m$; quel que soit l'entier N, on aura $a^N \notin \mathfrak{p}$, donc $a^N \notin \vartheta(z)$ ou $a^N z \notin A$. Mais d'autre part on a $\omega(a^N z) \geqslant 0$ pour tout $\omega \in \Omega$ distinct des ω_i, et, pour chaque i, $\omega_i(a^N z) \geqslant 0$ dès que $N \geqslant |\omega_i(z)|$ puisque $\omega_i(a) \geqslant 1$. Donc on a $\omega(a^N z) \geqslant 0$ quel que soit $\omega \in \Omega$, c'est-à-dire $a^N z \in A$, dès que N est au moins égal au plus grand des $|\omega_i(z)|$; il y a contradiction.

<u>Proposition 2. Soient</u> A <u>un anneau normal</u>, Ω <u>un ensemble de définition de</u> A. <u>Soit</u> $\mathfrak{p}$ <u>un idéal premier de</u> A <u>tel que</u> $A_{\mathfrak{p}}$ <u>soit l'anneau d'une valuation discrète normée</u> v <u>de</u> K. <u>Alors on a</u> $v \in \Omega$; <u>il existe</u> $z \in K$ <u>tel que</u> $v(z) = -1$, <u>et que</u> $\omega(z) \geqslant 0$ <u>pour tout</u> $\omega \in \Omega$ <u>autre que</u> v ; <u>et on a alors</u> $\vartheta(z) = \mathfrak{p}$.

Soit $u \in K$ tel que $v(u) = -1$; d'après le lemme 1 du n°1, on a $\vartheta(u) \subset \mathfrak{p}$; d'après la prop. 1, il y a donc $\omega \in \Omega$ tel que $\mathfrak{p}(\omega) \subset \mathfrak{p}$; d'après le lemme 1 du n°1, ω est donc équivalente à v, d'où $\omega = v$ puisque toutes deux sont normées. Les ω autres que v tels que $\omega(u) < 0$ forment un ensemble fini $\{\omega_1, \ldots, \omega_m\}$; d'après le lemme 1 du n°1, on a $\mathfrak{p}(\omega_i) \not\subset \mathfrak{p}$; donc, pour tout i, il y a un $a_i \in \mathfrak{p}(\omega_i)$ tel que $a_i \notin \mathfrak{p}$. Soit $a = a_1 a_2 \ldots a_m$; on a $a \notin \mathfrak{p}$, donc (lemme 1) $v(a) = 0$, et $\omega_i(a) \geqslant 1$ pour tout i ; en posant $z = a^N u$, on aura donc

 77

$v(z)=-1$, et $\omega_i(z) \geqslant 0$ pour N assez grand, donc, pour N assez grand, $\omega(z) \geqslant 0$ quel que soit $\omega \in \Omega$ autre que v . Dans ces conditions, pour que $a \in \vartheta(z)$, il faut et il suffit que l'on ait $v(a) \geqslant 1$; on a donc bien $\vartheta(z) = \mathfrak{p}$.

Définition 3. Une valuation discrète normée v de l'anneau normal A est dite essentielle si l'anneau de v est de la forme $A_{\mathfrak{p}}$, $\mathfrak{p}$ étant un idéal premier de A .

$\mathfrak{p}$ ne peut être autre alors que le noyau de v sur A .

La prop.2 montre que l'ensemble V des valuations essentielles d'un anneau normal A est contenu dans tout ensemble de définition Ω de A .

Proposition 3. Si A est un anneau normal, l'ensemble V de ses valuations essentielles est un ensemble de définition de A .

Il faut montrer que, pour tout $u \in K-A$, il y a $v \in V$ telle que $v(u) < 0$. Soit Ω un ensemble de définition de A ; soit $u \in K-A$; soit $\{\omega_1,\dots,\omega_m\}$ l'ensemble fini non vide des $\omega \in \Omega$ tels que $\omega_i(u) < 0$. Soit $\mathfrak{p}$ un élément minimal de l'ensemble fini formé par les idéaux $\mathfrak{p}(\omega_i)$, ordonné par inclusion ; en changeant au besoin la numérotation des ω_i , on aura donc $\mathfrak{p}(\omega_i) = \mathfrak{p}$ pour $1 \leqslant i \leqslant h$, et $\mathfrak{p}(\omega_j) \not\subset \mathfrak{p}$ pour $h < j \leqslant m$, h étant un entier tel que $1 \leqslant h \leqslant m$. Pour $h < j \leqslant m$, il y aura donc un $a_j \in \mathfrak{p}(\omega_j)$ tel que $a_j \notin \mathfrak{p}$; soit $a = \prod_{h<j\leqslant m} a_j$, d'où $\omega_j(a) > 0$ pour $h < j \leqslant m$, et $a \notin \mathfrak{p}$, donc $\omega_i(a)=0$ pour $1 \leqslant i \leqslant h$. En posant $u'=a^N u$, on aura donc $\omega_i(u') < 0$ pour $1 \leqslant i \leqslant h$, et $\omega_j(u') \geqslant 0$ pour N assez grand ; autrement dit, en remplacant u par u' avec N assez grand, on peut supposer que $m = h$. Si $p \in \mathfrak{p}$, on a $\omega_i(p) \geqslant 1$ pour $1 \leqslant i \leqslant h$; il s'ensuit que l'on a $u\mathfrak{p}^N \subset A$ dès que N est au moins égal au plus grand des entiers $|\omega_i(u)|$ pour $1 \leqslant i \leqslant h$.

Soit alors n le plus petit entier $\geqslant 1$ tel que $u\mathfrak{p}^n \subset A$, c'est-à-dire tel que $\vartheta(u) \supset \mathfrak{p}^n$; on va démontrer, par récurrence sur n, que l'une des valuations ω_i est essentielle. Si $n=1$, cela est contenu dans le lemme 2 du n°1. Si $n>1$, on a $u\mathfrak{p} \not\subset A$, donc il existe $p \in \mathfrak{p}$ tel que $u_1 = up \notin A$; l'ensemble des $\omega \in \Omega$ tels que $\omega(u_1) < 0$ est alors une partie non vide de $\{\omega_1, \ldots, \omega_h\}$; mais, puisque $u\mathfrak{p}^n \subset A$, on a $u_1 \mathfrak{p}^{n-1} \subset A$; en vertu de l'hypothèse de récurrence, l'une des ω_i est donc essentielle.

<u>Proposition 4.</u> <u>Soit</u> $\mathfrak{p}$ <u>un idéal premier d'un anneau normal</u> A. <u>Alors il existe une valuation essentielle</u> v <u>de</u> A <u>telle que</u> $\mathfrak{p}(v) \subset \mathfrak{p}$.

Soit $p \in \mathfrak{p}$, $p \neq 0$; on a $\vartheta(p^{-1}) = pA \subset \mathfrak{p}$ .. La conclusion résulte alors de la prop.1 appliquée à $\mathfrak{p}$, à p^{-1}, et à l'ensemble des valuations essentielles de A qui en est un ensemble de définition d'après la prop.3 .

<u>Corollaire 1.</u> <u>Soit</u> $\mathfrak{p}$ <u>un idéal premier d'un anneau normal</u> A. <u>Pour que</u> $A_{\mathfrak{p}}$ <u>soit l'anneau d'une valuation essentielle de</u> A, <u>il faut et il suffit que</u> $\mathfrak{p}$ <u>soit un idéal premier minimal de</u> A.

Appliquons la prop.4 ; si $\mathfrak{p}$ est minimal, $\mathfrak{p}(v) \subset \mathfrak{p}$ entraîne $\mathfrak{p}(v) = \mathfrak{p}$. La réciproque résulte du lemme 1 du n°1 .

<u>Corollaire 2.</u> <u>Soit</u> $\mathfrak{p}$ <u>un idéal premier d'un anneau normal</u> A, <u>contenu dans un idéal principal</u> $(a)=aA$ <u>de</u> A <u>autre que</u> A ; <u>alors on a</u> $\mathfrak{p}=aA$, <u>et</u> $\mathfrak{p}$ <u>est un idéal premier minimal.</u>

L'hypothèse $\mathfrak{p} \subset aA$ équivaut à $a^{-1}\mathfrak{p} \subset A$, c'est-à-dire à $\mathfrak{p} \subset \vartheta(a^{-1})$. D'après le lemme 2, on a alors $\mathfrak{p} = \vartheta(a^{-1})$, c'est-à-dire $\mathfrak{p} = aA$, et $A_{\mathfrak{p}}$ est l'anneau d'une valuation essentielle de A ; $\mathfrak{p}$ est donc minimal d'après le coroll.1 .

Proposition 5. Soient v_i $(1 \leqslant i \leqslant h)$ des valuations essentielles distinctes, en nombre fini h, d'un anneau normal A ; soient m_i $(1 \leqslant i \leqslant h)$ des entiers. Alors il existe $x \in K^*$ tel que $v_i(x) = m_i$, et que $w(x) \geqslant 0$ pour toute valuation essentielle w de A distincte des v_i.

D'après la prop.3, l'ensemble V des valuations essentielles de A est un ensemble de définition de A ; donc, d'après la prop.2, si $v \in V$, il existe $z \in K^*$ tel que $v(z)=-1$, et $w(z) \geqslant 0$ pour tout $w \in V$ autre que v. Soit donc, pour $1 \leqslant i \leqslant h$, z_i tel que $v_i(z_i) = -1$ et $w(z_i) \geqslant 0$ pour $w \in V$, $w \neq v_i$. Alors, si tous les m_i sont < 0, on satisfera aux conditions imposées en prenant $x = \sum_{i=1}^{h} z_i^{-m_i}$. Pour passer de là au cas général, choisissons, pour chaque i, un $a_i \in \mathfrak{P}(v_i)$ autre que 0, et soit $a = a_1 a_2 \ldots a_h$; on aura $v_i(a) \geqslant 1$ pour $1 \leqslant i \leqslant h$, et $w(a) \geqslant 0$ pour tout $w \in V$ autre que les v_i. Posons, dans ces conditions, $m_i' = m_i - Nv_i(a)$, N étant pris assez grand pour que tous les m_i' soient < 0 ; déterminons x' tel que $v_i(x') = m_i'$, $w(x') \geqslant 0$ pour w distinct des v_i ; alors $x = a^N x'$ satisfait aux conditions imposées.

Remarque. Dans la prop.5, on ne peut en général remplacer la condition $w(x) \geqslant 0$ par la condition plus stricte $w(x)=0$. Les anneaux pour lesquels le problème plus strict ainsi posé admet toujours une solution sont les anneaux factoriels (§).

3. Diviseurs dans les anneaux normaux.

Dans ce n°, on conviendra de désigner une fois pour toutes par A un anneau normal et par V l'ensemble des valuations essentielles de A ; d'après le coroll.1 de la prop.4, n°3, V est en correspondance biunivoque avec l'ensemble des idéaux premiers minimaux de A.

Proposition 6. Soit $\mathfrak{a} \neq (0)$ un idéal fractionnaire de K relativement à l'anneau normal A. Pour tout $v \in V$, posons $n(\mathfrak{a}, v) = \inf_{z \in \mathfrak{a}} v(z)$.

Alors les $v \in V$ **tels que** $n(\mathfrak{a}, v) \neq 0$ **sont en nombre fini.**

Par définition d'un idéal fractionnaire, il y a $x \in K^*$ tel que $\mathfrak{a} \subset xA$; si de plus $y \in \mathfrak{a}$, $y \neq 0$, on aura $xA \subset \mathfrak{a} \subset yA$, d'où $v(x) \leqslant n(\mathfrak{a}, v) \leqslant v(y)$ pour tout $v \in V$. On a donc $n(\mathfrak{a}, v) = 0$ chaque fois que $v(x) = v(y) = 0$.

A l'idéal $\mathfrak{a}$, on peut donc faire correspondre l'élément $(n(\mathfrak{a}, v))$ dans le groupe $Z^{(V)}$, somme directe des groupes des ordres des valuations $v \in V$. Nous conviendrons de donner à ce groupe sa structure de groupe ordonné, en prenant pour éléments positifs les $(n(v))$ tels que $n(v) \geqslant 0$ quel que soit v . Ce groupe est canoniquement isomorphe au groupe abélien libre engendré par les $v \in V$, par l'isomorphisme qui, à tout générateur $v \in V$ de ce dernier groupe, fait correspondre l'élément $(n(v))$ du premier pour lequel $n(v) = 1$, $n(w) = 0$ pour $w \neq v$. Pour des raisons de commodité, c'est le groupe abélien libre engendré par les $v \in V$ qu'on considérera dans ce qui suit ; on conviendra de l'écrire multiplicativement, on l'ordonnera en y transportant la structure d'ordre naturelle de $Z(V)$, c'est-à-dire en y prenant pour éléments positifs les éléments $\prod_{v \in V} v^{n(v)}$ avec $n(v) \geqslant 0$ quelque soit v .

Définition 4. On appelle diviseur d'un anneau normal A tout élément du groupe abélien libre (noté multiplicativement) engendré par les valuations essentielles de A . Ce groupe sera ordonné en posant $\prod_{v \in V} v^{n(v)} \succcurlyeq 0$ quand $n(v) \geqslant 0$ quel que soit $v \in V$. Les diviseurs $\succcurlyeq 0$ seront dits entiers . Si D, D' sont deux diviseurs, on dira que D est multiple de D', et que D' divise D , si $D \succcurlyeq D'$.

Le groupe des diviseurs est réticulé ; on notera par p.p.c.m. et p.g.c.d. les lois de composition sup et inf dans ce groupe.

Définition 5. *Avec les notations de la prop. 6, le diviseur* $\prod_{v \in V} v^{n(\mathfrak{a},v)}$ *sera appelé le diviseur associé à* $\mathfrak{a}$ *et sera noté* $D(\mathfrak{a})$.

En particulier, si $x \in K^*$, on aura $D((x)) = D(xA) = \prod_{v \in V} v^{v(x)}$.

Proposition 7. *Pour tout* $v \in V$, *on a* $D(\mathfrak{p}(v)) = v$.

En effet, d'après la prop. 5 du n°2, quel que soit $w \neq v$ dans V, il existe $x \in A^*$ tel que $v(x)=1$, donc $x \in \mathfrak{p}(v)$, et $w(x)=0$.

Proposition 8. *Soient* $\mathfrak{a}$, $\mathfrak{b}$ *deux idéaux fractionnaires de* K *(relativement à* A*), autres que* (0) *; alors* $\mathfrak{a} \supset \mathfrak{b}$ *entraîne que* $D(\mathfrak{b})$ *est multiple de* $D(\mathfrak{a})$. *Si* $\mathfrak{a} \subset A$, $D(\mathfrak{a})$ *est un* ~~idéal~~ diviseur *entier, et réciproquement. Pour que* $D(\mathfrak{a})=1$, *il faut et il suffit que* $\mathfrak{a}$ *soit contenu dans* A *et ne soit contenu dans aucun idéal premier minimal de* A.

La première assertion résulte de la définition de $D(\mathfrak{a})$, $D(\mathfrak{b})$. Dire que $D(\mathfrak{a})$ est entier signifie que $n(\mathfrak{a},v) \geqslant 0$ pour tout $v \in V$, c'est-à-dire que $v(a) \geqslant 0$ pour tout $v \in V$ et tout $a \in \mathfrak{a}$, donc que tout $a \in \mathfrak{a}$ est dans A. Enfin, si $\mathfrak{a} \subset A$, dire que $D(\mathfrak{a}) \neq 1$ équivaut à dire qu'il existe $v \in V$ tel que $n(\mathfrak{a},v) \geqslant 1$, c'est-à-dire tel que $v(a) \geqslant 1$ pour tout $a \in \mathfrak{a}$, donc, puisque $\mathfrak{a} \subset A$, que $\mathfrak{a} \subset \mathfrak{p}(v)$.

Corollaire. *Si* $\mathfrak{p}$ *est un idéal premier non minimal de* A, *on a* $D(\mathfrak{p}) = 1$.

En effet, $\mathfrak{p}$ ne peut évidemment être contenu dans un idéal premier minimal.

Remarque. Ce cas se présente effectivement ; par exemple, on verra plus loin que, si k est un corps, $k[X,Y]$ est un anneau normal ; dans cet anneau, l'idéal (X) est premier et n'est pas minimal, car il contient strictement l'idéal premier engendré par X et Y. Il s'ensuit que, dans un anneau normal, $D(\mathfrak{b})$ peut être multiple de $D(\mathfrak{a})$ sans que l'on ait

82

La propriété essentielle des anneaux normaux est que l'application $\mathfrak{a} \longrightarrow D(\mathfrak{a})$ de l'ensemble des idéaux fractionnaires $\neq (0)$ dans le groupe des diviseurs se comporte d'une manière très simple vis-à-vis des lois de composition qui opèrent dans le premier de ces ensembles. Nous connaissons quatre lois de cette sorte : les trois premières sont celles qui associent à deux idéaux $\mathfrak{a}, \mathfrak{b}$ les idéaux $\mathfrak{a} \cap \mathfrak{b}$, $\mathfrak{a}+\mathfrak{b}$ et $\mathfrak{b} : \mathfrak{a}$, respectivement ; la dernière se définit (cf. Alg...) associant à $\mathfrak{a}, \mathfrak{b}$ l'idéal fractionnaire $\mathfrak{a} \perp \mathfrak{b}$ engendré par l'ensemble $\mathfrak{a}\mathfrak{b}$ des produits ab, où $a \in \mathfrak{a}$, $b \in \mathfrak{b}$; comme désormais ce dernier ensemble n'aura plus à intervenir au cours de ce chapitre, nous convien-drons à partir de maintenant de désigner par $\mathfrak{a}\mathfrak{b}$, non pas cet ensemble, mais l'idéal fractionnaire qu'il engendre, c'est-à-dire (Alg...) l'ensem-ble des éléments $\sum_i a_i b_i$ avec $a_i \in \mathfrak{a}$, $b_i \in \mathfrak{a}$.

<u>Théorème 1.</u> <u>Si</u> $\mathfrak{a}, \mathfrak{b}$ <u>sont des idéaux fractionnaires de K autres que</u> (0) <u>(relativement à l'anneau normal</u> A), <u>on a</u> :

$$D(\mathfrak{a}\mathfrak{b}) = D(\mathfrak{a})D(\mathfrak{b}) , \qquad D(\mathfrak{a}+\mathfrak{b}) = \mathrm{pgcd}\,[D(\mathfrak{a}),D(\mathfrak{b})]$$
$$D(\mathfrak{a}\cap\mathfrak{b}) = \mathrm{ppcm}\,[D(\mathfrak{a}), D(\mathfrak{b})] , \qquad D(\mathfrak{b} : \mathfrak{a}) = D(\mathfrak{b})D(\mathfrak{a})^{-1} .$$

Les deux premières relations résultent immédiatement des définitions, ainsi que le fait que, dans chacune des deux dernières, le premier membre est multiple du second. Soit $v \in V$; posons $r = n(\mathfrak{a},v)$, $s = n(\mathfrak{b},v)$, et soient $a \in \mathfrak{a}$, $b \in \mathfrak{b}$ tels que $v(a) = r$, $v(b) = s$. Pour achever de démontrer la troisième relation, il faut construire un $x \in \mathfrak{a} \cap \mathfrak{b}$ tel que $v(x) = \max(r,s)$. D'après la prop. 5 du n°2, il y a un $x \in K^*$ tel que $w(x) = \max[w(a),w(b)]$ pour $w = v$ et pour tous les $w \in V$ en nombre fini tels que $w(a) > 0$ ou $w(b) > 0$, et tel que $w(x) \geqslant 0$ pour tout autre $w \in V$. Alors, quel que soit $w \in V$, on a $w(x) \geqslant w(a)$, c'est-à-dire $w(x/a) \geqslant 0$; on a donc $x/a \in A$, donc $x \in aA \subset \mathfrak{a}$, et de même $x \in \mathfrak{b}$, donc $x \in \mathfrak{a} \cap \mathfrak{b}$. De même, pour achever de démontrer la dernière relation

NDR 060 83

il faut construire un $x \in \mathfrak{b} : \mathfrak{a}$ tel que $v(x) = s-r$. D'après la prop.5 du n°2, il y a un $x \in K^*$ tel que $w(x) = w(b)-n(\mathfrak{a},w)$ pour $w = v$ et pour tous les $w \in V$ en nombre fini tels que $w(b) > 0$ ou $n(\mathfrak{a},w) < 0$, et $w(x) \geqslant 0$ pour tout autre $w \in V$. Alors, si $y \in \mathfrak{a}$, on a $w(x) \geqslant w(b)-w(y)$, c'est-à-dire $w(xy/b) \geqslant 0$, pour tout $w \in V$, donc $xy \in bA \subset \mathfrak{b}$, donc $x \in \mathfrak{b} : \mathfrak{a}$.

Corollaire 1. Avec les notations du th.1, les relations $A : \mathfrak{a} = A : \mathfrak{b}$ et $D(\mathfrak{a}) = D(\mathfrak{b})$ sont équivalentes.

D'après le th.1, la première relation entraîne la seconde. D'autre part, les éléments $\neq 0$ de $A : \mathfrak{a}$ sont les $x \in K^*$ tels que $v(ax) \geqslant 0$ pour tout $a \in \mathfrak{a}$ et tout $v \in V$, donc tels que $v(x) \geqslant -n(\mathfrak{a},v)$ pour tout $v \in V$. Donc $A:\mathfrak{a}$ est complétement déterminé par la donnée de $n(\mathfrak{a},v)$ pour tout v, ou autrement dit par $D(\mathfrak{a})$.

Corollaire 2. $\mathfrak{a} \longrightarrow D(\mathfrak{a})$ est une application de l'ensemble des idéaux fractionnaires $\neq (0)$ de K sur le groupe des diviseurs de A ; elle induit sur le groupe ordonné P^* des idéaux fractionnaires principaux $\neq (0)$ de K un isomorphisme croissant de ce groupe dans celui des diviseurs de A.

Le premier point résulte aussitôt de la prop.7 et du th.1. Il est clair que $xA \longrightarrow D(xA)$ est un homomorphisme ; pour que $D(xA) = D(yA)$, il faut et il suffit que $v(x) = v(y)$ quel que soit v, c'est-à-dire que x/y soit inversible dans A, ou encore que $xA = yA$. Le fait que l'isomorphisme $xA \longrightarrow D(xA)$ est croissant résulte de la prop.8 .

4. Anneaux factoriels.

Le coroll.2 du th.1 montre en particulier que le groupe P^* des idéaux principaux fractionnaires $\neq (0)$ d'un anneau normal est isomorphe à un groupe abélien libre ; un cas particulier important est celui où il est, en tant que groupe ordonné (et non pas seulement en tant que groupe) isomorphe à un groupe $Z^{(I)}$.

<u>Définition 6</u>. <u>Soient</u> A <u>un anneau d'intégrité</u>, K <u>son corps des fractions</u> P^* <u>le groupe ordonné des idéaux principaux fractionnaires de K relativement à</u> A ; <u>on dira que</u> A <u>est factoriel si</u> P^* <u>est isomorphe à un groupe</u> $Z^{(I)}$.

En d'autres termes, A est factoriel s'il existe une famille (p_ι) d'éléments de A ayant la propriété suivante : tout $x \in K^*$ peut s'écrire d'une manière et d'une seule sous la forme

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

où u est un élément inversible de A , et où les n_ι sont des entiers, tous nuls sauf un nombre fini d'entre eux, et tous $\geqslant 0$ chaque fois que $x \in A^*$. Le groupe P^* étant alors réticulé, toutes les propriétés de divisibilité démontrées en algèbre (Alg.,Chap...) concernant le pgcd, le ppcm, les éléments étrangers, etc., s'appliquent aux anneaux factoriels ; la famille (p_ι) étant comme ci-dessus, il est clair que tout p_ι est un "élément extrémal" de A (Alg.,...), et que réciproquement tout élément extrémal est de la forme up_ι , où u est inversible dans A , c'est-à-dire est associé à un p_ι et à un seul.

Dans ces conditions, A est normal. En effet, pour tout $x \in K^*$, soit $v_\iota(x)=n_\iota$ l'exposant de p_ι dans l'expression (1) de x ; et soit $v_\iota(0) = +\infty$. D'après l'unicité de (1), on a $v_\iota(xy) = v_\iota(x)+ v_\iota(y)$ quels que soient x, y . Par hypothèse, $x \in A$ entraîne $v_\iota(x) \geqslant 0$ quel que soit ι ; la réciproque est évidente. Il s'ensuit que, pour $x \in A$, $x \in p_\iota^{n_A}$ est équivaut à $v_\iota(x) \geqslant n$; on en conclut aussitôt que, pour $x \in A$, $v_\iota(x+y) \geqslant \min[v_\iota(x), v_\iota(y)]$; d'après la prop.2 du §3, n°2, la même propriété reste valable alors quels que soient x,y dans K ; donc les v_ι sont des valuations discrètes de A et forment un ensemble de définition de A , qui est donc normal. Le centre de v_ι est l'idéal principal $p_\iota A$; d'après le coroll.2 de la prop.4, n°2, c'est donc un un idéal premier minimal ; par suite, v_z est une valuation essentielle de A . Comme d'ailleurs tout ensemble de définition de A contient toutes les valuations essentielles de A (prop.2 du n°2), on en conclut que l'ensemble des v_z est l'ensemble V des valuations essentielles de A ; et les idéaux $p_z A$ sont les idéaux premiers minimaux de A .

Réciproquement, si A est normal et si tout idéal premier minimal de A est principal, il résulte de la prop.7 du n°3 et du coroll.2 du th.1 du n°3 que $xA \rightarrow D(xA)$ est un isomorphisme du groupe ordonné P^* sur le groupe des diviseurs de A , donc que A est factoriel. Par suite :

Théorème 2. Pour qu'un anneau d'intégrité A soit factoriel, il faut et il suffit qu'il soit normal et que tout idéal premier minimal de A soit principal.

Corollaire 1. Si A est factoriel, et si (1) donne la décomposition unique des éléments de K^* en éléments extrémaux p_z de A , l'ensemble des idéaux premiers minimaux de A est formé des $p_z A$, et la valuation essentielle $v_z(x)$ de noyau $p_z A$ sur A donne l'exposant $n_z = v_z(x)$ de p_z dans la décomposition (1) de x .

Corollaire 2. Dans un anneau factoriel A , tout idéal principal aA autre que A et (0) est à la fois l'intersection et le produit de puissances d'idéaux premiers minimaux en nombre fini.

Qu'il en soit le produit résulte de ce qui précède ; qu'il soit alors aussi l'intersection de ces mêmes idéaux est immédiat, et est d'ailleurs contenu dans Alg....

5. Anneaux de Dedekind.

Théorème 3. Soient A un anneau normal, K son corps des fractions. Alors les propriétés suivantes sont équivalentes :

a) <u>$D(\mathfrak{a}) = D(\mathfrak{b})$ entraîne $\mathfrak{a} = \mathfrak{b}$; autrement dit, $\mathfrak{a} \rightarrow D(\mathfrak{a})$ est une application biunivoque de l'ensemble des idéaux fractionnaires de K autres que (0) (relativement à A) sur le groupe des diviseurs de A</u> ;

b) <u>toute valuation non triviale de A est équivalente à une valuation essentielle</u> ;

c) <u>tout idéal premier de A autre que (0) est minimal</u> ;

d) <u>tout idéal premier de A autre que (0) est maximal</u>.

Tout d'abord, c) et d) reviennent tous deux à dire qu'il n'existe pas d'idéaux premiers $\mathfrak{p} \neq (0)$, $\mathfrak{p}' \neq (0)$ dans A tels que $\mathfrak{p} \supset \mathfrak{p}'$, et sont donc bien équivalentes. S'il en est ainsi, le noyau sur A de toute valuation ω de A est un idéal premier minimal $\mathfrak{p}$, donc ω est équivalente à la valuation essentielle de noyau $\mathfrak{p}$ (lemme 1 du n°1) ; comme, réciproquement, tout idéal premier de A est le noyau sur A d'une valuation de A (th.2 du § 3, n°1), b) et c) sont équivalentes. D'après le coroll. de la prop.8, n°3, a) entraîne c). Enfin, supposons c) vérifiée ; et soit d'abord $\mathfrak{a}$ tel que $D(\mathfrak{a})=1$; alors, d'après la prop.8 du n°3, on a $\mathfrak{a} \subset A$; si $\mathfrak{a}$ était $\neq A$, il serait contenu dans un idéal premier de A (à savoir dans un idéal maximal, en vertu du th.2, Alg., Chap.I, §8, no7), qui serait ~~maxi~~ minimal d'après c) ; d'après la prop.8 du n°3, cela est impossible, donc on a $\mathfrak{a} = A$. Soient alors $\mathfrak{a}$, $\mathfrak{b}$ tels que $D(\mathfrak{a}) = D(\mathfrak{b})$; d'après le th.1 du n°3, on a $D((\mathfrak{a} \cap \mathfrak{b}) : \mathfrak{a}) = 1$, donc $(\mathfrak{a} \cap \mathfrak{b}) : \mathfrak{a} = A$ d'après ce qu'on vient de démontrer, d'où $1 \in (\mathfrak{a} \cap \mathfrak{b}) : \mathfrak{a}$ c'est-à-dire $\mathfrak{a} \subset \mathfrak{a} \cap \mathfrak{b}$ ou encore $\mathfrak{a} \subset \mathfrak{b}$; on a donc de même $\mathfrak{b} \subset \mathfrak{a}$, donc $\mathfrak{a} = \mathfrak{b}$.

<u>Corollaire</u>. <u>Si</u> <u>est un idéal fractionnaire autre que</u> (0) <u>d'un anneau</u> A <u>jouissant des propriétés</u> a),b),c),d) <u>du th.3</u>, $\mathfrak{a}$ <u>est l'ensemble des</u> $x \in K$ <u>tels que</u> $v(x) \geq n(\mathfrak{a}, v)$ <u>quelle que soit la valuation essentielle</u> v <u>de</u> A .

En effet, soit $\mathfrak{a}' = A:\mathfrak{a}$; d'après le th.1 du n°3 et le th.3, on a $D(\mathfrak{a}') = D(\mathfrak{a})^{-1}$ et $\mathfrak{a} = A:\mathfrak{a}'$; cette dernière relation signifie que la relation $x \in \mathfrak{a}$ équivaut à $xx' \in A$ quel que soit $x' \in \mathfrak{a}'$, donc à $v(x) \geqslant -n(\mathfrak{a}',v) = n(\mathfrak{a},v)$ quelle que soit $v \in V$.

Le corollaire du th.3 s'exprime parfois brièvement en disant que, pour un tel anneau A , tout idéal $\mathfrak{a}$ peut être défini par des "conditions valuatives" .

Définition 7. Un anneau A est dit anneau de Dedekind si c'est un anneau d'intégrité normal jouissant des propriétés équivalentes a), b), c), d) du th.3 .

D'après le th.1 du n°3 et le th.3, si A est un anneau de Dedekind, $\mathfrak{a} \longrightarrow D(\mathfrak{a})$ est un isomorphisme du monoïde des idéaux fractionnaires non nuls de K (pour la loi $\mathfrak{a}\mathfrak{b}$) sur le groupe des diviseurs ; le monoïde en question est donc un groupe. La réciproque de ce résultat est vraie ; pour la démontrer, nous aurons besoin d'un résultat auxiliaire :

Proposition 9.- Si A est un anneau d'intégrité, K son corps des fractions, et $\mathfrak{a}$, $\mathfrak{b}$ deux idéaux fractionnaires tels que $\mathfrak{a}\mathfrak{b} = A$, les idéaux $\mathfrak{a}$, $\mathfrak{b}$ sont des A-modules de type fini, c'est-à-dire engendrés par un nombre fini d'éléments.

Par hypothèse, on a $1 = \sum_i a_i b_i$, avec $a_i \in \mathfrak{a}$, $b_i \in \mathfrak{b}$. Soit a un élément quelconque de $\mathfrak{a}$; on aura $a = a(\sum a_i b_i) = \sum a_i(ab_i)$; comme $\mathfrak{a}\mathfrak{b} = A$, on a $ab_i \in A$ quel que soit i ; donc les a_i engendrent $\mathfrak{a}$.

Corollaire. Tout anneau de Dedekind est "noethérien", c'est-à-dire que tout idéal y est de type fini.

Proposition 10. Soient A un anneau d'intégrité, K son corps des fractions. Pour que A soit un anneau de Dedekind, il faut et il suffit que le monoïde M des idéaux fractionnaires non nuls de K (relativement à A) soit un groupe.

On a déjà vu que c'est nécessaire. Supposons donc que M soit un groupe. D'après la prop.9, tout idéal de K est alors de type fini ; il s'ensuit que, si M est ordonné par inclusion, toute partie non vide de M a un élément maximal (Alg.,Chap...) ; ce fait, joint à la propriété de M d'être réticulé, entraîne que M est un groupe ordonné isomorphe à un groupe $Z^{(I)}$ (Alg...) ; soit $\mathfrak{a} \longrightarrow (\varphi_i(\mathfrak{a})) \in Z^{(I)}$ un isomorphisme de M sur $Z^{(I)}$; les φ_i sont donc des homomorphismes de M dans Z , tels que, pour $\mathfrak{a} \in M$, tous les $\varphi_i(\mathfrak{a})$ soient nuls sauf un nombre fini d'entre eux ; $\mathfrak{a} \subset \mathfrak{b}$ est équivalent à $\varphi_i(\mathfrak{a}) \leqslant \varphi_i(\mathfrak{b})$ quel que soit i , et en particulier $\mathfrak{a} \subset A$ est équivalent à $\varphi_i(0) \leqslant 0$ quel que soit i . Soit $\mathfrak{p}_i$ l'idéal défini par $\varphi_i(\mathfrak{p}_i)=-1$, $\varphi_K(\mathfrak{p}_i)=0$ pour $K \neq i$; c'est un idéal maximal de A , et réciproquement tout idéal maximal de A est l'un des $\mathfrak{p}_i$; tout idéal de A est produit de puissances d'idéaux $\mathfrak{p}_i$, et ne peut donc être premier s'il n'est l'un des $\mathfrak{p}_i$, puisqu'en vertu de l'isomorphisme entre M et $Z^{(I)}$ tous ces produits de puissances sont distincts. Posons maintenant $v_i(x)=-\varphi_i(xA)$ pour $x \in K^*$, et $v_i(0)=+\infty$; il est immédiat que v_i est une valuation de K ; comme $x \in A$ équivaut à $v_i(x) \geqslant 0$ quel que soit i , les v_i forment un ensemble de définition de A . Donc A est normal et satisfait à la condition d) du th.3 .

D'après le th.3, et le th.1 du n°3, si A est un anneau de Dedekind, l'inverse d'un idéal fractionnaire $\mathfrak{a} \neq (0)$ dans le groupe M des idéaux fractionnaires est l'idéal $A : \mathfrak{a}$, qui sera donc désormais noté $\mathfrak{a}^{-1}$. Dans le groupe M , on écrira naturellement $\mathfrak{a}^{-n}=(\mathfrak{a}^{-1})^n$, et $\mathfrak{a}^0 = A$.

Théorème 4. Soient A un anneau de Dedekind, et K son corps des fractions ; soient $\mathfrak{p}_i$ les idéaux premiers de A autres que (0). Alors tout idéal fractionnaire non nul de K, relativement à A, peut se mettre d'une manière et d'une seule sous la forme $\mathfrak{a} = \prod_i \mathfrak{p}_i^{n_i}$, où les n_i sont des entiers tous nuls sauf un nombre fini d'entre eux, et tous $\geqslant 0$ si $\mathfrak{a} \subset A$. Si en même temps on a $\mathfrak{b} = \prod_i \mathfrak{p}_i^{m_i}$, alors on a :

$$\mathfrak{a}\mathfrak{b} = \prod_i \mathfrak{p}_i^{n_i+m_i} \quad ; \quad \mathfrak{a}+\mathfrak{b} = \prod_i \mathfrak{p}_i^{\min(n_i,m_i)} ,$$

$$\mathfrak{a}\cap\mathfrak{b} = \prod_i \mathfrak{p}_i^{\max(n_i,m_i)} \quad , \quad \mathfrak{b}:\mathfrak{a} = \prod_i \mathfrak{p}_i^{m_i-n_i}$$

Enfin, si v_i est la valuation essentielle de A, de noyau $\mathfrak{p}_i$ sur A, et si $x \in K^*$, $v_i(x)$ est l'exposant n_i de $\mathfrak{p}_i$, dans l'expression $xA = \prod_i \mathfrak{p}_i^{n_i}$ de l'idéal xA ; et toute valuation non triviale de A est équivalente à l'une des v_i.

Ce sont là des conséquences immédiates de ce qui précède, à savoir du th.3, et du th.1 et de la prop.7 du n°3.

Nous allons examiner maintenant les conséquences pour les anneaux de Dedekind de la prop.5 du n°2 ; cette proposition, traduite au moyen du th.4 dans le langage propre à ces anneaux, donne ce qui suit :

Proposition 11. Soit $\mathfrak{a}$ un idéal fractionnaire $\neq (0)$ relativement à un anneau de Dedekind A, et soient $\mathfrak{p}_i$ des idéaux premiers de A en nombre fini. Alors il existe $x \in \mathfrak{a}$ tel que $x \notin \mathfrak{a}\mathfrak{p}_i$ quel que soit i.

Corollaire 1. Soient $\mathfrak{a}$ un idéal fractionnaire $\neq (0)$, et $\mathfrak{b}$ un idéal entier $\neq (0)$, relativement à l'anneau de Dedekind A. Alors il existe un $x \in \mathfrak{a}$ tel que les idéaux entiers $(xA)\mathfrak{a}^{-1}$ et $\mathfrak{b}$ soient étrangers.

Cet énoncé est équivalent à la prop.11 : il suffit de prendre pour les $\mathfrak{p}_i$, dans celle-ci, les idéaux premiers qui divisent $\mathfrak{b}$.

90

Corollaire 2. Soient $\mathfrak{a}$, $\mathfrak{a}'$ deux idéaux fractionnaires non nuls relativement à l'anneau de Dedekind A . Alors, si $\mathfrak{a} \supset \mathfrak{a}'$, il existe $x \in K$ tel que $\mathfrak{a} = \mathfrak{a}' + xA$; si $\mathfrak{a} \subset \mathfrak{a}'$, il existe $x \in K$ tel que $\mathfrak{a} = \mathfrak{a}' \cap xA$.

Dans le premier cas, on prendra $x \in \mathfrak{a}$ tel que $(xA)\mathfrak{a}^{-1}$ soit étranger à $\mathfrak{a}'\mathfrak{a}^{-1}$; dans le second, on prendra $x = y^{-1}$, avec $y \in \mathfrak{a}^{-1}$ tel que $(yA)\mathfrak{a}$ soit étranger à $\mathfrak{a}'^{-1}\mathfrak{a}$.

Corollaire 3. Si $\mathfrak{a}$ est un idéal entier $\neq (0)$ de l'anneau de Dedekind A , il existe $x \in K^*$ tel que $\vartheta(x) = \mathfrak{a}$.

En effet, cela équivaut à $\mathfrak{a} = A \cap x^{-1}A$; c'est donc un cas particulier de la seconde partie du coroll.2 .

Corollaire 4. Soient $\mathfrak{a}$ un idéal fractionnaire $\neq (0)$, et $\mathfrak{b}$ un idéal entier $\neq (0)$, relativement à un anneau de Dedekind A . Alors le A-module $\mathfrak{a}/\mathfrak{a}\mathfrak{b}$, quotient des sous-A-modules $\mathfrak{a}$ et $\mathfrak{a}\mathfrak{b}$ de K , est monogène et isomorphe à $A/\mathfrak{b}$; tout $a \in \mathfrak{a}$ tel que $(aA)\mathfrak{a}^{-1}$ soit étranger à $\mathfrak{b}$ détermine un générateur de ce module.

Un tel $a \in \mathfrak{a}$ étant choisi par application du coroll.1, posons $\mathfrak{m} = (aA)\mathfrak{a}^{-1}$; on a alors $\mathfrak{b} + \mathfrak{m} = A$, donc il existe $b \in \mathfrak{b}$ et $m \in \mathfrak{m}$ tels que $b+m = 1$. Soit alors $x \in \mathfrak{a}$; on sait que $b+m = 1$. Soit alors $x \in \mathfrak{a}$; on aura $x = x(b+m) \equiv xm \pmod{\mathfrak{a}\mathfrak{b}}$, et $xm \in \mathfrak{a}\mathfrak{m} = aA$, donc $y = xm/a \in \mathfrak{a}$, et $x \equiv ya \pmod{\mathfrak{a}\mathfrak{b}}$; autrement dit, l'image de A dans $\mathfrak{a}/\mathfrak{a}\mathfrak{b}$ par l'application composée de l'homomorphisme $y \longrightarrow ya$ de A dans $\mathfrak{a}$, et de l'homomorphisme canonique de $\mathfrak{a}$ sur $\mathfrak{a}/\mathfrak{a}\mathfrak{b}$, est un homomorphisme de A sur $\mathfrak{a}/\mathfrak{a}\mathfrak{b}$; ce dernier module est donc monogène. Pour achever la démonstration, il faut montrer que le noyau de cet homomorphisme est $\mathfrak{b}$. Supposons donc, avec les notations ci-dessus, qu'on ait $ya \in \mathfrak{a}\mathfrak{b}$; cela donne $(yA)(aA)\mathfrak{a}^{-1} \subset \mathfrak{b}$, d'où $y\mathfrak{m} \subset \mathfrak{b}$, d'où $ym \in \mathfrak{b}$, d'où $y = y(b+m) \in \mathfrak{b}$; et il est clair que réciproquement $y \in \mathfrak{b}$ entraîne $ya \in \mathfrak{a}\mathfrak{b}$.

[N-B : Le coroll.2, peut-être même 3, pourrait à la rigueur être renvoyés en exercices ; le coroll.4 est d'une grande importance en théorie des nombres et doit en tout cas être maintenu].

D'autre part, dans un anneau de Dedekind, la prop.5 du n°2 peut être généralisée comme suit :

<u>Proposition 12</u>. <u>Soient</u> A <u>un anneau de Dedekind</u>, <u>et</u> K <u>son corps des fractions</u> ; <u>soient</u> v_i <u>des valuations normées de</u> A, <u>distinctes</u>, <u>en nombre fini</u> h ; <u>pour chaque</u> i, <u>soit</u> $x_i \in K$ <u>et</u> $m_i \in Z$; <u>il existe alors un</u> $x \in K$ <u>tel que</u> $v_i(x-x_i) = m_i$ <u>pour tout</u> i, <u>et que</u> $w(x) \geqslant 0$ <u>pour toute valuation</u> w <u>de</u> K <u>non équivalente à l'une des</u> v_i.

Comme dans la démonstration du th.4' du §3, n°3, posons $x = \sum_i x_i t_i$, d'où $x - x_i = x_i(t_i - 1) + \sum_{j \neq i} x_j t_j$; x satisfera aux conditions imposées pourvu que les t_i satisfassent aux conditions $v_i(t_i-1) = m_i - v(x_i)$, $v_j(t_i) > m_j - v_j(x_i)$, $w(t_i) \geqslant -w(x_i)$ pour tout i, tout $j \neq i$, et toute valuation normée w, autre que les v_i. En tenant compte de ce qu'on a $w(x_i) = 0$ sauf pour un nombre fini de valuations w, on voit que la détermination de chacun des t_i est un problème du type suivant. Soient $w_0, w_1, \ldots, w_k$ des valuations normées distinctes de A en nombre fini ; soient $m_0, m_1, \ldots, m_k$ des entiers ; il faut déterminer t tel que $w_0(t-1) = m_0$, $w_i(t) \geqslant m_i$ pour $1 \leqslant i \leqslant k$, et $w(t) \geqslant 0$ pour toute autre valuation normée w. Si $m_0 < 0$, la première condition équivaut à $w_0(t) = m_0$, et il n'y a qu'à appliquer la prop.5 du n°2 ; on peut donc supposer $m_0 \geqslant 0$; on peut aussi supposer $m_i \geqslant 0$ pour $1 \leqslant i \leqslant k$, car on rend le problème plus strict en remplaçant l'un de ces m_i par un entier plus grand. Soit $\mathfrak{p}_i$ le noyau de w_i sur A, pour $0 \leqslant i \leqslant k$; soit $\mathfrak{q} = \mathfrak{p}_0^{m_0}$, et soit $\mathfrak{a} = \prod_{i=1}^{k} \mathfrak{p}_i^{m_i}$; alors tout revient à déterminer

$t \in A$ tel que $t \equiv 1 \bmod. \mathfrak{q}$, et $t \equiv 0 \bmod. \mathfrak{a}$. Mais $\mathfrak{q}$ et $\mathfrak{a}$ sont étrangers, donc on a $\mathfrak{q} + \mathfrak{a} = A$; donc il existe $q \in \mathfrak{q}$, et $t \in \mathfrak{a}$, tels que $q+t = 1$.

<u>Corollaire. Soient</u> $\mathfrak{a}_1, \dots, \mathfrak{a}_h$ <u>des idéaux</u> $\neq (0)$ <u>d'un anneau de Dedekind</u> A, <u>et</u> $x_1, \dots, x_h$ <u>des éléments de</u> A. <u>Pour qu'il existe</u> $x \in A$ <u>tel que</u> $x \equiv x_i \bmod. \mathfrak{a}_i$ <u>pour tout</u> i, <u>il faut et il suffit que l'on ait</u> $x_i \equiv x_j \bmod. \mathfrak{a}_i + \mathfrak{a}_j$ <u>quels que soient</u> i,j.

C'est évidemment nécessaire. Supposons ces conditions satisfaites ; soient $\mathfrak{p}_\mu$ $(1 \leqslant \mu \leqslant m)$ tous les idéaux premiers qui divisent au moins l'un des $\mathfrak{a}_i$. Pour chaque μ, soit $\mathfrak{p}_\mu^{n_\mu}$ la plus haute puissance de $\mathfrak{p}_\mu$ qui divise l'un des $\mathfrak{a}_i$; soit $\mathfrak{a}_{i(\mu)}$ l'un des $\mathfrak{a}_i$ qu'elle divise, et soit $y_\mu = x_{i(\mu)}$. Pour tout i, $x_i - y_\mu$ appartient à l'idéal $\mathfrak{a}_i + \mathfrak{a}_{i(\mu)}$; cet idéal est multiple de la plus haute puissance de $\mathfrak{p}_\mu$ qui divise $\mathfrak{a}_i$; donc la relation $x \equiv y_\mu \bmod \mathfrak{p}_\mu^{n_\mu}$ entraîne que, pour chaque i, $x - x_i$ est multiple de la plus haute puissance de $\mathfrak{p}_\mu$ qui divise $\mathfrak{a}_i$. Le problème est donc ramené au système de congruences $x - y_\mu \equiv 0 \bmod. \mathfrak{p}_\mu^{n_\mu}$, qui a une solution en vertu de la prop.12.

<u>Remarque</u>. Il y a une autre démonstration du coroll. de la prop.12 [cf. précédente rédaction p.61 : en exercice !].

[N.B : La Tribu prescrivait au rédacteur de "raccourcir le théorème chinois" : il s'en avoue incapable (à moins de prendre "raccourcir" en sens qu'il n'a pas cru devoir envisager)].

<u>Proposition 13. Pour qu'un anneau d'intégrité</u> A <u>soit principal, il faut et il suffit que ce soit un anneau de Dedekind factoriel</u>.

C'est suffisant ; car si A est anneau de Dedekind, les idéaux fractionnaires relativement à A forment un groupe engendré par les idéaux premiers minimaux de A ; si donc ceux-ci sont principaux, c'est-à-dire

NBR 080 93

si A est factoriel, tout idéal de A sera principal. Réciproquement, il a été démontré dans la $I^{è}$ partie (Alg...) que tout anneau d'intégrité principal répond à la définition des anneaux factoriels ; dans un tel anneau A , d'après le coroll.1 du th.2, n°4, tous les idéaux principaux qui sont premiers sont minimaux, et comme il n'y a pas d'autre idéal premier que ceux-là, A est anneau de Dedekind.

Pour mémoire : <u>Proposition. Soient</u> K <u>un corps, et</u> A <u>l'intersection d'anneaux de valuations discrètes</u> v_i <u>de</u> K <u>en nombre fini ; alors</u> A <u>est un anneau principal dont les seuls idéaux premiers non nuls sont les noyaux des</u> v_i <u>sur</u> A .

Soient $v_1,\dots,v_h$ les valuations en question, qu'on peut supposer normées et distinctes les unes des autres ; d'après la prop.11 du § 3, n°7, elles sont indépendantes deux à deux. Si donc $x \in K^*$, il y a, d'après le th.4 du § 3, n°3, un $a \in K^*$ tel que $v_i(a-x) > v_i(x)$, et par suite $v_i(a) = v_i(x)$, chaque fois que $v_i(x) > 0$, et $v_j(a) \geqslant 0$ chaque fois que $v_j(x) \leqslant 0$; on a donc $a \in A^*$, et d'autre part $v_i(a/x) \geqslant 0$ quel que soit i , donc $b = a/x \in A^*$, d'où $x = a/b$. Dans ces conditions, A est un anneau normal ; comme d'ailleurs, toujours d'après le même théorème, il y a, quel que soit i, un $x \in K^*$ tel que $v_i(x) < 0$ et $v_j(x) \geqslant 0$ pour tout $j \neq i$, A n'est pas intersection des anneaux des v_j autres que v_i ; d'après la prop.3 du n°2, il s'ensuit que toutes les v_i sont des valuations essentielles de A . Soit $p_i' \in K^*$ tel que $v_i(p_i')=1$; toujours d'après le même théorème, il y a p_i tel que $v_i(p_i-p_i') > 1$, donc $v_i(p_i)=1$, et $v_j(p_i-1) > 0$, donc $v_j(p_i)=0$, pour $j \neq i$; il est clair alors que le noyau de v_i sur A est l'idéal principal p_iA ; donc A est factoriel. Supposons qu'il y ait un idéal premier $\mathfrak{p} \neq (0)$ dans A , autre que les p_iA ; comme les p_iA sont minimaux, on a $\mathfrak{p} \not\subset p_iA$ quel que soit i ; donc, pour tout i , il y a un $x_i \in \mathfrak{p}$ tel que $x_i \notin p_iA$.

Soit $x = \sum_i x_i q_i$, avec $q_i = p_1 p_2 \cdots p_h / p_i$; pour $j \neq i$, q_i est multiple de p_j ; $x_i q_i$ n'étant pas multiple de p_i , on a $x \notin p_i A$, donc $v_i(x)=0$, pour tout i ; donc x est inversible dans A . Mais cela est impossible puisque $x \in \mathfrak{p}$. Donc tout idéal premier de A est minimal, et A est anneau de Dedekind.

[Cette proposition (prop.3, p.55 de la rédaction précédente, où elle servait à la théorie de la ramification p.72) ne sert plus à rien, et semble mûre pour le rejet en exercice].

§ 6. Théorèmes de permanence.

Notre objet dans ce § est de montrer que, si un anneau A possède certaines des propriétés qu'on a étudiées dans ce chapitre (p.ex. s'il est intégralement clos, s'il est normal, etc..), certains anneaux qu'on peut construire à partir de A jouissent des mêmes propriétés ; c'est en cela que consistent les "théorèmes de permanence".

1. Anneaux de fractions.

Proposition 1. Soient A un anneau d'intégrité, et S une partie non vide de A , multiplicativement stable, ne contenant pas O. Si A est intégralement clos, resp. normal, resp. factoriel, resp. anneau de Dedekind, resp. principal, il en est de même de l'anneau de fractions A_S .

[N-B : Le rédacteur déplore l'usage de resp. dans ce genre d'énoncé, mais n'a pas trouvé d'autre moyen de s'en tirer. Au concours.]

Le premier point a déjà été démontré (coroll. de la prop.3, §4,n°1). Supposons A normal ; soit Ω un ensemble de définition de A (on peut prendre pour Ω l'ensemble V des valuations essentielles de A) ; soit Ω_S l'ensemble des $\omega \in \Omega$ qui prennent la valeur O sur S ; soit B l'intersection des anneaux des $\omega \in \Omega_S$; il est clair qu'on a $A_S \subset B$. Si $x \in B^*$, soient ω_i les valuations de Ω , en nombre fini, telles que $\omega_i(x) < 0$; alors, pour tout i , on a $\omega_i \in \Omega_S$, donc il existe $s_i \in S$

tel que $\omega_i(s_i) \geqslant 1$. Il s'ensuit qu'en posant $s = \prod_i s_i$, on aura $xs^N \in A$ pour N assez grand, donc $x \in A_S$ puisque $s^N \in S$. On a donc $B = A_S$, c'est-à-dire que A_S est un anneau normal ayant Ω_S pour ensemble de définition. D'ailleurs, d'après le coroll.3 de la prop.2, §1, les idéaux $\mathfrak{a}'$ de A_S sont en correspondance biunivoque, au moyen des relations $\mathfrak{a}' = \mathfrak{a} A_S$, $\mathfrak{a} = A \cap \mathfrak{a}'$, avec les idéaux $\mathfrak{a}$ de A tels que $as \in \mathfrak{a}$, $a \in A$, $s \in S$ entraîne $a \in \mathfrak{a}$; ce même coroll. montre que, si l'un des idéaux $\mathfrak{a}, \mathfrak{a}'$ est premier, l'autre l'est aussi ; et, si $\mathfrak{a}$ est premier, la condition que $as \in \mathfrak{a}$, $a \in A$, $s \in S$ entraîne $a \in \mathfrak{a}$ équivaut à $\mathfrak{a} \cap S = \emptyset$. Donc les idéaux premiers $\mathfrak{p}'$ de A_S sont en correspondance biunivoque, au moyen des relations $\mathfrak{p}' = \mathfrak{p} A_S$, $\mathfrak{p} = A \cap \mathfrak{p}'$, avec les idéaux premiers $\mathfrak{p}$ de A tels que $\mathfrak{p} \cap S = \emptyset$; comme il est clair que cette correspondance conserve les relations d'inclusion, $\mathfrak{p}'$ est minimal si $\mathfrak{p}$ est minimal. Soit V_S l'ensemble des valuations essentielles de A qui prennent la valeur 0 sur S , c'est-à-dire des $v \in V$ telles que $\mathfrak{p}(v) \cap S = \emptyset$; si $v \in V_S$, et si on désigne par $\mathfrak{p}'(v)$ le noyau de v sur A_S , on aura $\mathfrak{p}(v) = A \cap \mathfrak{p}'(v)$, donc, d'après ce qui précède, $\mathfrak{p}'(v) = \mathfrak{p}(v) A_S$, et $\mathfrak{p}'(v)$ est minimal. Donc V_S est l'ensemble des valuations essentielles de A_S. Si $\mathfrak{p}(v)$ est un idéal principal pA , on a $\mathfrak{p}'(v) = pA_S$; donc, si A est factoriel, A_S l'est aussi. Si tout idéal premier de A est minimal, il en est de même a fortiori de A_S d'après ce qui précède. Si A est principal, la prop.13 du n°6 montre alors que A_S est principal.

[N-B : Le rédacteur regrette d'avoir eu à répéter un bout de la démonstration du th.3 du § 2, n°5 ; cela lui donne l'occasion de constater une fois de plus qu'il a eu beaucoup de peine à tracer (conformément aux instructions de LA TRIBU) une ligne de démarcation entre les §§1 et 2, et qu'il n'y a pas complètement réussi. Comme il commence à être légèrement fatigué, il renonce à apporter de nouvelles retouche aux §§ en question, et se contente de livrer ce thème aux méditations de son illustre Maître].

2. Anneaux de polynomes.

La théorie de ces anneaux repose sur le résultat suivant :

Proposition 2. Soit ω une valuation d'un corps K ; soit $L = K((X_\iota))$ le corps des fonctions rationnelles sur K à un nombre quelconque d'indéterminées X_ι. Pour $P \in K[(X_\iota)]$, $P \neq 0$, soient a_i tous les coefficients $\neq 0$ de polynome P, et soit $\omega'(P) = \min_i \omega(a_i)$. Alors ω' se prolonge, au moyen de $\omega'(P/Q) = \omega'(P) - \omega'(Q)$ pour $P \in K[(X_\iota)]$, $Q \in K[(X_\iota)]$, $P \neq 0$, $Q \neq 0$, à une valuation ω' du corps L qui prolonge ω.

En vertu de la prop.2 du § 3, n°2, nous avons simplement à vérifier que ω' satisfait sur $K[(X_\iota)]$ aux conditions énoncées dans cette proposition ; pour $\omega'(P+Q) \geqslant \min[\omega'(P), \omega'(Q)]$, c'est immédiat. Pour vérifier que $\omega'(PQ) = \omega'(P) + \omega'(Q)$ pour $P \neq 0$, $Q \neq 0$, observons que c'est immédiat si P ou Q se réduit à son terme constant. Alors, soit a un coefficient de P tel que $\omega'(P) = \omega(a)$, et soit b un coefficient de Q tel que $\omega'(Q) = \omega(b)$; en remplacant P, Q par $a^{-1}P$, $b^{-1}Q$, on est ramené au cas où $\omega'(P) = \omega'(Q) = 0$. Dans ce cas, P et Q ont leurs coefficients dans l'anneau A de ω ; il en est donc de même de PQ, d'où $\omega'(PQ) \geqslant 0$. Soit $\mathfrak{p}$ l'idéal de la valuation ω, et soit φ l'extension à $A[(X_\iota)]$ de l'homomorphisme canonique de A sur son corps des restes $k = A/\mathfrak{p}$; alors $\omega'(PQ) > 0$ équivaut à $\varphi(PQ)=0$; comme $\varphi(PQ) = \varphi(P)\varphi(Q)$, et qu'un anneau de polynomes sur un corps est sans diviseurs de 0 (Alg., Chap. IV, § 1, n°4, th. 1), $\varphi(PQ)=0$ entraîne $\varphi(P)=0$, c'est-à-dire $\omega'(P) > 0$, ou $\varphi(Q)=0$ c'est-à-dire $\omega'(Q) > 0$, ce qui est contraire à l'hypothèse.

Définition 1. Avec les notations de la prop.2, ω' s'appellera l'extension canonique de ω à $K((X_\iota))$.

Définition 2. Soit A un anneau factoriel (resp. un anneau de Dedekind). Soit P un polynome $\neq 0$, à coefficients dans le corps des fractions K de A ; et soient a_i les coefficients $\neq 0$ de P. Alors tout pgcd des a_i relativement à A (resp. l'idéal fractionnaire $\sum_i a_i A$ dans K) s'appellera un contenu (resp. le contenu idéal) du polynome P relativement à A.

Proposition 3 ("lemme de Gauss"). Soit A un anneau factoriel (resp. un anneau de Dedekind) ; soient P,Q des polynomes $\neq 0$, à coefficients dans le corps des fractions K de A, à indéterminées X_ι. Alors le produit de contenus (resp. des contenus idéaux) de P,Q est un contenu (resp. le contenu idéal) de PQ.

En effet, compte-tenu de la théorie des anneaux factoriels et des anneaux de Dedekind exposée au §5, la prop.3 n'est autre chose que la propriété $v'(PQ) = v'(P) + v'(Q)$ pour l'extension canonique v' à $K((X_\iota))$ de toute valuation essentielle v de A.

Théorème 1. Si A est un anneau d'intégrité intégralement clos, resp. normal, resp. factoriel, il en est de même de l'anneau $A[X_1,\ldots,X_n]$ des polynomes sur A à un nombre fini quelconque d'indéterminées X_i.

Procédant par récurrence, on voit qu'il suffit de faire la démonstration pour $n=1$, donc pour un anneau $A[X]$ à une seule indéterminée X. Soit K le corps des fractions de A ; alors $A[X]$ est un sous-anneau de $K[X]$, et $K(X)$ est leur corps des fractions commun. On sait (Alg...) que $K[X]$ est un anneau principal ; soit V_0 l'ensemble des valuations non triviales normées de $K[X]$, c'est-à-dire des valuations non triviales normées de $K(X)$ dont l'anneau contient $K[X]$; $K[X]$ est alors intersection des anneaux des valuations appartenant à V_o . Supposons que A soit intégralement clos, donc (prop.1 du § 4, n°1) qu'il soit intersection des anneaux d'un ensemble Ω de valuations de K ; soit Ω' l'ensemble des extensions canoniques à K(X) des $\omega \in \Omega$. Il est clair que $A[X]$ est contenu dans les anneaux des valuations appartenant à $V_o \cup \Omega'$. Réciproquement, tout élément de l'intersection de ces anneaux appartient à l'intersection $K[X]$ des anneaux des valuations de V_o , donc est un polynome $P \in K[X]$; par définition des $\omega' \in \Omega'$, il est immédiat que P a tous ses coefficients dans A . Donc $A[X]$ est l'intersection des anneaux de valuation en question, et est donc intégralement clos. Supposons A normal, et prenons pour Ω l'ensemble V des valuations essentielles de A ; il est immédiat, d'après ce qui précède, que $V_o \cup V'$ est un ensemble de définition de $A[X]$, qui est donc normal. Supposons A factoriel ; alors, si $v \in V$, le noyau de v sur A est un idéal principal pA ; il est clair qu'alors le noyau sur $A[X]$ de l'extension canonique v' de v est $pA[X]$, donc principal. D'autre part, si $w \in V_o$, le noyau de w sur $K[X]$ est un idéal principal engendré par un polynome $P \in K[X]$, bien déterminé à un facteur constant près ; en multipliant P par un élément convenable de A , on peut supposer que $P \in A[X]$. Comme A est factoriel, les coefficients $\neq 0$ de P ont un pgcd $\underline{a}$ dans A , bien déterminé à un facteur inversible près ; en remplaçant P par $a^{-1}P$, on peut donc supposer que les coefficients de P sont dans A et étrangers dans leur ensemble ; dans ces conditions, on aura $v'(P)=0$ pour tout $v' \in V'$. Cela étant, soit $Q \in A[X]$ tel que $w(Q) > 0$; on aura donc $Q/P \in K[X]$. Si le polynome Q/P n'avait pas tous ses coefficients dans A , il y aurait $v' \in V'$ telle que $v'(Q/P) < 0$, ce qui est impossible puisque $v'(Q/P) = v'(Q) \geqslant 0$. Donc on a $Q \in P.A[X]$; autrement dit, le noyau de w sur $A[X]$ est un idéal principal. Comme l'ensemble $V_o \cup V'$ contient toutes les valuations essentielles de $A[X]$, $A[X]$ est donc factoriel.

Remarque : Avec les notations ci-dessus, on peut même montrer que $V_o \cup V'$ est l'ensemble des valuations essentielles de $A[X]$ (exercice ...)

Corollaire 1. Si A est un anneau factoriel, et K son corps des fractions, les éléments extrémaux de l'anneau $A[X_1,\dots,X_n]$ des polynomes sur A à un nombre fini n d'indéterminées X_i sont les éléments extrémaux de A, et les polynomes irréductibles de $K[X_1,\dots,X_n]$ de contenu 1 relativement à A.

Il est clair que tout élément extrémal de A, et tout polynome irréductible de contenu 1, est extrémal dans $A[X_1,\dots,X_n]$; il n'y a donc qu'à démontrer la réciproque. Soit P un élément extrémal de $A[X_1,\dots,X_n]$; s'il était dans A, il serait extrémal dans A ; donc on peut supposer $P \notin A$; il est clair qu'alors P est de contenu 1. Supposons que P ne soit pas irréductible dans $K[X_1,\dots,X_n]$, donc qu'on a $P = QQ'$, Q et Q' étant dans $K[X_1,\dots,X_n]$. Soient a,a' des contenus de Q,Q' ; d'après la prop.3, $u=aa'$ est un contenu de P, et est donc associé à 1 c'est-à-dire est un élément inversible de A. Alors on a $P = (a^{-1}Q)(a'^{-1}uQ')$, et $a^{-1}Q$, $a'^{-1}uQ'$ sont des polynomes de contenu 1, donc sont dans $A[X_1,\dots,X_n]$; P n'est donc pas extrémal.

Corollaire 2. Les anneaux $k[X_1,\dots,X_n]$, où k est un corps, et $Z[X_1,\dots,X_n]$, sont factoriels.

Remarque : Pour $n \geqslant 2$, les anneaux $k[X_1,\dots,X_n]$ et $Z[X_1,\dots,X_{n-1}]$ ne sont pas des anneaux de Dedekind. On peut le vérifier, soit en construisant dans ces anneaux des couples d'idéaux premiers emboîtés, soit en construisant des valuations de rang n de ces anneaux (cf. la démonstration de la prop.7 du § 3, n°5, ainsi que l'exemple 5 c) du § 3, n°1).

[N-B : Le rédacteur est d'avis de rejeter en ex. le fait que les anneaux de polynomes à une infinité d'indéterminées sur un anneau factoriel sont factoriels ; cf. La Tribu, p.23] .

[N-B : Le rédacteur propose aussi de faire des exercices des coroll. 2 et 3, p.67, de la rédaction précédente. Si Bourbaki désirait les conserver, ils s'insèreraient tout naturellement entre les coroll.1 et 2 ci-dessus. Quant à la prop.4 de la p.66, elle découle d'une manière tellement triviale de la détermination faite plus haut des des éléments extrémaux de $A[X_1,\dots,X_n]$, et des propriétés générales des anneaux factoriels, qu'elle ne mérite même pas un exerc. Le rédacteur s'est d'ailleurs vainement demandé pourquoi son prédécesseur n'a formulé ces résultats que pour les polynomes à une indéterminée].

Proposition 4. Soient K un corps, L une extension de K. Alors, si deux polynomes sont étrangers dans $K[X_1,\dots,X_n]$, ils le sont encore dans $L[X_1,\dots,X_n]$.

Procédant par récurrence sur n , on est ramené à montrer que, si A est un sous-anneau factoriel d'un anneau factoriel B tel que deux éléments étrangers de A le soient nécessairement encore dans B , deux éléments étrangers P, Q de $A[X]$ le sont encore dans $B[X]$. Soient K', L' les corps des fractions de A et de B . Comme les contenus de P et Q sont étrangers dans A , ils le sont dans B ; donc P et Q ne sont pas tous deux multiples d'un même élément extrémal de B . Alors, d'après le coroll.1 du th.1, s'ils n'étaient pas étrangers dans $B[X]$; ils ne le seraient pas dans $L'[X]$, et par suite, d'après la prop.... d'Alg.,Chap...., ils ne le seraient pas dans $K'[X]$; alors, si D est un pgcd de P et Q dans $K'[X]$, la décomposition de P, Q et D en produits d'éléments extrémaux de $A[X]$ montre immédiatement que P et Q ne peuvent être étrangers dans $A[X]$.

3. Anneaux d'entiers algèbriques.

Théorème 2. Soient A un anneau d'intégrité, K son corps des fractions, L une extension algèbrique de K de degré fini n, B la fermeture intégrale de A dans L. Alors, si A est normal, B l'est aussi ; si A est un anneau de Dedekind, il en est de même de B.

Supposons A normal ; soit Ω un ensemble de définition de A ; soit Ω' l'ensemble des valuations de L qui prolongent celles de Ω ; toutes ces valuations sont discrètes d'après le coroll.1 du th.7, § 3, n°7. Soit Θ l'ensemble des valuations discrètes normées de L respectivement équivalentes aux valuations $\omega' \in \Omega'$. D'après le coroll.2 de la prop.5, § 4, B est l'intersection des anneaux des valuations $\theta \in \Theta$. Soit $x \in B^*$; soit $x^n+a_1x^{n-1}+\ldots+a_n = 0$ une équation de dépendance intégrale pour x sur A ; comme B est anneau d'intégrité, on peut supposer, en divisant au besoin cette équation par une puissance de x, que $a_n \neq 0$; d'après cette équation, on a $a_n/x \in B$; donc, si $\omega' \in \Omega$ et si $\omega'(x) > 0$, on a $\omega'(a_n) > 0$, c'est-à-dire $\omega(a_n) > 0$ si ω est la valuation induite par ω' sur K. Mais, puisque Ω est un ensemble de définition de A, il n'y a qu'un nombre fini de $\omega \in \Omega$ ayant cette propriété ; chacune n'a qu'un nombre fini de prolongements inéquivalents à L d'après le th.7 du § 3, n°7 ; il n'y a donc qu'un nombre fini de $\theta \in \Theta$ tels que $\theta(x) > 0$, de sorte que Θ est un ensemble de définition de L. Le coroll. de la prop.4, § 4, montre alors que si tout idéal premier est minimal dans A, il en est de même dans B ; il montre aussi qu'en général, pour qu'une valuation $\theta \in \Theta$ soit essentielle, il faut et il suffit que la valuation correspondante $\omega \in \Omega$ le soit pour A.

Corollaire. Soit K une extension algèbrique de degré fini du corps Q des nombres rationnels ; soit B l'anneau des entiers algèbriques de K, c'est-à-dire l'anneau des éléments de K qui sont entiers sur Z. Alors B est un anneau de Dedekind.

Le résultat ci-dessus détermine la structure multiplicative de l'anneau B ; sur sa structure additive, on a le résultat suivant :

Proposition 5. Soient A un anneau d'intégrité, K son corps des fractions, L une extension algèbrique de K de degré fini n , B la fermeture intégrale de A dans L . Alors on a $BK = L$. Si de plus A est intégralement clos, et L séparable sur K , B est contenu dans un sous-A-module de L isomorphe à A^n .

La première assertion résulte de la prop.3 du §4 si on y prend $R = L$ et $S = A^*$, ce qui donne $R_S=R$, $B_S=BK$, $A_S=K$. Supposons L séparable ; soit $(x_i)_{1\leqslant i\leqslant n}$ une base de L sur K ; d'après la prop.12, Alg., Chap.V, §10, n°6, la matrice $(Tr(x_ix_j))$, à éléments dans K , est inversible ; si on désigne par (a_{ij}) la matrice inverse, et qu'on pose $y_i = \sum_{j=1}^{n} a_{ij}x_j$, on aura $Tr(y_ix_k) = \delta_{ik}$, et cette relation subsiste si on remplace les y_i par ay_i et les x_k par $a^{-1}x_k$, avec $a\in K^*$. Puisque $BK=L$, il y a, pour tout i , un $a_i \in A^*$ tel que $a_iy_i \in B$; en prenant $a = a_1a_2\ldots a_n$, tous les ay_i seront donc dans B . Autrement dit, après avoir ainsi remplacé les x_i par $a^{-1}x_i$ et les y_i par ay_i , on peut supposer $y_i\in B$ pour $1\leqslant i\leqslant n$. Cela posé, soit $x\in B$; mettons x sous la forme $x = \sum_i t_ix_i$ avec $t_i\in K$ $(1\leqslant i\leqslant n)$; en multipliant cette relation par y_j et prenant la trace, on trouve $t_i = Tr(y_ix)$ $(1\leqslant i\leqslant n)$. D'après le coroll.1 de la prop.5, §4, $x\in B$ entraîne alors $t_i\in A$ pour tout i . Autrement dit, B est un sous-module du sous-A-module de L engendré par $x_1,x_2,\ldots,x_n$.

Corollaire. Si de plus A est un anneau principal (donc en particulier si $A = Z$), B est isomorphe à A^n .

Dans ce cas, en effet, il résulte d'Alg... que B est un A-module libre de rang $\leqslant n$; et son rang est n , puisque l'espace vectoriel qu'il engendre sur K contient BK et n'est donc autre que L, donc est de dimension n sur K .

OUF .