RÉDACTION N° 146

COTE : NBR 048

TITRE : DEUXIÈME PARTIE : ANALYSE ALGÉBRIQUE
LIVRE I : ALGÈBRE SUPÉRIEURE
CHAP. I SPÉCIALISATIONS ET VALUATIONS (ÉTAT 2)

ASSOCIATION DES COLLABORATEURS DE NICOLAS BOURBAKI

NOMBRE DE PAGES : 74

NOMBRE DE FEUILLES : 74

Nov. 1950 - Février 1951

DEUXIEME PARTIE

ANALYSE ALGÈBRIQUE

LIVRE I.
ALGÈBRE SUPÈRIEURE.

CHAPITRE I.
SPECIALISATIONS ET VALUATIONS. (Etat 2)

Introduction.

Le présent chapitre et le suivant ("Anneaux noethériens") constituent une introduction aux Livres II et III de cette deuxième Partie, respectivement relatifs à l'Algèbre Unidimensionnelle et à la Géomètrie Algèbrique. Les chapitres suivants du Livre I, au contraire, donneront les outils algèbriques nécessaires à l'étude des autres parties de ce Traité, principalement en ce qui concerne la Topologie Algèbrique et la théorie des Groupes de Lie.

Afin d'éviter au lecteur d'avoir à suspendre son jugement jusqu'à la lecture des Livres II et III, nous donnerons, dans ce chapitre, de nombreux exemples empruntés à l'Arithmétique et à la Géomètrie Algèbrique, matières que certains lecteurs pourraient connaître par ailleurs. Cependant, étant donnée la diversité des points de vue auxquels les auteurs ayant traité de ces questions se sont placés (principalement en Géomètrie Algèbrique), nous avons pensé qu'il pourrait être utile d'exposer brièvement ici les définitions et le terminologie qui seront utilisées dans ces exemples.

Soit U un corps algèbriquement clos et de degré de transcendance infini sur son corps premier ; nous appellerons U un "domaine universel" le corps C des nombres complexes est un domaine universel de caractéristique 0 . Dans l'espace affine de dimension n $A_n(U)$, l'ensemble B des points $(x_1,\ldots,x_n)$ où s'annullent une famille (F_α) de polynomes à

n indéterminées sur un sous-corps K de U dont U soit une extension de degré de transcendance infini, s'appelle un ensemble algèbrique ; l'ensemble des polynomes $F \in K[X_1,\ldots,X_n]$ qui s'annulent en tout point de l'ensemble algèbrique B est évidemment un idéal $I_K(B)$, contenant les F_a, et appelé l'idéal associé à B sur K . Dans le cas où l'idéal $I_K(B)$ est "premier" (c'est-à-dire si l'anneau quotient $K[X_1,\ldots,X_n]/I_K(B)$ est un anneau d'intégrité) et "reste premier par toute extension de K" (c'est-à-dire si l'idéal engendré par $I_K(B)$ dans $E[X_1,\ldots,X_n]$ est premier pour tout surcorps E de K), l'ensemble algèbrique B est appelé une variété, et K est appelé un corps de définition de B ; alors (1ère Partie, Livre II, chap.V) l'anneau quotient $K[X_1,\ldots,X_n]/I_K(B)$ est K-isomorphe à un sous-anneau A de U, et, x_i désignant l'image de la classe (mod. $I_K(B)$) de X_i par cet isomorphisme, on a $A = K[x_1,\ldots,x_n]$; le point $(x_1,\ldots,x_n)$ est appelé un point générique de la variété B sur K , et l'anneau A est appelé un anneau de coordonnées de B sur K ; tous les anneaux de coordonnées de B sur K sont K-isomorphes. Le corps des fractions $F = K(x)$ de l'anneau de coordonnées A est appelé un corps de fractions rationnelles sur B relativement à K ; tous ceux-ci sont K-isomorphes. Soient V et W deux variétés, K un corps de définition de V et W , $(x) = (x_1,\ldots,x_n)$ et $(y) = (y_1,\ldots,y_m)$ des points génériques de V et W sur K ; si les corps de fonctions rationnelles K(x) et K(y) sont K-isomorphes, on dit que les variétés V et W sont birationnellement équivalentes sur K ; par un changement éventuel de points génériques, on peut supposer que l'on a $K(x)=K(y)$.

Si tous les points de la variété W sont aussi points de la variété V, on dit que W est une sous variété de V ; si K est corps de définition de V et W , ceci revient à dire qu'on a, entre les idéaux associés, la relation $I_K(V) \subset I_K(W)$; autrement dit un anneau de coordonnées

de W sur K est K-isomorphe à un anneau quotient d'un anneau de coordonnées de V sur K . Par exemple l'espace affine A_n est une variété dont l'idéal associé est (0), et dont les anneaux de coordonnées sont K-isomorphes à l'anneau des polynomes à n indéterminées sur K .

Le degré de transcendance (sur K) d'un corps de fractions rationnelles sur V relativement à K est appelé la dimension de V et se note dim V . On démontre que cette dimension est indépendante du corps de définition K choisi. Si W est sous variété de V , le fait que l'anneau de coordonnées de W soit isomorphe à un quotient de celuid de V montre que $\dim(W) \leqslant \dim(V)$, puisque toute relation algèbrique à coefficients dans K satisfaite par une famille d'éléments de l'anneau de coordonnées de V est satisfaite par les éléments correspondants de l'anneau de coordonnées de W ; on montre même que, si $V \neq W$, alors $\dim W < \dim V$.

Soit V une variété de point générique $(x_1,\ldots,x_n)$ sur K . L'idéal $I_K(V) \cap K[X_1,\ldots,X_m]$ $(m \leqslant n)$ est premier et reste premier par toute extension de K . Les polynomes $F(X_1,\ldots,X_m)$ qui s'annulent en tous les points de la projection (au sens ensembliste) de V sur l'espace affine A_m des m coordonnées $(X_1,\ldots,X_m)$, sont évidemment les éléments de cet idéal. Cet idéal est donc l'idéal associé à une variété W de A_m , appelée la projection de V sur A_m . Les théorèmes d'isomorphisme montrent aussitôt que $(x_1,\ldots,x_m)$ est point générique de W sur K . On a $\dim.W \leqslant \dim.V$. L'exemple de l'hyperbole $XY=1$ et de l'axe OX montre que la projection définie ici peut être strictement plus grande que la projection "ensembliste" de V .

---

§ 1.- Spécialisations.

1 - Définition des spécialisations.

Définition 1 - Etant donné un anneau commutatif A ayant un élément unité, on appelle spécialisation de A tout homomorphisme f de A dans un corps K tel que $f(1)=1$; deux spécialisations f et f' de A seront dites équivalentes s'il existe un isomorphisme g d'un corps contenant $f(A)$ sur un corps contenant $f'(A)$ tel que $f' = g \circ f$.

Exemples - 1) Si A est l'anneau des polynomes à n indéterminées sur un corps K , et si $(x) = (x_1,\dots,x_n)$ est une suite de n éléments de K , l'application f qui, à tout polynome $P(X_1,\dots,X_m)$ de A , fait correspondre sa valeur $P(x_1,\dots,x_m)$ est une spécialisation de A .

2) Soit V une variété ayant (x) pour point générique sur K , et $A = K[x]$ un anneau de coordonnées de V ; si (x') est un point quelconque de V , l'application f qui, à tout élément $P(x)$ de $K[x]$ fait correspondre $P(x')$ est bien définie, car, si $P(x) = Q(x)$, on a $P(x') = Q(x')$ par définition de la notion de point générique ; et f est évidemment une spécialisation de A . On dit aussi que (x') est une spécialisation du point générique (x) sur K .

3) Soit Z l'anneau des entiers rationnels et p un nombre premier ; l'homomorphisme canonique de Z sur $Z/(p)$ est une spécialisation de Z.

4) Soit A l'anneau des séries formelles en n indéterminées sur un corps K ; l'application qui, à toute série formelle de A , fait correspondre son terme constant est une spécialisation de A .

Si f est une spécialisation de l'anneau A , $f(A)$ est isomorphe à A/P où P est l'idéal $f^{-1}(0)$ noyau de f , et A/P est un anneau d'intégrité. Si réciproquement l'anneau quotient A/P est d'intégrité, c'est un sous anneau de son corps des fractions K , et l'homomorphisme canonique de A sur A/P est une spécialisation f_0 de A , équivalente à toute spécialisation f de A ayant P pour noyau (Alg., chap.I, § 8, n°8, th.3). Ceci nous amène à poser la définition suivante :

Définition 2 - Un idéal P d'un anneau commutatif A ayant un élément unité est dit premier si A/P est un anneau d'intégrité, c'est-à-dire si $P \neq A$ et si $x \in A$, $y \in A$ et $xy \in P$ entraînent $x \in P$ ou $y \in P$; l'homomorphisme canonique de A sur A/P est alors une spécialisation de A, appelée spécialisation canonique de A sur A/P .

Ainsi les spécialisations f de A sont les homomorphismes de A dont le noyau est un idéal premier. Et la donnée du noyau d'une spécialisation f détermine celle-ci à une équivalence près.

Exemples - 1) Dans un anneau principal A (Alg., chap. VII) les seuls idéaux premiers sont de la forme (p) où p est élément extrémal de A.

2) Plus généralement tout idéal maximal M d'un anneau commutatif quelconque A est premier, car A/M est un corps. Mais il existe des idéaux premiers qui ne sont pas maximaux, par exemple les idéaux (X) et (Y) de l'anneau des polynomes à deux indéterminées X et Y sur un corps K ; en effet ils sont tous deux contenus dans l'idéal maximal (X,Y).

3) L'idéal associé à une variété V est un idéal premier.

2 - Prolongement des spécialisations : anneaux locaux.

Soient B un anneau commutatif ayant un élément unité, et A un sous-anneau de B ; conformément aux définitions générales, nous dirons qu'une spécialisation g de B est un prolongement d'une spécialisation f de A si la restriction de g à A est égale à f . Dans les n° qui suivent nous nous proposons, étant donnés une spécialisation f de l'anneau A et un corps K contenant A , de trouver des prolongements de f qui soient définis sur des sous-anneaux aussi grands que possible de K .

Soit d'abord K_0 le corps des fractions de A , que nous pouvons supposer plongé dans K . Si g est un prolongement de f tel que g(x)

soit défini pour l'élément $x = a/b$ ($a \in A$, $b \in A$) de K_0 , on a $a = bx$, donc $f(a) = f(b)g(x)$. Comme les valeurs prises par g sont éléments d'un corps L , cette formule déterminera $g(x)$ de façon unique à condition que l'on ait $g(b) \neq 0$, c'est-à-dire si b n'appartient pas à l'idéal premier $P = f^{-1}(0)$. En vertu de la définition 2 le complémentaire S de P dans A ne contient pas 0 et est stable pour la multiplication ; ceci nous amène à étudier la situation plus générale suivante :

Proposition 3.- Soit A un anneau commutatif quelconque, et S une partie non vide de A ne contenant ni 0 ni de diviseur de 0 , et stable pour la multiplication ; alors l'ensemble des éléments a/s ($a \in A$, $s \in S$) de l'anneau des fractions de A (Alg., chap. I, § 9) est un anneau A_S contenant A , et ayant les propriétés suivantes :

a) Si (y_i) $(1 \leqslant i \leqslant n)$ est une famille finie d'éléments de A_S , il existe $s \in S$ tel que $sy_i \in A$ pour tout i .

b) Si I est un idéal de A_S , I est engendré dans A_S par l'idéal $I \cap A$ de A .

c) Si P est un idéal premier de A tel que $P \cap S = \emptyset$, l'idéal PA_S de A_S engendré par P est premier, et on a $P = PA_S \cap A$.

L'ensemble A_S est bien un anneau en vertu des règles de calcul $(a/s)+(a'/s') = (as'+a's)/ss'$ et $(a/s).(a'/s') = (aa')/(ss')$; il contient A car $a = as/s$. Si $y_i = a_i/s_i$ ($s_i \in S$) , le produit s des s_i appartient à S par hypothèse, et on a $sy_i \in A$ pour tout i ce qui démontre a). Si I est un idéal de A_S , pour tout $y \in I$, il existe $s \in S$ tel que $sy \in A$; comme $s \in A_S$, on a $sy \in I$, donc $sy \in I \cap A$; et, puisque $y = (s/s^2).sy$, et que $s/s^2 \in A_S$, I est bien engendré, dans A_S , par $I \cap A$, ce qui démontre b) . Si enfin P est un idéal premier de A ne rencontrant pas S , et si le produit $(a/s).(a'/s')$ appartient à l'idéal engendré PA_S , cet élément est de la forme

$\sum_{i=1}^{n} (a_i/s_i).p_i$ $(p_i \in P)$, c'est-à-dire, par réduction à un même dénominateur, de la forme p/s'' où $p \in P$ et $s'' \in S$; on a donc $aa's'' = ss'p \in P$; comme $s'' \notin P$ par hypothèse, on a $aa' \in P$ par définition des idéaux premiers ; donc a, par exemple, appartient à P , et $a/s \in PA_S$, ce qui montre que PA_S est premier. Enfin si $a \in A$ appartient à PA_S , on a $a = p/s$ où $p \in P$ et $s \in S$, donc $as \in P$; comme $s \notin P$, on en déduit $a \in P$, et $PA_S \cap A = P$, ce qui démontre c) .

Ajouter, dans l'énoncé de la prop.3, que si $\mathfrak{a}$ est un idéal de A , l'idéal engendré $\mathfrak{a}A_S$ est l'ensemble des a/s $(a \in \mathfrak{a}, s \in S)$.

Définition 3 - Avec les notations de la prop.3, l'anneau A_S est appelé l'anneau des fractions de la partie multiplicativement stable S (relativement à A). Si S est le complément, dans A , d'un idéal premier P , A_S est aussi appelé l'anneau des fractions de l'idéal premier P et se note A_P .

Lorsque S est le complément d'un idéal premier P de A , l'idéal PA_P est un idéal premier de A_P en vertu de la prop.3,c). Tout élément de PA_P non contenu dans P est de la forme s/s' où $s \in S$ et $s' \in S$, et admet donc, dans A_P , un inverse qui est s'/s . Ceci nous conduit à poser la définition suivante :

Définition 4 - On dit qu'un anneau commutatif avec élément unité est un anneau local si l'ensemble M des éléments non inversibles de B est un idéal (qui est alors le plus grand idéal distinct de B dans B) ; M est appelé l'idéal maximal de B , et B/M le corps des restes de B .

Remarque - La plupart des auteurs réserve le nom d'anneaux locaux aux anneaux noethériens qui satisfont à la déf. 4.

Revenons maintenant au problème de prolongement des spécialisations :

Proposition 4 - Soit A un sous-anneau d'un corps K tel que $1 \in A$, et soit f une spécialisation de A de noyau $P = f^{-1}(0)$; alors la spécialisation f se prolonge, d'une manière et d'une seule, en une spécialisation g de l'anneau de fractions A_P (identifié à un sous-anneau de K) ; le noyau de g est l'idéal maximal PA_P de l'anneau local A_P ; et $g(A_P)$ est l'idéal maximal PA_P de l'anneau local A_P ; et $g(A_P)$ est le corps des fractions de l'anneau $f(A)$.

En effet, pour tout $x \in A_P$, on a $x = a/s$ où $a \in A$ et $s \notin P$; si g est un prolongement de f à A_P, on a donc $f(s)g(x) = f(a)$, d'où $g(x) = f(a)/f(s)$ puisque $f(s) \neq 0$, ce qui montre l'unicité de g. D'autre part la valeur $g(x)$ définie par $g(x) = f(a)/f(s)$ ne dépend pas de la représentation de x sous la forme $x = a/s$ ($a \in A$, $s \notin P$), car, si $a/s = a'/s'$, on a $as' = a's$ et donc $f(a)f(s') = f(a')f(s)$; ceci montre l'existence de l'application g de A_P dans le corps des fractions de $f(A)$; et on vérifie comme l'âne qui trotte que g est un homomorphisme prolongeant f. Comme $f(s) \neq 0$ pour $s \notin P$, les relations $f(a/s)=0$ et $f(a)=0$ sont équivalentes, ce qui montre que PA_P est le noyau de g. Enfin, comme l'ensemble des $f(s)$ pour $s \notin P$ est l'ensemble des éléments non nuls de $f(A)$, l'ensemble des $f(a)/f(s)$ ($a \in A$, $s \notin P$) est bien le corps des fractions de $f(A)$.

Définition 5 - Les notations étant celles de la prop.4, l'anneau de fractions A_P est appelé l'anneau local de la spécialisation f.

Exemples.- 1) Si f est la spécialisation canonique de Z sur Z/(p) (p:premier), l'anneau local de f se compose des nombres rationnels qui peuvent se mettre sous la forme m/n, où m et n sont des entiers tels que n ne soit pas multiple de p.

2) Si V est une variété de point générique x sur un corps K, si f est une spécialisation de l'anneau de coordonnées $K[x]$ et si

$x'_i = f(x_i)$, l'anneau local A de f se compose des fonctions rationnelles sur V (définies sur K) dont le dénominateur ne s'annule pas au point spécialisé (x'). On appelle cet anneau l'anneau local de V au point (x') (ou de (x') sur V). Si (x') est point générique sur K d'une variété W , W est évidemment sous-variété de V , et A est appelé l'anneau local de V le long de W (ou de W sur V). Si le point (x') de V est l'origine des coordonnées, l'anneau local de V en (x') est l'anneau des fonctions rationnelles $r(x) \in K(x)$ qui peuvent se mettre sous la forme $r(x) = p(x)/q(x)$ où p et q sont des polynomes tels que le terme constant de q ne soit pas nul.

3) L'anneau de séries formelles $B = K[[X_1,\dots,X_n]]$ est un anneau local dont l'idéal maximal M est engendré par $(X_1,..,X_n)$ puisque toute série formelle dont le terme constant n'est pas nul est inversible (Alg.,chap.IV, § 6). Donc l'anneau local de la spécialisation canonique de B sur B/M est identique à B .

3 - Prolongement des spécialisations : corps projectifs.

Soit encore f une spécialisation d'un sous-anneau A d'un corps K , et soit x un élément de K qui se mette sous la forme $x = a/b$ où $a \in A$ et $b \in A$. Si g est un prolongement de f tel que g(x) soit défini, on a $g(x)f(b) = f(a)$. Nous avons, au n°2, étudié le cas où $f(b) \neq 0$. Supposons maintenant que l'on ait $f(b)=0$ et $f(a) \neq 0$; alors la relation $g(x)f(b) = f(a)$ ne peut être satisfaite par aucune valeur de g(x).

Ceci nous conduit à faire la convention suivante : pour tout corps F considérons l'ensemble F_∞ obtenu par adjonction à F (muni de sa structure de corps) d'un élément unique, qui sera toujours noté ∞ (de même que l'élément zéro est toujours noté 0) ; nous conviendrons de prolonger l'application biunivoque $x \longrightarrow 1/x$ de K^* sur lui-même en une application biunivoque de K_∞ sur lui-même en posant $1/0 = \infty$ et $1/\infty = 0$; muni de cette structure, l'ensemble K_∞ sera

appelé un corps projectif. Alors, avec les notations de l'alinéa précédent, nous poserons $g(x) = \infty$ pour $x = a/b$ tels que $f(b) = 0$ et $f(a) \neq 0$, et en particulier pour l'élément $x = \infty = 1/0$ du corps projectif K_∞ .

Au moyen de cette convention, nous avons prolongé la spécialisation f du sous-anneau A du corps K en une application g de l'ensemble A" des éléments x du corps projectif K_∞ tels que x ou $1/x$ appartienne à l'anneau local A' de f , dans le corps projectif K'_∞ déduit du corps des fractions de f(A) . L'application g induit une spécialisation de l'anneau local A' , et prend la valeur ∞ sur le complémentaire de A' dans A" . Pour tous x et y de A" tels que xy soit élément de A" , on a la relation $g(x)g(y) = g(xy)$, à condition que le premier membre ne se présente pas sous la forme $0.\infty$. L'ensemble A" est appelé le domaine de la spécialisation f , et, par abus de langage, g est dite une spécialisation de A" .

4 - Prolongement des spécialisations : le théorème de prolongement.

Considérons toujours une spécialisation f d'un sous-anneau d'un corps K . Dans les deux n° précédents nous avons vu comment f se prolonge, et de façon canonique, en une spécialisation du domaine A" de f . Mais il arrive souvent que A" soit distinct du corps projectif K_∞ .

Il peut, d'une part, arriver que K soit distinct du corps des fractions de A . Et, même s'il en est ainsi, certains éléments de K ont toutes leurs représentations sous la forme a/b ($a \in A$ $b \in A$) telles que $f(a) = f(b) = 0$: ainsi, si A est l'anneau des polynomes à deux indéterminées X et Y sur un corps K' , et si f est la spécialisation de A qui, à tout polynome $P(X,Y)$ fait correspondre sa valeur à l'origine $P(0,0)$, l'élément Y/X ne fait pas partie du domaine de f (en vertu des rôles

symétriques joués par X et Y, on peut, si Y/X fait partie du domaine de f , supposer qu'il s'écrive $Y/X = P(X,Y)/Q(X,Y)$ où $Q(0,0) \neq 0$; alors $YQ(X,Y) = XP(X,Y)$, et $YQ(0,Y)=0$; on en déduit que l'on a $Q(0,Y)=0$, en contradiction avec $Q(0,0)\neq 0$).

Proposition 5 - Soit f une spécialisation d'un sous-anneau A d'un corps K et x un élément de K ; f peut alors se prolonger en une spécialisation g dont le domaine contient x , et telle que ceux des éléments $g(x)$ et $g(1/x)$ qui ne sont pas infinis soient algèbriques sur le corps des fractions de $f(A)$.

Nous ne restreindrons pas la généralité en supposant que A est l'anneau local de f ; notons M son idéal maximal. Si le prolongement g cherché existe, et si, par exemple, $g(x) \neq \infty$, le noyau de la restriction de g à $A[x]$ est un idéal premier P tel que $P \cap A = M$. Si nous parvenons à montrer que l'un au moins des idéaux $MA[x]$, $MA[1/x]$ engendrés par M dans $A[x]$ et $A[1/x]$ ne contient pas 1 , nous prendrons pour P un idéal maximal (de $A[x]$ pour fixer les idées) contenant cet idéal. Comme $P \cap A$ contient M et ne contient pas 1 , on a $P \cap A = M$; alors la restriction à A de la spécialisation canonique de $A[x]$ sur $A[x]/P$ est équivalente à f , ce qui montre l'existence du prolongement g de f . En effet le point laissé de côté résulte du lemme suivant :

Lemme - Soit A un sous-anneau d'un corps K , I un idéal de A ne contenant pas 1 , et x un élément de K ; alors l'un au moins des idéaux $IA[x]$, $IA[1/x]$ engendrés par I dans $A[x]$ et $A[1/x]$ ne contient pas 1

En effet, dans le cas contraire, il existerait des éléments p_i $(0 \leqslant i \leqslant m)$ et q_j $(0 \leqslant j \leqslant n)$ de I tels que l'on ait les relations

$$1 \pm \sum_{i=0}^{m} p_i x^i = 0$$

$$1 \pm \sum_{i=0}^{n} q_j x^{-j} = 0 \quad .$$

Nous supposerons que ces relations sont de degrés m et n les plus petits possible. Si on a, par exemple, $m \geqslant n$, nous multiplierons la première relation par $1+q_0$ et la seconde par $-p_m x^m$, et nous ajouterons ; alors nous obtiendrons une relation de la même forme que la première, mais de degré $\leqslant m-1$, contrairement aux hypothèses. En procédant de même dans le cas où $m \leqslant n$, nous avons démontré le lemme.

Reste la précision supplémentaire que l'on peut prendre $g(x)$ (ou $g(1/x)$) algébrique sur le corps des fractions de $f(A)$. Supposons par exemple que $1 \notin MA[x]$, et soit $u=g'(x)$ la valeur de x pour la spécialisation canonique de $A[x]$ sur $A[x]/P$. Si u est algébrique sur $g'(A)$ nous prendrons $g=g'$. Si u est transcendant sur $g'(A)$, $g'(A[x]) = g'(A)[u]$ est isomorphe à l'anneau de polynomes $g'(A)[X]$; alors l'application h qui, à tout élément de $g'(A)[u]$, fait correspondre son terme constant, est une spécialisation, et il suffit de prendre $g = h \circ g'$.

Corollaire - Si f est une spécialisation non prolongeable d'un sous-anneau A d'un corps K , le domaine A^* de f est identique au corps projectif K_∞ ; autrement dit, pour tout $x \in K$, on a, soit $x \in A$, soit $1/x \in A$.

Définition 6 - Un anneau commutatif A est dit anneau de valuation s'il est d'intégrité et si, pour tout élément x du corps des fractions de A , on a, soit $x \in A$, soit $1/x \in A$.

Nous étudierons les anneaux de valuation dans le § suivant. Notions immédiatement que, en vertu du cor. et de la prop.4 (n^0 2), tout anneau de valuation est un anneau local ; l'exemple des anneaux de séries formelles à plusieurs variables montre que la réciproque est inexacte.

Théorème 1 ("théorème de prolongement") - Si A est un sous-anneau (contenant 1) d'un corps K , et si f est une spécialisation de A prenant ses valeurs dans un corps algèbriquement clos U , il existe un prolongement g de f , prenant ses valeurs dans U_∞ , et tel que le domaine de g soit identique à K_∞ (l'anneau local de g étant alors un anneau de valuation).

En effet, l'ensemble des spécialisations, dans U, et prolongeant f de sous-anneaux de K , est inductif si on l'ordonne par prolongement. Il admet donc, en vertu du th. de Zorn, un élément maximal g . La spécialisation g n'est pas prolongeable, sinon elle serait prolongeable en une spécialisation prenant ses valeurs dans U , en vertu de la prop.5 et du fait que U contient tout élément algèbrique sur U . Et on conclut en utilisant le cor. de la prop.5 .

---

§ 2. Valuations.

1 - Divisibilité dans les anneaux de valuation.

Soit A un anneau de valuation (§ 1,déf.6) et K son corps des fractions. Rappelons (Alg.,chap.VI, §1) que la relation de divisibilité dans K^* (relativement à A) munit le groupe multiplicatif K^* d'une structure de groupe préordonné, et que le groupe ordonné canoniquement associé à celui-ci est isomorphe au groupe $\mathcal{P}^*$ des idéaux principaux fractionnaires de K , ordonné par inclusion. Dire que A est anneau de valuation équivaut, par définition, à dire que l'on a $A^* \cup (A^*)^{-1} = K^*$, ou que $\mathcal{P}^*$ est un groupe totalement ordonné (Alg.,chap.VI, §1,n°2, prop.). Par conséquent :

Théorème 1 - Pour qu'un anneau d'intégrité A soit anneau de valuation il faut et il suffit que le groupe ordonné $\mathcal{P}^*$ des idéaux principaux fractionnaires du corps des fractions de A (relativement à A) soit totalement ordonné.

Si A est un sous-anneau quelconque d'un corps K , l'application canonique v de K^* dans le groupe ordonné $\mathcal{P}^*$ des idéaux principaux fractionnaires de K (noté additivement) satisfait aux conditions suivantes :

(V_I) $v(xy) = v(x) + v(y)$ pour tous x,y de K^*.

(V_{II}) Les relations $v(x) \geqslant v(z)$ et $v(y) \geqslant v(z)$ entraînent $v(x+y) \geqslant v(z)$ qui se déduisent aussitôt de la définition des idéaux fractionnaires. Si $\mathcal{P}^*$ est réticulé, la relation (V_{II}) s'écrit aussi :

(V'_{II}) $v(x+y) \geqslant \inf(v(x),v(y))$ pour tous x,y de K^* tels que $x+y \in K^*$.

Si, réciproquement, v est une application de K^* dans un groupe ordonné Γ satisfaisant aux conditions (V_I) et (V_{II}), le sous-ensemble A de K composé de 0 et des éléments x de K^* tels que $v(x) \geqslant 0$, est un sous-anneau de K , comme on le vérifie aussitôt. L'ensemble $v^{-1}(0)$ est identique à l'ensemble des éléments inversibles de A . Donc $v(K^*)$ est isomorphe au groupe ordonné $\mathcal{P}^*$ des idéaux principaux fractionnaires de K (relativement à A), par un isomorphisme h tel que l'on ait $v = h \circ p$, p étant l'application canonique de K^* sur $\mathcal{P}^*$. Par conséquent

Théorème 2 - Pour qu'un sous-anneau A d'un corps K soit anneau de valuation, il faut et il suffit qu'il existe une application v de K^* dans un groupe totalement ordonné Γ , satisfaisant aux conditions (V_I) et (V'_{II}), et telle que A^* soit l'ensemble des $x \in K^*$ tels que $v(x) \geqslant 0$.

2 - Notion de valuation.

Etant donné un corps K , il résulte des th.1 et 2 et du cor. de la prop.5 (§ 1) que les données suivantes sont équivalentes :

1) Un sous-anneau A de K , qui soit anneau de valuation et qui admette K pour corps des fractions.

2) Une spécialisation non prolongeable d'un sous-anneau A de K .

3) Une application v de K^* dans un groupe totalement ordonné Γ qui satisfasse aux conditions

(V_I) $v(xy) = v(x)+v(y)$ pour tous x,y de K^*.

(V'_{II}) $v(x+y) \geqslant \min(v(x),v(y))$ pour tous x,y de K^* tels que $x+y \in K^*$.

Définition 1 - Etant donné un corps K, on dit que l'une quelconque des données précédentes définit une valuation du corps K.

Une valuation V d'un corps K définit donc à la fois un sous-anneau A de K, une spécialisation non prolongeable f de A, et une application v de K^* dans un groupe totalement ordonné Γ satisfaisant aux conditions (V_I) et (V'_{II}). Le sous-anneau A est appelé l'anneau de la valuation V ; c'est l'ensemble des $x \in K$ tels que $f(x) \neq \infty$, et aussi la réunion de $\{0\}$ et de l'ensemble des x de K^* tels que $v(x) \geqslant 0$. L'anneau A est un anneau local, dont l'idéal maximal M est la réunion de $\{0\}$ et des x tels que $v(x) > 0$; cet idéal maximal est appelé l'idéal de la valuation V.

L'application f est définie pour tout $x \in K$, grâce aux conventions du $\S 1, n^0 3$. L'application v est définie pour tout x de K^* ; afin de donner un sens à $v(0)$ et $v(\infty)$, nous conviendrons d'adjoindre à tout groupe ordonné Γ deux éléments qui seront toujours notés $+\infty$ et $-\infty$; nous prolongerons à $\Gamma \cup \{-\infty, +\infty\}$ la relation d'ordre de Γ en posant $\gamma \leqslant +\infty$ et $\gamma \geqslant -\infty$ pour tout $\gamma \in \Gamma$; nous prolongerons à $\Gamma \cup \{-\infty, +\infty\}$ la loi de composition de Γ en posant $\gamma+(+\infty) = +\infty$, $\gamma-(-\infty) = +\infty$, $\gamma + (-\infty) = \gamma-(+\infty) = -\infty$ alors, si, on pose $v(0) = +\infty$ et $v(\infty) = -\infty$, on vérifie aussitôt que les conditions (V_I) et (V'_{II}) sont vérifiées, sans restrictions sur les éléments x,y et $x+y$ de K_∞.

Définition 2 - Etant donnée une valuation V d'un corps K , soient f la spécialisation non prolongeable, et v l'application dans un groupe totalement ordonné définies par V . Pour tout x de K les éléments f(x) et v(x) sont appelés la valeur et l'ordre de x pour la valuation V. Si A est l'anneau de V , f(A) est appelé le corps des valeurs de V , et $v(K^*)$ le groupe des ordres de V .

Exemples de valuations - 1) Soit K le corps $K_0((X))$ des séries formelles en une indéterminée X sur un corps K_0 (Alg., chap.IV, § 6, n° 5) ; rappelons que tout élément de K est de la forme $x = \sum_{j=m}^{+\infty} a_j X^j$ $(a_j \in K_0)$, où m est un entier rationnel quelconque, positif ou négatif. Le sous-anneau A de K composé des séries formelles à exposants positifs est un anneau de valuation. Si V désigne la valuation définie par A , l'ordre pour V de la série formelle x est le plus petit entier j tel que le coefficient a_j de X^j soit $\neq 0$; et la valeur de x pour V est ∞ si l'ordre de x est < 0 , et le coefficient a_0 du terme constant de x si x est une série formelle à exposants positifs.

2) Soit p un nombre premier ; pour tout nombre rationnel $x \neq 0$, on définit $v_p(x)$ comme étant l'exposant de p dans la décomposition de x en facteurs premiers (Alg., chap.VII, § 1, n° 3) ; on vérifie aussitôt que v_p satisfait aux conditions (V_I) et (V'_{II}), et prend ses valeurs dans le groupe totalement ordonné Z . Ainsi v_p définit une valuation de Q , appelée la valuation p-adique. L'anneau de la valuation p-adique se compose de 0 et des éléments r/s de Q^* où $r \in Z$, $s \in Z$, et où s n'est pas multiple de p . Les valeurs des éléments de Q pour la valuation p-adique sont les éléments du corps projectif fini (F_p) .

3) L'exemple 2) se généralise aussitôt au corps des fractions de n'importe quel anneau principal (Alg., chap.VII, § 1, déf.1). En particulier, si K est le corps $K_0(X)$ des fractions rationnelles à une indéterminée sur un corps algèbriquement clos K_0, à tout élément a de K_0 correspond une valuation V_a de K : l'ordre de la fraction rationnelle $x \in K$ étant l'exposant avec lequel figure X-a dans la décomposition de x en polynomes irréductibles ; d'autre part l'application v qui à toute fraction rationnelle $x = P(X)/Q(X)$ (P,Q : polynomes) fait correspondre l'entier $d^0Q - d^0P$ définit une valuation V_∞ de K . Nous verrons que ce sont là les seules valuations de $K_0(X)$ dont l'anneau contient K_0 . Ces valuations sont en correspondance biunivoque avec les éléments du corps projectif $(K_0)_\infty$. Dans le cas où K_0 est le corps C des nombres complexes, toute fraction rationnelle $x \in C(X)$ admet un développement en série de Laurent par rapport à $T = x-a$ (ou $1/X$) ; en considérant x comme série formelle en T , on voit aussitôt que la valuation définie à l'exemple 1) coïncide avec V_a (ou V_∞).

4) Considérons le corps $K_0(X,Y)$ des fractions rationnelles à deux indéterminées sur un corps K_0 . Voici quelques valuations de ce corps :

a) On peut considérer $K_0(X,Y)$ comme corps de fractions rationnelles à une indéterminée sur $K_0(X)$, et considérer les valuations correspondant aux polynomes irréductibles de $K_0(X)[Y]$. Toutes ces valuations ont Z pour groupe des ordres ; leurs corps des valeurs sont isomorphes à des extensions algèbriques de $K_0(X)$. Par exemple la valuation définie par l'exposant de Y a un corps des valeurs isomorphes à $K_0(X)$.

b) Des valuations analogues sont obtenues en écrivant $K_0(X,Y) = K_0(Y)(X)$, ou $K_0(X,Y) = K_0(Y/X)(X)$. Si, dans ce dernier cas, on considère la valuation définie par l'exposant de X , X et Y sont éléments de l'idéal de cette valuation.

c) Soit $v(r)$ l'exposant de X dans la fraction rationnelle non nulle $r(X,Y)$. La fraction rationnelle $r_1(X,Y) = X^{-v(r)}r(X,Y)$ est d'ordre 0 pour la valuation V_X définie par v ; donc $r_1(0,Y)$ est un élément non nul de $K_0(Y)$; soit $w(r)$ l'exposant de Y dans $r_1(0,Y)$. Nous poserons $u(r) = (v(r),w(r))$, considéré comme élément du produit lexicographique $Z \times Z$. L'application u vérifie (V_I) puisque $X^{-(v(r)+v(s))}r(X,Y)s(X,Y)$ est d'ordre 0 pour V_X . La condition (V'_{II}) $u(r+s) \geqslant \min(u(r),u(s))$ s'écrit $(v(r+s), w(r+s)) \geqslant$ $\geqslant \min((v(r),w(r),(w(s),w(s))$; si $v(r) < v(s)$, on a $\min((v(r),w(r)), (v(s),w(s)) = (v(x),w(r))$ en vertu de la définition de l'ordre lexicographique, et $v(r+s) = v(r)$ car, si $t(X,Y) = X^{-v(r)}(r+s)$, on a $t(0,Y) = r_1(0,Y)$(où $r = X^{-v(r)}r_1$) , d'où (V'_{II}) car $v(r+s) \geqslant v(r)$ et $w(r+s) = w(r)$; lorsque $v(r)=v(s)$ et $v(r+s) > v(r)$, la condition est encore vérifiée en vertu de la définition de l'ordre lexicographique ; enfin, dans le cas où $v(r)=v(s)=v(r+s)$, les fractions rationnelles $r_1 = X^{-v(r)}r$, $s_1 = X^{-v(r)}s$ et $r_1+s_1 = X^{-v(r)}(r+s)$ sont d'ordre 0 pour V_Y , et on a $w(r+s) \geqslant \min(w(r),w(s))$ en vertu de (V'_{II}) appliquée à $r_1(0,Y),s_1(0,Y)$, et $r_1(0,Y)+s_1(0,Y)$ pour la valuation définie par l'exposant de Y . Ainsi u définit une valuation U de $K_0(X,Y)$. Le groupe des ordres de U est le produit lexicographique $Z \times Z$. L'anneau A de U se compose des fractions rationnelles multiples de X , et de celles r d'ordre 0 pour V_X telles que $r(0,Y)$ n'ait pas Y en facteur de leur dénominateur ; l'idéal de U est engendré, dans A , par Y , et contient les XY^{-n} $(n \in N)$; en particulier X et Y font partie de l'idéal de U . A tout $r \in A$ faisons correspondre 0 si r est multiple de X , et $r(0,0)$ si r est d'ordre 0 pour V_X ; l'application f ainsi

définie satisfait évidemment à $f(rs) = f(r)f(s)$; la relation $f(r+s) = f(r)+f(s)$ également car $r(0,Y)$ est définie pour tout $r \in A$, et égal à 0 pour r d'ordre > 0 pour V_X ; ainsi f est un homomorphisme de A sur K_0, dont le noyau est évidemment l'idéal de U ; l'homomorphisme f est donc une spécialisation équivalente à la spécialisation non prolongeable définie par U ; et K_0 est le corps des valeurs de U .

d) Considérons, dans le corps de séries formelles $K_0((T))$, deux séries formelles x et y algèbriquement indépendantes sur K_0 (par exemple $x=T$ et $y = \sum_{n=1}^{\infty} T^n/n!$ en caractéristique 0). L'application h de $K_0(X,Y)$ dans $K_0((T))$ définie par $h(X)=x$ et $h(Y)=y$ est un isomorphisme. Si nous prenons pour $v(r)$ $(r \in K_0(X,Y))$ l'ordre de la série formelle $h(r)$, v définit une valuation de $K_0(X,Y)$. Cette valuation admet Z pour groupe des ordres et K_0 pour corps des valeurs. Si x et y sont des séries formelles d'ordre > 0, X et Y sont éléments de l'idéal de la valuation ainsi définie. Une telle valuation est appelée une <u>branche analytique</u> de $K_0(X,Y)$.

e) Considérons un nombre réel irrationnel positif a, et le sous-groupe $\Gamma = Z+Za$ de R (ordonné par l'ordre induit). Considérons les "sommes formelles" $\sum_{i=0}^{\infty} a_{\gamma_i} T^{\gamma_i}$ où $a_{\gamma_i} \in K_0$ et où les exposants $\gamma_i \in \Gamma$ forment une suite strictement croissante et tendant vers $+\infty$. On vérifie, comme pour les séries formelles à une indéterminée, que ces sommes formelles constituent un corps F , les opérations étant définies comme l'âne qui trotte (pour le produit on remarque qu'il n'existe qu'un nombre fini de $\gamma_i+\gamma'_j$ inférieurs à un nombre réel donné. On définit l'ordre d'une de ces sommes formelles x comme étant l'exposant du terme non nul de plus petit exposant de x ; ceci définit une valuation de F , ayant Γ pour groupe des ordres et K_0 pour

pour corps des valeurs. Il existe des couples (x,y) d'éléments de F algèbriquement indépendants sur K_o , par exemple $x=T$, $y=T^a$: en effet, dans un polynome $P(x,y) = P(T,T^a)$ tous les termes ont des exposants distincts puisque a est irrationnel, et l'on ne peut avoir $P(x,y)=0$ que si $P=0$. Il existe donc un isomorphisme h de $K_o(X,Y)$ dans F défini par $h(X)=x$ et $h(Y)=y$ (par exemple $h(X)=T$ et $h(Y)=T^a$) ; si nous prenons pour $v(r)$ $(r\in K_o(X,Y))$ l'ordre de h(r), v définit une valuation de $K_o(X,Y)$. Cette valuation admet le sous-groupe dense Γ de R pour groupe des ordres, et K_o pour corps des valeurs. Dans le cas où $h(X)=T$ et $h(Y)=T^a$ $(a > 0)$, X et Y sont éléments de l'idéal de la valuation ainsi définie. Une telle valuation est appelée une <u>branche transcendante</u> de $K_o(X,Y)$.

On remarquera que les valuations définies en b),c),d) et e) définissent des spécialisations non prolongeables (toutes distinctes) qui prolongent la spécialisation $P(X,Y) \to P(0,0)$ de $K_o[X,Y]$.

4) Soit K un corps ; c'est évidemment un anneau de valuation, qui définit une valuation de K , dite <u>valuation triviale</u>. La spécialisation associée à cette valuation est l'automorphisme identique de K . Son groupe des ordres est réduit à $\{0\}$, tout élément non nul de K ayant l'ordre 0 .

2 - <u>Premières propriétés des valuations</u>.

Nous ferons souvent l'abus de langage suivant : étant donnée une valuation V d'un corps K , nous appellerons encore valuation l'application v qui, à tout $x\in K$, fait correspondre son ordre $v(x)$.

<u>Proposition</u> 1 - <u>Soit</u> v <u>une valuation d'un corps</u> K . <u>On a les relations suivantes</u> : $v(1)=0$, $v(-x)=v(x)$, $v(\sum_{i=1}^{m} x_i) \geqslant \min_{1\leqslant i\leqslant m}(v(x_i))$ <u>pour tous</u> $x_i \in K$, <u>et les deux membres de cette dernière relation sont égaux s'il n'y a qu'un seul indice</u> i <u>tel que</u> $v(x_i) = \min_{1\leqslant j\leqslant m}(v(x_j))$.

Comme 1 est inversible dans l'anneau A de la valuation, on a $v(1)=0$. La relation $v(x)=v(-x)$ résulte aussitôt de ce que x et -x sont associés (relativement à A). La relation $v(\sum_{i=1}^{m} x_i) \geqslant \min(v(x_i))$ est évidente pour $m=1$, et identique à (V'_{II}) pour $m=2$; et le cas $m > 2$ se déduit aussitôt de cas $m=2$ par récurrence sur m . Supposons enfin que i soit l'unique indice pour lequel $v(x_j)$ atteigne son minimum ; on a $v(\sum_{j\neq i} x_j) \geqslant \min_{j\neq i}(v(x_j)) > v(x_i)$; d'autre part on a $v(x_i) = v(\sum_{j=1}^{m} x_j + (-\sum_{j\neq i} x_j)) \geqslant \min(v(\sum_{j=1}^{m} x_j), v(\sum_{j\neq i} x_j))$; on en déduit $v(x_i) \geqslant v(\sum_{j=1}^{m} x_j)$, et l'inégalité de l'énoncé montre qu'il a bien égalité dans ce cas.

Corollaire 1 - Si x et y sont des éléments de K tels que $v(x)\neq v(y)$, on a $v(x+y) = \min(v(x),v(y))$.

Ceci est la dernière assertion dans le cas $m=2$.

Corollaire 2 - Si $x_1,\ldots,x_m$ $(m \geqslant 2)$ sont m éléments de K tels que $\sum_{i=1}^{m} x_i = 0$, il existe des indices distincts i et j tels que $v(x_i) = v(x_j) = \min_{1\leqslant k\leqslant m}(v(x_k))$.

Ceci est évident si tous les x_i sont nuls. Sinon on a $+\infty = v(\sum_{k} x_k) \geqslant \min_{1\leqslant i\leqslant m}(v(x_k))$, et le corollaire résulte aussitôt de la dernière assertion de la prop.1 .

Nous avons remarqué, au §1, que la donnée d'une spécialisation d'un anneau d'intégrité A n'entraîne pas automatiquement celle d'une spécialisation de son corps des fractions K . Il n'en est pas de même de la donnée d'une valuation de A (considérée comme application dans un groupe totalement ordonné) :

Proposition 2 - Soit A un anneau d'intégrité, et v une application de A^* dans un groupe totalement ordonné Γ telle que l'on ait $v(xy) = v(x)+v(y)$ et $v(x+y) \geqslant \min(v(x),v(y))$ $(x\in A^*, y\in A^*$, tels que

$x+y \in A^*$ dans la seconde condition) ; on peut alors prolonger, d'une manière et d'une seule, v en une valuation du corps des fractions K de A .

On peut prolonger et de façon unique v en un homomorphisme (que nous noterons encore v) du groupe multiplicatif K^* dans Γ (Alg., chap.I). Soient x et y des éléments de K^* tels que $x+y \in K^*$; il existe $z \in A^*$ tel que $zx \in A$ et $zy \in A$; on a alors $v(x+y) = v(xz+yz) - v(z) \geqslant$ $\geqslant \min(v(xz),v(yz)) - v(z) = \min(v(x)+v(z),v(y)+v(z)) - v(z) = \min(v,x),v(y))$, ce qui montre que v est une valuation de K .

Il résulte enfin du théorème de prolongement qu'on a le résultat suivant :

Théorème 3 - Etant donnée une valuation V d'un corps K , et un surcorps L de K , il existe une valuation de L prolongeant U .

3 - Centre d'une valuation.

Définition 3 - Soient V une valuation d'un corps K , A et M l'anneau et l'idéal de V , et B un sous-anneau de A ; on appelle centre de V sur B l'idéal $M \cap B$ de B .

Comme A/M est un corps, l'anneau quotient $B/(M \cap B)$, qui s'identifie à un sous-anneau de A/M (Alg.,chap.I, §8), est anneau d'intégrité, et le centre (sur B) de V est un idéal premier de B .

Proposition 3 - Etant donnés un corps K , un sous-anneau B de K et un idéal premier P de B , il existe une valuation V de K de centre P sur B .

Il suffit en effet de prolonger à K la spécialisation canonique de B sur B/P (§ 1, th.1).

La notion de centre d'une valuation va nous permettre de déterminer les valuations de certains corps :

Proposition 4 - Un corps fini K n'admet que la valuation triviale.

En effet tout sous-anneau de A est un corps (chap.V, § 1), en particulier l'anneau d'une valuation V de K ; donc l'idéal de V est (0).

Proposition 5 - Toute valuation non triviale du corps Q des nombres rationnels, est une valuation p-adique.

Soit V une valuation non triviale de Q ; l'anneau A de V , qui contient 1 , contient Z . On peut donc parler du centre de V sur Z , et ce centre est un idéal premier de Z , c'est-à-dire de la forme (p), où p est un nombre premier. Ainsi A contient l'anneau local B des éléments r/s ($r \in Z$, $s \in Z$, $s \notin (p)$). Si A était distinct de B , il contiendrait $1/p$, et donc tout nombre rationnel r/sp^n ; il serait alors égal à Q , contrairement au fait que V est non triviale ; par conséquent B est l'anneau de V .

Proposition 6 - Les valuations non triviales du corps de fractions rationnelles $K_o(X)$ qui sont triviales sur K_o sont les valuations définies par les exposants des polynomes irréductibles de $K_o[X]$, et la valuation V_∞ définie par $v(x) = d^oQ - d^oP$ pour $x=P/Q$ (P,Q : polynomes) .

Soit V une valuation non triviale de $K_o(X)$ qui soit triviale sur K_o ; alors son anneau A contient K_o . Supposons d'abord que A contienne l'anneau de polynomes $K_o[X]$; le centre de V sur cet anneau est un idéal premier, donc de la forme (P) où P est un polynome irréductible ; alors A contient l'anneau local B des éléments F/G , où F et G sont des polynomes, et où G n'est pas multiple de P ; si A était distinct de B , il contiendrait $1/p$, et serait égal à $K_o(X)$, contrairement aux hypothèses ; donc $A=B$, et V est la valuation définie par l'exposant de P (NB : on pourrait bloquer la prop.5 et le début de la prop.6 en une seule, relative aux valuations dont l'anneau contient un anneau principal).

Si, au contraire, l'anneau A de V ne contient pas $K_o[X]$, il ne contient pas X ; il contient alors $1/X$, qui fait même partie de l'idéal de V ; alors A contient l'anneau de polynomes $K_o[1/x]$, et, comme le centre de V sur $K_o[1/X]$ contient $1/X$, c'est l'idéal $(1/X)$ en vertu de la première partie ; comme d^oQ-d^oP est l'exposant de $1/x$ dans la décomposition en facteurs irréductibles (par rapport à $K_o[1/X]$) de $x = P(X)/Q(X) = X^{d^oP}P_1(1/X)/X^{d^oQ}Q_1(1/X)$, V est identique à V_∞.

Remarque - Nous avons vu (n^oI, exemple 3)) que les valuations du corps de fractions rationnelles à deux indéterminées $K_o(X,Y)$ qui sont triviales sur K_o sont de types bien plus divers et compliqués ; nous n'essaierons pas d'en donner ici une énumération complète.

Lorsque V est une valuation du corps K(x) des fonctions rationnelles sur une variété W, et si l'anneau A de V contient l'anneau de coordonnées C de W, le centre P de V sur C, qui est un idéal premier de C, définit une sous-variété U de W, que l'on appelle l'origine de la valuation V sur W.

Dans l'exemple 3) (n^o1), on peut considérer $K_o(X,Y)$ comme le corps des fractions rationnelles sur le plan. La valuation définie par l'exposant de Y(a)) admet la droite Y=0 pour origine. Les valuations définies en b),c),d),e) admettent le point (0,0) pour origine.

4 - Valuations discrètes.

Définition 4 - On dit qu'une valuation V d'un corps K est discrète si son groupe des ordres est isomorphe à Z. Une valuation est dite normée si son groupe des ordres est identique à Z.

Il est clair que toute valuation discrète est équivalente à une valuation normée et à une seule. Si elle n'est pas triviale la restriction de V à un sous-corps L de K est aussi une valuation discrète ; car tout sous-groupe de Z est isomorphe ; mais elle n'est pas nécessairement normée, même si V est normée et si sa restriction n'est pas triviale.

Il en est ainsi lorsque V est la valuation de $K_o(X)$ définie par l'exposant de X , et si $L = K_o(X^2)$.

Proposition 7 - Pour qu'un sous-anneau A d'un corps K soit l'anneau d'une valuation discrète, il faut et il suffit qu'il satisfasse aux conditions suivantes :

1) A contient 1 , est distinct de K , et admet K pour corps des fractions.
2) A est un anneau local principal.

Si A est l'anneau d'une valuation discrète V , les conditions 1) sont évidemment satisfaites, et A est un anneau local. Supposons V normée, et soit x un élément d'ordre 1 de A : $v(x)=1$; soit I un idéal de A , et a un élément d'ordre minimum n de I ; pour tout $y \in I$, on a $v(y) \geqslant v(a)$, donc $v(ya^{-1}) \geqslant 0$, $ya^{-1} \in A$, et $I=Aa$; d'autre part, comme $v(a)=v(x^n)$, les éléments a et x^n sont associés (dans A), et on a $I = Ax^n$.

Supposons réciproquement 1) et 2) vérifiées, et soit Ap l'idéal maximal de A . On a $p \neq 0$ puisque $A \neq K$. Soit I l'idéal $\bigcap_{n=1}^{\infty} Ap^n$; comme A est un anneau principal I est de la forme Aq . Puisque $q \in Ap^{n+1}$, on a $qp^{-1} \in Ap^n$ pour tout n , donc $qp^{-1}=aq$, et $q(1-ap)=0$. Comme p n'est pas inversible dans A ceci entraîne $q=0$, et $I=(0)$. Si x est un élément non nul de A , il existe donc un plus grand entier m tel que $x \in Ap^m$; posons $v(x)=m$; on a alors $x = p^{v(x)}x_1$ où x_1 est un élément inversible de A . Si x et y sont des éléments non nuls de A , soit $x=p^{v(x)}x_1$ et $y = p^{v(y)}y_1$ on a alors $xy = p^{v(x)+v(y)}x_1y_1$ où x_1y_1 est inversible ;

on a donc $xy \in Ap^{v(x)+v(y)}$, et $xy \in Ap^{v(x)+v(y)+1}$ est impossible ; par conséquent on a $v(xy)=v(x)+v(y)$. Si, de plus, $x+y$ n'est pas nul, il est clair que l'on a $v(x+y) \geqslant \min(v(x),v(y))$. En vertu de la prop.2, l'application v de A^* dans Z peut se prolonger en une valuation de K, qui est discrète. Si x/y est un élément de K tel que $v(x/y) \geqslant 0$ $(x,y \in A)$ on a $v(x) \geqslant v(y)$, et, en utilisant les notations ci-dessus, $x/y = p^{v(x)-v(y)}x_1y_1^{-1} \in A$; A est donc l'anneau de la valuation v.

Remarque - Il résulte de la prop.7 que les seuls idéaux non triviaux d'un anneau de valuation discrète A sont de la forme Ap^n ; on appelle un générateur p de l'idéal de la valuation discrète V une uniformisante locale pour V.

On peut remplacer la condition 2) par : A est un anneau local dont l'idéal maximal est un idéal principal Ap, et on a $\bigcap_{n=1}^{\infty} Ap^n = (0)$; cette condition d'intersection n'est pas conséquence de la première, comme le montre l'exemple de l'anneau d'une valuation dont le groupe des ordres est $Z \times Z$ ordonné lexicographiquement (cf.n°1, exemple 3)}, c)).

Proposition 8 - Soit V une valuation discrète d'un corps K, et L une extension algèbrique de degré fini n de K ; alors les valuations de L qui prolongent V sont toutes discrètes,.

Soit en effet x un élément de L, et v(x) son ordre pour une valuation prolongeant V. L'élément x est racine d'une équation $\sum_{i=0}^{m} a_i x^i = 0$ $(a_i \in K)$ de degré $\leqslant n$. D'après le cor.2 de la prop.1 il existe deux indices distincts i et j tels que $v(a_ix^i) = v(a_jx^j)$; d'où $(i-j)v(x) = v(a_ja_i^{-1})$. Le groupe des ordres $\Gamma = v(L^*)$ contient donc un sous-groupe Δ isomorphe à Z, et tel que, pour tout $\gamma \in \Gamma$, on ait $n!\gamma \in \Delta$. Comme Γ est un groupe totalement ordonné, l'application $\gamma \to n!\gamma$ est un isomorphisme de Γ sur un sous-groupe (non réduit à $\{0\}$) de Δ ; donc Γ est isomorphe à Z.

Remarque - Le même raisonnement prouve que, si V est triviale, il en est de même de ses prolongements.

5 - Valuations composées ; valuations archimédiennes ; indépendance des valuations.

Nous allons étudier ici les relations entre plusieurs valuations d'un même corps K . Soient donc K un corps, V et V' deux valuations distinctes de K , d'anneaux A et A' . On remarquera d'abord que si B est un sous-anneau de K contenant l'anneau de valuation A , B est lui-même anneau de valuation : en effet, si $x \notin B$, on a $x \notin A$, donc $1/x \in A$ et $1/x \in B$. Par conséquent l'anneau $A[A']$, engendré par A et A' , est un anneau de valuation. On notera que cet anneau n'est autre que l'ensemble AA' des produits aa' où $a \in A$ et $a' \in A'$: en effet AA' est un anneau car, si $a \in A$, $b \in A$, $a' \in A'$ et $b' \in B'$, on a soit $a/b \in A'$, soit $b/a \in A'$, par exemple $b/a \in A'$, d'où $aa'+bb' = a(a'+bb'/a) \in AA'$.

Proposition 9 - Etant données deux valuations V et V' d'un corps K , soient A,A' leurs anneaux, v(x) et v'(x) les ordres de $x \in K$ pour V et V' . Les conditions suivantes sont équivalentes :

a) L'anneau AA' engendré par A et A' est identique à K .

b) Quels que soient a et a' dans K^*, il existe $x \in K^*$ tel que $v(x) \geqslant v(a)$ et $v'(x) \leqslant v'(a')$.

La condition b) entraîne a), car, en prenant a=1, on a $a' = x(a'/x) \in AA'$ pour tout $a' \in K$. Réciproquement, étant donnés a et a' dans K^*, on a $a'/a = bb'$ ($b \in A$, $b' \in A'$) ; si on pose $x = ab$, on a évidemment $v(x) \geqslant v(a)$, et, comme $a' = abb' = xb'$, on a aussi $v'(x) \leqslant v'(a')$

Définition 5 - Deux valuations V et V' satisfaisant aux conditions de la prop.9 sont dites indépendantes.

Théorème 4 - ("théorème d'approximation") - Soit (v_i) $(1 \leqslant i \leqslant n)$ une famille finie de valuations deux à deux indépendantes d'un corps K ; si (a_i) et (b_i) $(1 \leqslant i \leqslant n)$ sont des familles d'éléments de K^* et de K respectivement, il existe $x \in K$ tel que $v_i(x-b_i) \geqslant v_i(a_i)$ pour tout indice i $(1 \leqslant i \leqslant n)$.

Posons d'abord $x = \sum_{i=1}^{n} t_i b_i$; alors $x-b_i = (t_i-1)b_i + \sum_{j \neq i} t_j b_j$; et les conditions étudiées seront satisfaites si l'on a $v_i(t_i-1) \geqslant v_i(a_i/b_i)$ et $v_i(t_j) \geqslant v_i(a_j/b_j)$. Nous sommes donc ramenés, étant donnés n éléments non nuls c_j de K_∞ , à trouver un élément $t \in K$ tel que $v_i(t-1) \geqslant v_i(c_i)$ et $v_j(t) \geqslant v_j(c_j)$ $(j \neq i)$.

Nous pouvons, sans inconvénient, supposer que tous les $v_j(c_j)$ $(1 \leqslant j \leqslant n)$ sont > 0 . Posons $t = z/(z+1)$; alors $t-1 = -(z+1)^{-1}$. Si, pour $j \neq i$, on a $v_j(z) \geqslant v_j(c_j) > 0$, on aura $v_j(z+1) = 0$ (cor.1 de la prop.1) et donc $v_j(t) = v_j(z) \geqslant v_j(c_j)$. Si, d'autre part, on a $v_i(z) \leqslant v_i(1/c_i) < 0$, on aura $v_i(z+1) = v_i(z)$ (cor.1 de la prop.1), et donc $v_i(t-1) = -v_i(z+1) \geqslant v_i(c_i)$. Ainsi (en changeant la numérotation des indices), nous sommes ramenés à démontrer le lemme suivant :

Lemme - Etant données m+1 valuations $v, v_1, \ldots, v_m$ d'un corps K , telles que v et v_i soient indépendantes pour $1 \leqslant i \leqslant m$, et m+1 éléments $a, b_1, \ldots, b_m$ de K^* , il existe $x \in K$ tel que $v(x) \leqslant v(a)$ et $v_i(b_i) \geqslant v_i(x)$ pour $1 \leqslant i \leqslant m$.

Nous pourrons, sans inconvénient, supposer $v(a) < 0$ et $v_i(b_i) > 0$ pour $1 \leqslant i \leqslant m$. Le lemme est conséquence immédiate de la déf.5 pour m=1. Démontrons-le par récurrence sur m . Il existe alors c et d dans K tels que $v(c) \leqslant v(a)$, $v_j(c) \geqslant v_j(b_j)$ pour $j = 1, 2, \ldots, m-1$, $v(d) \leqslant v(a)$ et $v_j(d) \geqslant v_j(b_j)$ pour $j = 2, 3, \ldots, m$. Nous distinguerons quatre cas selon les signes de $v_1(d)$ et $v_m(c)$.

a) Si $v_1(d) \geqslant 0$ et $v_m(c) \geqslant 0$, on prend $x = cd$.

b) Si $v_1(d) \geqslant 0$ et $v_m(c) < 0$, on prend $x = cd/(c+1)$; en effet on a $v(c+1) = v(c)$ puisque $v(c) < 0$, et $v_j(c+1)=0$ $(j=1,\ldots,m-1)$ puisque $v_j(c) \geqslant v_j(b_j) > 0$ (cor.1 de la prop.1) ; d'où $v(x) = v(d) \leqslant v(a)$, et $v_j(x) = v_j(cd) \geqslant v_j(c) \geqslant v_j(b_j)$ pour $1 \leqslant j \leqslant m-1$; enfin, comme $v_m(c) < 0$, on a $v_m(c+1) = v_m(c)$ et $v_m(x) = v_m(d) \geqslant v_m(b_m)$.

c) Si $v_1(d) < 0$ et $v_m(c) \geqslant 0$, on prend de même $x = cd/(d+1)$.

d) Si $v_1(d) < 0$ et $v_m(c) < 0$, on prend $x = dd/(c+d+1)$. En remplaçant éventuellement c par c^2 , on peut, par exemple, supposer que l'on a $v(c) < v(d) < 0$, d'où $v(c+d+1) = v(c)$ et $v(x)=v(d) \leqslant v(a)$. Comme $v_1(d) < 0 < v_1(c)$, on a $v_1(c+d+1) = v_1(d)$, et $v_1(x) = v_1(c) \geqslant v_1(b_1)$; on démontre de même que $v_m(x) \geqslant v_m(b_m)$. Enfin, pour $j=2,\ldots,m-1$, on a $v_j(c) \geqslant 0$ et $v_j(d) > 0$, d'où $v_j(c+d+1)=0$, et $v_j(x)=v_j(cd) \geqslant v_j(c) \geqslant v_j(b_j)$.

Remarque - En faisant abstraction de ce qui se rapporte à la valuation v , le raisonnement ci-dessus montre que, étant donnés m valuations quelconques (v_j) de K et m éléments (b_j) de K , il existe $x \in K^*$ tel que $v_j(x) \geqslant v_j(b_j)$ pour tout j .

Etant données deux valuations non indépendantes V et V' du corps K , l'anneau AA' engendré par les anneaux A et A' de V et V' est distinct du corps K , et contient A et A' . Nous sommes donc amenés à poser la définition suivante :

Définition 6 - Etant donné un corps K , une valuation V de K est dite plus fine qu'une valuation V' de K , si elles sont non triviales, et si l'anneau A de V est contenu dans l'anneau A' de V' .

Avec les notations de la déf.6 soient U et U' les groupes multiplicatifs des éléments inversibles de A et A' . Comme $U \subset U'$, le groupe des ordres $\Gamma' = K^*/U'$ de V' est isomorphe à un groupe quotient Γ/Δ de groupe des ordres $\Gamma = K^*/U$ de V ; nous identifierons Γ' à Γ/Δ. Si P est l'ensemble des éléments positifs de Γ , et P' celui de Γ', nous allons montrer que P' est l'image canonique de $P+\Delta$ dans Γ/Δ , c'est-à-dire celle de AU' dans K^*/U' . En effet, AU' est un sous-anneau de K , puisque, si a et b sont dans A et s' et t' dans U', l'un au moins des deux éléments s'/t' , t'/s' est dans A , et on a, par exemple, $as'+bt' = s'(a + bt'/s') \in AU'$; comme $A \subset AU'$, AU' est un anneau de valuation ; et, comme $AU' \subset A'$, U' est le groupe des éléments inversibles de AU' . Ceci nous montre que l'on a $AU' = A'$ en vertu du lemme suivant :

Lemme - Un anneau de valuation A est entièrement déterminé par la donnée du groupe multiplicatif U de ses éléments inversibles.

En effet la relation "$x \in A$, $x \notin U$" est équivalente à "$x \notin U$. et $x+1 \in U$" (cor.1 de la prop.1).

Si $t' \in U'$ et si $t'=as'$ avec $a \in A$ et $s' \in A'$, on a $1/s' = a(1/t') \in A'$, d'où $s' \in U'$; en d'autres termes, si γ est un élément positif de Δ , et si $0 \leqslant \delta \leqslant \gamma$, on a $\delta \in \Delta$.

Définition 7 - On dit qu'un sous-groupe Δ d'un groupe ordonné Γ est isolé, si $\gamma \in \Delta$ et $0 \leqslant \delta \leqslant \gamma$ entraînent $\delta \in \Delta$.

Nous avons ainsi démontré le résultat suivant :

Proposition 10 - Etant donnés un corps K , une valuation V de K d'anneau A d'idéal M et de groupe des éléments inversibles U , et une valuation V' de K , moins fine que V , d'anneau A', d'idéal M' et de groupe des éléments inversibles U', on a les propriétés suivantes :

a) On a $A \subset A'$, $U \subset U'$, $M \supset M'$ et $AU' = A'$.

b) Le groupe des ordres Γ' de V' est isomorphe à un groupe quotient Γ/Δ du groupe des ordres Γ de V , par un sous-groupe isolé Δ de Γ , l'ensemble P' des éléments positifs de Γ' étant isomorphe à l'image canonique dans Γ/Δ de $P+\Delta$, P désignant l'ensemble des éléments positifs de Γ .

Corollaire - Les valuations de K moins fines que V forment une famille totalement ordonnée par la relation d'ordre "plus fine que" .

En effet ces valuations sont en correspondance biunivoque avec les sous-groupes isolés du groupe des ordres Γ de V . Si Δ et Δ' sont deux sous-groupes isolés de Γ , et si $\Delta' \not\subset \Delta$, il existe un élément positif γ tel que $\gamma \in \Delta'$ et $\gamma \notin \Delta$; alors tout élément positif δ de Δ est inférieur à γ , sinon γ appartiendrait à Δ puisque Δ est isolé ; donc $\delta \in \Delta'$ puisque Δ' est isolé, et $\Delta \subset \Delta'$.

Proposition 11 - Soient V et V' deux valuations d'un corps K telles que V soit plus fine que V', f et f' les spécialisations correspondantes ; alors V définit une valuation V^* du corps des valeurs F' de V' , dont la spécialisation correspondante h est définie par $f = h \circ f'$.

En effet, si $f'(x)=f'(y)$ $(x, y \in K)$, on a, soit $f'(x)=f'(y) = \infty$, c'est-à-dire $x \notin A'$ et $y \notin A'$, donc $x \notin A$ et $y \notin A$ puisque $A \subset A'$, et $f(x)=f(y) = \infty$, soit $f'(x-y)=0$, $x-y \in M'$, donc $x-y \in M$ puisque $M' \subset M$, et $f(x-y)=0$. Ainsi la valeur $f(x)$ ne dépend que de $f'(x)$, ce qui définit une application h de F'_∞ dans le corps projectif F_∞ des valeurs de V . Et il est clair que h est une spécialisation.

Ainsi les valuations plus fines que V' sont en correspondance biunivoque avec les valuations du corps des valeurs F' de V' .

Définition 7 - Avec les notations de la prop.11, la valuation V est dite composée des valuations V' et V^* .

Exemple - La valuation V de $K_o(X,Y)$ ayant le produit lexicographique $Z \times Z$ pour groupe des ordres, définie à l'ex.3,c) (n^o2) est plus fine que la valuation V' définie par l'exposant de X . Dans cet exemple f' est définie par $f'(r(X,Y))=r(0,Y)$ et h par $h(s(y))=s(0)$; ainsi $f(r(X,Y))$ est obtenue en faisant d'abord $X=0$ dans r , puis $Y=0$ dans le résultat obtenu. Et voilà la "prose" où amènent ces savantes contorsions !

Proposition 12 - Etant donnés un sous-anneau B d'un corps K et deux idéaux premiers distincts P et P' de B tels que $P \supset P'$, il existe deux valuations V et V' de K , de centres P et P' sur B , et telles que V soit plus fini que V' . La valuation V' de centre P' peut être donnée à l'avance.

Soit F' le corps des valeurs de V' ; il contient B/P' comme sous-anneau et P/P' est un idéal de ce sous-anneau. On peut prolonger la spécialisation canonique de B/P' sur (B/P')/(B/P') en une spécialisation non prolongeable h de F' (§ 1, th.1) ; soit V^* la valuation définie par h . Alors la valuation V de K composée de V' et V^* répond évidemment à la question.

Nous allons maintenant étudier les valuations les plus fines possible ;

Proposition 13 - Etant donné un anneau local B d'idéal maximal P , il existe une valuation V , de centre P sur B , et telle qu'il n'existe pas de valuation plus fine ayant la même propriété ; le corps des valeurs de V est alors algèbrique sur B/P .

Soit en effet A l'anneau d'une valuation W de centre P sur B (prop.3); l'anneau A contient B . Considérons la famille Φ de tous les anneaux de valuation (de K) contenus dans A et contenant B ; pour tout $A' \in \Phi$, l'idéal maximal M' de A' contient l'idéal maximal M de A (prop.10, a)) ,

donc $M' \cap B = P$ puisque P est maximal. En vertu du th. de Zorn l'existence d'un élément minimal de la famille Φ , ordonnée par inclusion, résulte du lemme suivant :

Lemme - L'intersection d'une famille Φ totalement ordonnée par inclusion (A_α) d'anneaux de valuation d'un corps K est un anneau de valuation A de K .

En effet, si un élément $x \in K$ n'appartient pas à A , il existe un indice β tel que $x \notin A_\beta$; on a alors $x \notin A_\alpha$ pour tout A_α tel que $A_\alpha \subset A_\beta$. Comme les A_α sont anneaux de valuation $1/x$ appartient donc à tous les A_α contenus dans A_β . Et comme Φ est totalement ordonnée, A est l'intersection des A_α contenus dans A_β ; par conséquent, on a $1/x \in A$, et A est anneau de valuation.

Nous avons donc démontré l'existence d'une valuation V la plus fine possible parmi celles dont le centre sur B est P . Si le corps des valeurs F de V n'était pas algèbrique sur B/P , il contiendrait un élément u transcendant sur B/P ; il existerait alors une valuation non triviale de (B/P)(u) triviale sur B/P , par exemple celle définie par l'exposant de u ; nous pourrions alors prolonger celle-ci en une valuation V^* non triviale de F et triviale sur B/P (th.3) ; et la valuation V', composée de V et V^* , serait strictement plus fine que V , et aurait P pour centre sur B , puisque la valeur pour V' de tout élément x de B s'identifie à la classe de x mod.P .

Remarque - En vertu du th. de Zorn, le lemme montre aussi qu'il existe une valuation la plus fine possible parmi celles qui sont plus fines qu'une valuation donnée V .

Etudions enfin les valuations non triviales les moins fines possible d'un corps K, c'est-à-dire celles dont l'anneau est le plus grand possible. Comme à tout sous-groupe isolé Δ du groupe des ordres Γ d'une valuation V correspond une valuation moins fine que V (prop.10,b)), le groupe des ordres Γ d'une valuation non triviale la moins fine possible V n'admet pas d'autres sous-groupes isolés que lui-même et $\{0\}$. Or remarquons que, étant donné un élément γ d'un groupe réticulé Γ, l'ensemble Δ des éléments δ de Γ tels que $|\delta| \leqslant |n\gamma|$ par certain entier n, est un sous-groupe isolé de Γ : en effet, si $\delta \in \Delta$ et $\delta' \in \Delta$, on a $|\delta| \leqslant |p\gamma|$ et $|\delta'| \leqslant |q\gamma|$, p et q étant des entiers positifs, donc $|\delta - \delta'| \leqslant |p\gamma| + |q\gamma| = |(p+q)\gamma|$ et $\delta - \delta'$ appartient à Δ ; et il est clair que Δ est isolé. Nous avons donc démontré le résultat suivant :

Proposition 14 - Pour qu'un sous-anneau A d'un corps K, contenant 1 et distinct de K, soit tel qu'il n'existe pas d'anneau R, autre que A et K, tel que $A \subset R \subset K$, il faut et il suffit que A soit l'anneau d'une valuation V dont le groupe des ordres Γ satisfasse à la condition suivante :

(Arch) Quels que soient $\gamma > 0$, $\gamma' > 0$ dans Γ, il existe un entier naturel n tel que $\gamma' < n\gamma$.

La condition (Arch) a été rencontrée en Top.Géné,chap.V sous le nom d'axiome d'Archimède ; elle exprime que le groupe totalement ordonné Γ est isomorphe à un sous-groupe du groupe additif des nombres réels (loc.cit, §2,exerc.1). Une valuation dont le groupe des ordres satisfait à (Arch) est souvent dite archimédienne.

Une valuation discrète (n°4) est archimédienne. Il en est de même d'une branche transcendante de $K_0(X,Y)$ (n°2,ex.3, e)).

Proposition 15 - Deux valuations archimédiennes distinctes sont indépendantes.

En effet l'anneau AA' engendré par les anneaux A et A' de ces valuations, contient A et A', et est donc égal à K en vertu de la prop.14

Corollaire - Si L est une extension algèbrique finie de degré n d'un corps K , et V une valuation discrète de K , les valuations (V_i) de L qui prolongent V sont en nombre fini $\leqslant n$.

En effet les valuations (V_i) sont discrètes (prop.8), donc archimédiennes, et par conséquent deux à deux indépendantes. Soit (V_i) $(1 \leqslant i \leqslant s)$ une famille finie quelconque de ces valuations ; en vertu du th. d'approximation (th.4) il existe s éléments (t_i) $(1 \leqslant i \leqslant s)$ de L tels que $v_i(t_i - 1) > 0$ et $v_j(t_i) > 0$ pour $i \neq j$. Si les (t_i) n'étaient pas linéairement indépendants sur K , on aurait une relation $\sum_{i=1}^{s} x_i t_i = 0$, où les x_i seraient des éléments non tous nuls de K . Soit, par exemple, x_1 celui des x_i dont l'ordre pour V est le plus petit possible. Comme $v_1(t_1) = v_1(1 + (t_1 - 1)) = 0$ (cor.1 de la prop.1), on a $v_1(x_1 t_1) = v_1(x_1) \leqslant v_1(x_i) < v_1(t_i x_i)$ pour tout $i \neq 1$, contrairement au cor.2 de la prop.1 . Les t_i sont donc linéairement indépendants sur K , et on a $s \leqslant n$, ce qui démontre le corollaire.

---

§ 3 - Eléments entiers sur un anneau.

1 - Caractérisation des éléments entiers.

Théorème 1 - *Soient B un anneau commutatif, x un élément de B et A un sous-anneau de B contenant 1 . Les propriétés suivantes sont équivalentes.*

(E_I) *L'élément x est racine d'un polynome unitaire à coefficients dans A :* $x^n + a_1 x^{n-1} + \ldots + a_n = 0$ $(a_i \in A)$.

(E_{II}) *L'anneau* $A[x]$ *est contenu dans un anneau R qui est un module de type fini sur A .*

Si, de plus, B est un anneau d'intégrité et si L désigne son corps des fractions, les propriétés précédentes sont équivalentes aux suivantes:

(E_{III}) *Pour toute spécialisation f de L telle que f(a) soit fini pour tout* $a \in A$, *f(x) est fini.*

(E_{IV}) *Pour toute valuation v de L dont l'anneau contient A , on a* $v(x) \geqslant 0$.

La propriété (E_I) entraîne (E_{II}) : en effet (E_I) exprime que x est élément du A-module engendré par $(1, x, \ldots, x^{n-1})$; par multiplication par x^p et récurrence sur p , on en déduit que x^{n+p} appartient, pour tout p , à cet A-module, qui est donc égal à l'anneau $A[x]$. Réciproquement, soit $(r_1, \ldots, r_s)$ un système fini de générateurs de l'anneau R , considéré comme A-module ; comme $xr_i \in R$ pour tout i , on a $xr_i = \sum_{j=1}^{s} a_{ij} r_j$ avec $a_{ij} \in A$; ceci est un système de s équations linéaires homogènes reliant les s quantités r_j ; si d désigne le déterminant de ce système, on a $dr_j = 0$ pour tout i (Alg., chap. III), et donc $dr = 0$ pour tout $r \in R$; comme R admet un élément unité, ceci implique $d = 0$; or $d = \det(a_{ij} - \delta_{ij} x)$ est un polynome unitaire de degré s en x à coefficients dans A ; par conséquent (E_{II}) entraîne (E_I) .

Supposons maintenant que B soit un anneau d'intégrité. Comme toute spécialisation de L se prolonge en une valuation de L (§ 1, th. 1), les propriétés (E_{III}) et (E_{IV}) sont équivalentes. Supposons (E_I) vérifiée, et soit $x^n+a_1x^{n-1}+\ldots+a_n=0$ avec $a_i \in A$; considérons une valuation v de L dont l'anneau contienne A ; si on avait $v(x) < 0$, on en déduirait $v(x^n) < v(a_i x^{n-i})$ pour $1 \leqslant i \leqslant n$, contrairement au cor. de la prop. 1 (§ 2) ; on a donc $v(x) \geqslant 0$, et (E_I) entraîne (E_{IV}). Enfin la propriété (E_{III}) entraîne que l'on a $f(1/x) \neq 0$ pour toute spécialisation f qui soit finie sur A ; ceci veut dire que, dans l'anneau $A[1/x]$, l'élément $1/x$ n'est contenu dans aucun idéal premier (§ 1, n° 1) ; il n'est donc contenu dans aucun idéal distinct de $A[1/x]$ puisqu'un tel idéal est contenu dans un idéal maximal, et donc premier (Alg., chap. I, § 8, th.); ainsi $1/x$ est inversible dans $A[1/x]$, et on a $x = a_0 + a_1/x + \ldots + a_n/x^n$, ce qui, par multiplication par x^n , montre que x est racine d'un polynome unitaire à coefficients dans A ; ceci prouve que (E_{III}) entraîne (E_I) .

Définition 1 - Avec les notations du th. 1, l'élément x est dit entier sur l'anneau A s'il vérifie les propriétés $(E_I),\ldots,(E_{IV})$.

Proposition 1 - Soient B un anneau commutatif, et A un sous-anneau de B ; les éléments x de B qui sont entiers sur A forment un sous-anneau C de B ; si B est un anneau d'intégrité, et si L désigne son corps des fractions, C est l'intersection des anneaux de valuation de L contenant A .

La dernière assertion est conséquence immédiate de (E_{IV}), et démontre la première dans le cas où B est d'intégrité. Pour démontrer la première assertion dans le cas général, nous utiliserons (E_{II}) : soient x et y deux éléments de B qui soient entiers sur A ; il existe alors deux

sous-anneaux R et S de B , contenant respectivement x et y , et qui sont des A-modules de type fini ; si (r_i) et (s_j) sont des systèmes finis de générateurs des A-modules R et S , la famille $(r_i s_j)$ est un système de générateurs du sous-anneau T de B engendré par R et S , T étant considéré comme A-module ; comme xy et x+y sont éléments de T , (E_{II}) montre que ce sont des éléments entiers sur A .

Définition 2 - Avec les notations de la prop.2, le sous-anneau C est appelé la fermeture intégrale de A dans B ; si B est le corps des fractions de A , C est appelé la clôture intégrale de A . Un anneau A qui est égal à sa fermeture intégrale dans B (resp. à sa clôture intégrale) est dit intégralement fermé dans B (resp. intégralement clos

Exemples - 1) Tout anneau principal A est intégralement clos : en effet, si x est un élément entier sur A du corps des fractions de A , on a $x = r/s$ où r et s sont des éléments étrangers de A , et (E_I) s'écrit $r^n + a_1 r^{n-1} s + \ldots + a_n s^n = 0$; ainsi s divise r^n , et, comme il lui est étranger (Alg., chap.VI) c'est un élément inversible de A , et on a $x \in A$.

2) Soit K une extension de degré fini n du corps Q des nombres rationnels ; la fermeture intégrale C de l'anneau Z des entiers rationnels dans K est appelée l'anneau des entiers algèbriques de K l'anneau C est un Z-module, et l'espace vectoriel qu'il engendre sur Q est égal à K : en effet, pour tout $x \in K$, on a $r_0 x^n + \ldots + r_n = 0$ avec $r_i \in Q$, et, si s est un entier dénominateur commun des r_i , sx est entier sur Z comme on le voit par multiplication par s^n de la relation précédente. Soit $(b_i)(1 \leqslant i \leqslant n)$ une base de K sur Q , et $x = \sum a_i b_i$ $(a_i \in Q)$ un entier algèbrique de K ; les conjugués $x^{(j)} = \sum_i a_i b_i^{(j)}$ $(1 \leqslant j \leqslant n)$ de x sur Q sont aussi

entiers sur Z en vertu de (E) ; la matrice carrée $(b_i^{(j)})$ est inversible puisque K est séparable sur Q (Alg.,chap.V, § 7,n°2) ; si donc c_{ij} est le cofacteur de $b_i^{(j)}$ dans cette matrice, on a $a_i = \sum_j c_{ij} x^{(j)}$ pour $1 \leqslant i \leqslant n$; par division des b_i par un même entier rationnel s, les c_{ij} se trouvent multipliés par s, et nous pouvons donc les supposer entiers sur Z ; alors les nombres rationnels (a_i) sont entiers sur Z (prop.1), et appartiennent donc à Z (ex.1). Ainsi l'anneau C des entiers algèbriques de K est contenu dans le Z-module engendré par les (b_i), et est donc un Z-module libre ayant une base de n éléments (Alg.,chap.VII) ; une telle base est appelée une base des entiers de K .

(N.B.: l'exemple 2 n'a été inséré que pour montrer au lecteur qu'il est en pays de connaissance ; naturellement sa place est au § 7 des théorèmes d'extension où, avec la même démonstration, il viendra en cor. d'une prop. un peu plus générale : si A est intégrT. clos, et si C est la fermeture int. de A dans une ext. ~~max~~ séparable de degré fini du corps des fractions de A , C est contenu dans un A-module de type fini, et est lui-même de type fini si A est noethérien. Ceci est à la base de la normalisation des variétés).

Proposition 2 - ("transitivité") Si x est entier sur l'anneau B , et si tout élément de B est entier sur le sous-anneau A de B , alors x est entier sur A .

En vertu de (E_I) x satisfait à une équation de dépendance intégrale $x^n + a_1 x^{n-1} + \ldots + a_n = 0$, où $a_i \in B$; il est donc entier sur le sous-anneau B' de B engendré par A et par les coefficients a_i . Or B' est un ~~mmm~~ A-module de type fini, car, d'après (E_I), il est engendré par un nombre fini de monômes en les a_i . Comme $B'[x]$ est un B'-module de

de type fini, il en résulte que c'est un A-module de type fini, et que x est entier sur A d'après (E_{II}).

2 - Notion d'anneau entier sur un autre.

Définition 3 - On dit qu'un anneau commutatif B est entier sur le sous-anneau A si tout élément de B est entier sur A .

Proposition 3 - Soit B un anneau entier sur le sous-anneau A , et S une partie multiplicativement stable de A , composée d'éléments qui ne sont pas diviseurs de 0 dans B ; alors l'anneau de fractions B_s est entier sur A_s . (§ 1, déf.3).

En effet, tout élément de B_s est de la forme x/s où x est entier sur A , et où $s \in S$; par division par s^r d'une équation de dépendance intégrale de degré n de x sur A , on obtient une équation de dépendance intégrale de x/s sur A_s .

Proposition 4 - Soient B un anneau d'intégrité entier sur le sous-anneau A , et P un idéal premier de A ; il existe alors un idéal premier P' de B tel que $P = A \cap P'$.

Il existe en effet (§ 2, prop.3) une valuation V du corps des fractions L de B admettant P pour centre sur A ; l'anneau de V contient B en vertu de (E_{IV}) ; et il suffit de prendre pour P' le centre de V sur B .

Corollaire - Soient A' un anneau entier sur le sous-anneau A , P et Q deux idéaux premiers de A tels que $Q \subset P$, et Q' un idéal premier de A' tel que $Q = A \cap Q'$; il existe alors un idéal premier P' de A' tel que $Q' \subset P'$ et que $P = A \cap P'$.

Il suffit en effet d'appliquer la prop.3 à l'anneau A'/Q' qui contient A/Q et est entier sur lui, comme on le voit en réduisant mod.Q les équations de dépendance intégrale.

Proposition 5 - Avec les notations du cor., P et Q sont distincts si P' et Q' le sont.

En opérant dans A'/Q', on se ramène au cas où $Q' = (0)$. Alors, si x est un élément non nul de P', on a une équation de dépendance intégrale $x^n + a_1 x^{n-1} + \ldots + a_n = 0$ avec $a_i \in A$; comme A' est un anneau d'intégrité, on peut supposer que l'on a $a_n \neq 0$; et, puisque $a_n \in A \cap P' = P$, on a $P \neq (0)$.

§ 3 - Propriétés des anneaux intégralement clos.

Proposition 6 - Si A est un anneau d'intégrité intégralement clos, et si S est une partie multiplicativement stable de A^*, alors l'anneau de fractions A_S est intégralement clos.

Soit en effet x un élément du corps des fractions K de A qui soit entier sur A_S ; on a alors une équation de dépendance intégrale $x^n + b_1 x^{n-1} + \ldots + b_n = 0$ où $b_i \in A_S$. Soit s un dénominateur commun des b_i : $b_i = a_i/s$ où $a_i \in A$ et $s \in S$. En multipliant par s^r la relation ci-dessus, on voit que xs est entier sur A, donc que $xs \in A$ puisque A est intégralement clos. On a donc $x \in A_S$ et A_S est intégralement clos.

On se gardera bien de croire qu'un anneau quotient d'un anneau intégralement clos soit intégralement clos (même s'il est d'intégrité) : par exemple le sous-anneau $K[X^2, X^3]$ de l'anneau de polynomes $K[X]$ sur le corps K n'est pas intégralement clos (X est en effet entier sur cet anneau), bien que ce soit un quotient de l'anneau de polynomes $K[Y,Z]$ que nous démontrerons être intégralement clos (§ 5).

Proposition 7 - Si l'anneau d'intégrité A est intégralement clos, et si x est un élément entier sur A d'une extension L du corps des fractions K de A , le polynome minimal F de x sur K a ses coefficients dans A (et est donc une équation de dépendance intégrale de x sur A).

Soit $G \in A[X]$ un polynome tel que $G(x)=0$ soit une équation de dépendance intégrale de x sur A . On a $G = FH$ où $H \in K[X]$ (Alg., chap.V, § 2,th.1). Soit alors R un anneau de valuation de K contenant A, et I l'idéal de valuation correspondant. Il existe a et b dans K tels que aF et bH aient leurs coefficients dans R , mais que chacun de ces polynomes ait au moins un coefficient en dehors de I ; alors, si F' et H' sont les polynomes obtenus à partir de aF et bH par réduction des coefficients mod.I, on a $F' \neq 0$ et $H' \neq 0$, d'où $F'H' \neq 0$, ce qui veut dire que les coefficients de abG ne sont pas tous dans I . Comme F et H sont des polynomes unitaires a et b sont dans R . Et, comme G a ses coefficients dans R , ab n'est pas élément de I . Ainsi a n'est pas élément de I, et est donc inversible dans R . Par conséquent F a ses coefficients dans R . Et, comme A est l'intersection des anneaux de valuation qui le contiennent (prop.1), F a ses coefficients dans A .

Autre démonstration (qui semble préférable au rédacteur) : les coefficients de F sont (au signe près) les fonctions symétriques élémentaires des conjugués de x sur K ; comme ceux-ci sont entiers sur A , il en est de même de leurs fonctions symétriques élémentaires (prop.1) ; et comme ces dernières sont éléments de K , elles appartiennent à A , puisque A est intégralement clos.

Proposition 8 - Soient A un anneau d'intégrité intégralement clos, P et Q des idéaux premiers de A tels que $Q \subset P$, A' un anneau d'intégrité entier sur A , et P' un idéal premier de A' tel que $P = A \cap P'$;

il existe alors un idéal premier Q' de A' tel que $Q' \subset P'$ et que $Q = A \cap Q'$.

Soit S l'ensemble des éléments de A' qui sont de la forme ab où $a \in A$, $a \notin Q$, $b \in A'$, $b \notin P'$; S est multiplicativement stable, puisque Q et P' sont premiers, et ne contient pas 0 puisque A' est anneau d'intégrité.

Montrons d'abord que S ne rencontre pas l'idéal QA' engendré par Q dans A' . Soit $x \in QA'$; les coefficients q_i de son polynome minimal F sur le corps des fractions K de A sont dans A (prop.7) ; montrons qu'ils sont dans Q . Pour cela soit V une valuation de K admettant Q pour centre sur A . Par définition on a $x = \sum_i x_i y_i$ où $x_i \in Q$ et $y_i \in A'$. Si x_1 est celui des x_i qui ait le plus petit ordre (> 0) pour V , on a $x = x_1 v$ où v est entier sur l'anneau R de V . Comme R est intégralement clos, les coefficients du polynome minimal de v sur K appartiennent à R ; or ceux-ci sont les $q_i x_1^{-i}$; il en résulte que les q_i sont dans le centre Q de V sur A . Ceci étant supposons que x soit de la forme ab, avec $a \in A$, $a \notin Q$, $b \in A'$, $b \notin P'$; alors le polynome minimal de b sur K a pour coefficients les q_i / a^i ; comme ceux-ci sont dans A (prop.7), ils sont dans Q puisque $a \notin Q$; l'équation de dépendance intégrale de b montre alors que l'on a $b^n \in QA' \subset P'$, d'où $b \in P'$, contrairement aux hypothèses.

Considérons alors l'anneau de fractions A'_S . L'idéal QA'_S ne contient pas 1 puisque S ne rencontre pas QA'_S ; il est donc contenu dans un idéal premier I de A'_S (par exemple un idéal maximal). Alors l'idéal $Q' = I \cap A'$ est premier, et ne rencontre pas S sinon $1 \in I$. Il contient Q , mais point d'autres éléments de A que ceux de Q , sinon il rencontrerait S ; ona donc $A \cap Q' = Q$. Et il est contenu dans P' , sinon il rencontrerait S. C.Q.F.D.

Contrairement au cor. de la prop.4 (où les inclusions sont en sens inverse), la prop.8 ne s'étend pas au cas d'un anneau A non intégralement clos (Exemple : $A = K[x,y,z]$ où x et y sont liés par $x^3+y^3-xy = 0$; $A' = K[x,y,z,u]$ où $u = x^2/y$ satisfait à l'équation de dépendance intégrale $u^2-u+xy = 0$ sur A ; $P = (x,y,z)$, $P' = (x,y,z,u)$, $Q = (xz-y,\ x(1+z^3)-z,\ y(1+z^3)-z^2)$; on a alors $(1+z^3)x^2 \equiv zx \equiv y \pmod{Q}$, ce qui, s'il existait Q' répondant aux conditions de la prop.8, impliquerait que la classe de u mod.Q' est inversible, contrairement à $Q' \subset (x,y,z,u)$. Le contenu géomètrique de ceci est clair.

§4.- Anneaux normaux.

Dans toute la suite de ce chapitre nous entendrons par valuation d'un anneau d'intégrité A une valuation du corps des fractions K de A dont l'anneau contienne A . Sauf mention expresse du contraire toutes les valuations considérées seront supposées non triviales. Si V est une valuation d'un corps K nous désignerons systématiquement par la minuscule correspondante v l'application de K^* dans un groupe totalement ordonné définie par V .

1 - Valuations essentielles d'un anneau normal.

Définition 1 - Un anneau A est dit normal si c'est un anneau d'intégrité, et s'il existe une famille Φ de valuations du corps des fractions K de A telle que

a) L'intersection des anneaux des valuations $V \in \Phi$ est égale à A

b) Toutes les valuations $V \in \Phi$ sont discrètes

c) Si $x \in A^*$, il n'existe qu'un nombre fini de valuations $V \in \Phi$ telles que $v(x) > 0$.

Une famille Φ de valuations répondant à ces conditions est appelée une famille de définition de A .

Il résulte de a) qu'un anneau normal est intégralement clos (§ 3, prop.1). La structure des valuations d'un anneau principal (§ 2, n° 3, prop.5) montre qu'un tel anneau est normal ; nous verrons d'autres exemples d'anneaux normaux au § 7 . La condition c) montre aussitôt que, si u est un élément non nul du corps des fractions K d'un anneau normal A , les valuations $V \in \Phi$ pour lesquelles $v(u) \neq 0$ sont en nombre fini.

Etant donnée une valuation V d'un anneau d'intégrité A , nous noterons P(V) le centre de V sur A , qui est un idéal premier de A .

Proposition 1 - Soient A un anneau normal, K son corps des fractions et Φ une famille de définition de A ; pour que la valuation discrète V de A soit telle que l'anneau de fractions $A_{P(V)}$ soit l'anneau de V , il faut et il suffit qu'il existe $u \in K$, $u \notin A$ tel que $uP(V) \subset A$ ..

Posons $P = P(V)$. Supposons d'abord que A_P soit l'anneau d'une valuation discrète de K , et soit x un générateur de son idéal maximal PA_P (§ 2, n°4, prop.7). Pour toute valuation W de A distincte de V , on a $P(W) \not\subset P$: en effet, $P(W) \subset P$ entraîne que A_P est contenu dans l'anneau de W , contrairement au fait que A est un sous-anneau propre maximal de K (§ 2, prop.14). Soient alors $V_1, \ldots, V_s$ les valuations de Φ , non équivalentes à V , et telles que $v_i(x) > 0$; posons $v_i(x) = n_i$. Comme $P(V_i) \not\subset P$, il existe $y_i \in P(V_i)$, $y_i \notin P$; alors l'élément $u = y_1^{n_1} \ldots y_s^{n_s}/x$ est tel que $v(u) = -1$ (V étant supposée normée) et $w(u) \geqslant 0$ pour toute $W \in \Phi$ non équivalente à V . On a donc, pour tout $p \in P$, $v(up) \geqslant 0$ et $w(up) \geqslant 0$, c'est-à-dire $up \in A$ en vertu de la déf.1, a) .

Supposons réciproquement l'existence de $u \in K$, $u \notin A$ tel que $uP \subset A$. Comme $u \notin A$, il existe $W \in \Phi$ telle que $w(u) < 0$; donc, étant donné $y \in A$, on ne peut avoir $w(yu^n) \geqslant 0$ pour tout entier naturel n puisque W est archimédienne, et il existe un entier $n(y) \geqslant 0$ tel que $yu^{n(y)} \in A$ et $yu^{n(y)+1} \notin A$. L'hypothèse $uP \subset A$ implique alors que l'on a $yu^{n(y)} \notin P$, c'est-à-dire $v(yu^{n(y)})=0$ et $v(y)=n(y)v(1/u)$ (ceci montre d'ailleurs que le groupe des ordres de V est engendré par $v(1/u)$, et que V est discrète, ce qu'on aurait pu,éviter de supposer à priori) ; d'où $v(u) < 0$ puisque V est non triviale. La relation $v(y) = n(y)v(1/u)$ montrant que $n(y)$ est entièrement déterminé par y, on a $yu^s \in A$ pour $0 \leqslant s \leqslant n(y)$. Soit $z = y/y'$ un élément de l'anneau de V, y et y' étant éléments de A ; de $v(y) \geqslant v(y')$, on déduit $n(y) \geqslant n(y')$; on a donc $z = yu^{n(y')}/y'u^{n(y')}$ avec $yu^{n(y')} \in A$, $y'u^{n(y')} \in A$ et $y'u^{n(y')} \notin P$, c'est-à-dire $z \in A_P$. Comme l'anneau de V contient évidemmen A_P, il lui est identique, ce qui démontre la prop.1 .

Remarques - 1) Nous ne nous sommes pas servis de la condition c) de la déf.1 dans la seconde partie de la démonstration.

2) Il résulte de la démonstration que l'on a $v(1/u) = 1$ (si V est normée), et que $1/u$ engendre l'idéal maximal de A_P .

Définition 2 - Une valuation non triviale V d'un anneau normal A est appelée une valuation essentielle de A, si elle est discrète, et si son anneau est égal à l'anneau des fractions A_P de son centre P sur A .

Nous dirons, par abus de langage, qu'un idéal premier P d'un anneau d'intégrité A est minimal s'il est minimal dans la famille, ordonnée par inclusion, des idéaux premiers $\neq (0)$ de A . Nous pouvons alors compléter quelque peu la prop.1 :

Proposition 2 - Le centre $P(V)$ sur A d'une valuation essentielle V d'un anneau normal A est un idéal premier minimal ; il existe un élément u du corps des fractions de A tel que $v(u) = -1$ et que $w(u) \geqslant 0$ pour toute valuation essentielle W de A non équivalente à V .

Comme $A_{P(V)}$ est l'anneau d'une valuation discrète, il n'a d'autres idéaux premiers que (0) et son idéal maximal $P(V)A_{P(V)}$; et, comme tout idéal premier de A contenu dans $P(V)$ engendre un idéal premier dans $A_{P(V)}$ ($\S$ 1, prop.3, a)), $P(V)$ est minimal. Prenons alors pour u un élément de K tel que $u \notin A$ et que $uP(V) \subset A$; la démonstration de la seconde partie de la prop.1 a montré que l'on a $v(u) = -1$ (si V est supposée normée). Et, si W est une valuation essentielle de A non équivalente à V , $P(V)$ et $P(W)$ sont distincts (sinon les anneaux de V et W seraient identiques), et on a $P(V) \not\subset P(W)$ puisque $P(W)$ est minimal ; si $x \in P(V)$ et $x \notin P(W)$, on a $w(x)=0$, $ux \in A$, $w(ux) \geqslant 0$, et donc $w(u) \geqslant 0$.

Corollaire - Etant donnés un anneau normal A , des valuations essentielles normées distinctes (V_i) $(1 \leqslant i \leqslant h)$ de A , et des entiers (m_i) $(1 \leqslant i \leqslant h)$, il existe un élément x du corps des fractions K de A tel que $v_i(x) = m_i$ $(1 \leqslant i \leqslant h)$ et $w(x) \geqslant 0$ pour toute valuation essentielle W de A qui n'est équivalente à aucune des V_i .

Supposons d'abord les entiers m_i strictement négatifs ; la prop.2 fournit, pour $1 \leqslant i \leqslant h$, un élément u_i de K tel que $v_i(u_i) = -1$ et $w(u_i) \geqslant 0$ pour toute valuation essentielle W non équivalente à V_i ; alors, d'après la prop.1 ($\S$ 2), l'élément $x = u_1^{m_1} + \ldots + u_h^{m_h}$ répond à la question. On passe de là au cas général "par homothétie" : choisissons des entiers $n_i > m_i$ et pour chaque i un élément non nul

y_i de $P(V_i)$; si on pose $y = \prod_{i=1}^{s} y_i^{n_i}$, on a $v_i(y) > m_i$ pour tout i ; on pourra alors prendre $x = yx'$ où x' est tel que $v_i(x') = m_i - v_i(y) < 0$, et que $w(x) \geqslant 0$ pour toute valuation essentielle W non équivalente à aucune des V_i .

Remarque - Il n'est pas en général possible, dans le cor., de remplacer la condition $w(x) \geqslant 0$ par $w(x)=0$; les anneaux normaux où ce problème est toujours possible sont les anneaux factoriels, que nous étudierons plus loin.

D'autre part un anneau normal possède en général d'autres valuations non triviales que ses valuations essentielles ; les anneaux normaux dont toutes les valuations non triviales sont essentielles sont dx les anneaux de Dedekind que nous étudierons plus loin. Enfin les anneaux qui sont à la fois factoriels et de Dedekind sont les anneaux principaux.

2 - Existence de valuations essentielles d'un anneau normal.

Proposition 3 - Soient A un anneau normal, Φ une famille de définition de A , P un idéal premier de A , et u un élément du corps K des fractions de A tel que $u \notin A$ et $A \cap Au^{-1} \subset P$; il existe alors une valuation $V \in \Phi$ telle que $v(u) < 0$ et $P(V) \subset P$.

Nous supposerons que les valuations de Φ sont normées. D'après la déf.1 il n'y a qu'un nombre fini (> 0) de valuation $V \in \Phi$ telles que $v(u) < 0$; soient $V_1, \ldots, V_s$ celles-ci. Supposons un instant que P ne contienne aucun des centres $P(V_i)$; soit alors x_i un élément de $P(V_i)$ non contenu dans P ; il existe un exposant n_i tel que $v_i(x_i^{n_i}) \geqslant v(1/u)$ puisque V_i est archimédienne ; en posant $x = \prod_{i=1}^{s} x_i^{n_i}$, on a alors $v_i(ux) \geqslant 0$; et, pour $W \in \Phi$ et distincte des V_i , on a $w(ux) \geqslant w(u) \geqslant 0$; d'où $ux \in A$ (déf.1,a)), $x \in Au^{-1}$ et $x \in P$.

Mais, P étant premier, un produit de plusieurs facteurs ne peut s'y trouver sans que l'un de ces facteurs ne s'y trouvât. Notre assertion est donc démontrée par l'absurde.

Corollaire - Si P est un idéal premier $\neq (0)$ de l'anneau normal A, il existe une valuation $V \in \Phi$ dont le centre $\mathfrak{p}(V)$ soit contenu dans P

Il suffit de prendre $u = 1/x$, où x est un élément non nul de P.

Proposition 4 - Soit A un anneau normal, et soit Φ une famille de définition de A ; la famille Φ' des valuations essentielles appartenant à Φ est alors une famille de définition de A.

Les conditions b) et c) de la déf. 1 étant évidemment satisfaites (je les vois d'ici qui se lèchent les babines), il nous suffit de nous occuper de la condition a), c'est-à-dire de montrer que, si u est un élément du complément C de A par rapport à son corps des fractions K, il existe une valuation essentielle $V \in \Phi'$ telle que $v(u) < 0$.

Pour tout $c \in C$ désignons par I_c l'idéal (propre) $A \cap Ac^{-1}$ de A ; la relation $x \in I_c$ est équivalente à "pour tout $V \in \Phi$, on a $v(x) \geqslant \max(0,-v(c))$". Comme les entiers $\geqslant 0$ $\max(0,-v(c))$ sont nuls à l'exception d'un nombre fini, il n'y a qu'un nombre fini d'idéaux I_d $(d \in C)$ contenant I_c. Parmi les idéaux I_d $(d \in C)$ contenant I_a nous pouvons donc en choisir un maximal I_c $(c \in C)$. Montrons que I_c est premier : en effet si x et y sont des éléments de A tels que $x \notin I_c$ et $xy \in I_c$, on a $x \notin Ac^{-1}$, donc $cx \in C$; comme $x \in A$, on a $Ac^{-1}x^{-1} \supset Ac^{-1}$, et $I_{xc} \supset I_c$; mais, comme I_c est maximal, on en déduit $I_{xc} = I_c$; or, de $xy \in I_c$, on déduit $y \in I_{cx}$, c'est-à-dire $y \in I_c$; et, comme $I_c \neq A$, I_c est bien premier. D'autre part, comme $I_c \supset I_u = A \cap Au^{-1}$, nous sommes dans les conditions d'application

de la prop.3 : il existe une valuation $V \in \Phi$ telle que $v(u) < 0$ et que $P(V) \subset I_c$. Mais alors on a $cP(V) \subset cI_c = A$, et V est essentielle d'après la prop.1 .

Corollaire - Dans un anneau normal A , tout idéal premier minimal est le centre d'une valuation essentielle de A , et réciproquement. La famille Φ_o de toutes les valuations essentielles de A est une famille de définition de A , contenue dans toutes les familles de définition de A .

Soit en effet Φ une famille de définition de A ; la famille Φ' des valuations essentielles appartenant à A est alors une famille de définition de A . Si P est un idéal premier minimal de A , le cor. à la prop.3 montre qu'il existe $V \in \Phi'$ tel que $P(V) \subset P$, c'est-à-dire $P(V) = P$; ainsi P est le centre d'une valuation essentielle V (qui est d'ailleurs unique en vertu de la déf.2). Comme une valuation essentielle V de A est entièrement déterminée par l'idéal premier minimal $P(V)$ (prop.2), la famille Φ' est identique à la famille de toutes les valuations essentielles de A .

(N-B : il ne faudra pas oublier de montrer au chap.II qu'un anneau d'intégrité noethérien et intégralement clos est normal).

---

§ 5 - Anneaux factoriels.

Remarquons que, si un idéal premier $P \neq (0)$ d'un anneau normal A est contenu dans un idéal principal Ax distinct de A , P est minimal et égal à Ax : soit en effet V une valuation discrète de A telle que $v(x) > 0$ (§ 4, déf. 1) ; on a $\min_{y \in P} v(y) > \min_{y \in Px^{-1}} v(y)$, donc les idéaux P et Px^{-1} de A sont distincts ; si z est un élément de Px^{-1} non contenu dans P , on a $zx \in P$, d'où $x \in P$ puisque P est premier ; ainsi $P = Ax$, et P est minimal car le même raisonnement appliqué à $P' \subset P$ montre que $P' = Ax$.

Définition 1 - Un anneau A est dit factoriel si c'est un anneau normal, et si tout idéal premier minimal de A est principal.

Comme un anneau principal A est normal (§ 4), c'est aussi un anneau factoriel.

Théorème 1 - Pour qu'un anneau d'intégrité A soit factoriel, il faut et il suffit que l'une des conditions suivantes soit satisfaite :

a) Le groupe ordonné $\mathcal{P}^*$ des idéaux principaux fractionnaires du corps des fractions K de A est isomorphe à une somme directe $Z^{(I)}$ de groupes Z des entiers rationnels.

b) Si (p_α) est une famille d'éléments extrémaux de A telle que tout élément extrémal de A soit associé à un p_α et à un seul, tout élément $x \in K^*$ se met, et d'une seule manière sous la forme

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

où les exposants n_α sont nuls sauf un nombre fini, où u est inversible dans A et où $n_\alpha \geqslant 0$ pour tout α caractérise les éléments de A . Les idéaux Ap_α sont tous distincts, et sont les idéaux premiers minimaux de A ; l'exposant n_α est l'ordre de x pour la valuation essentielle normée de centre Ap_α sur A .

Les conditions a) et b) étant déjà connues pour équivalentes, nous nous occuperons de b) (Alg., chap.VI, § 1, n). Supposons d'abord que A soit un anneau factoriel, et soit Ap_α la famille de ses idéaux premiers minimaux, et V_α la valuation essentielle normée de A de centre Ap_α. Pour $x \in K$, le produit $u = x \prod_\alpha p_\alpha^{-v_\alpha(x)}$ a un sens (§ 4, déf. 1, c)) et on a $v_\alpha(u)=0$ pour toute valuation essentielle V_α de A ; comme ces valuations forment une famille de définition de A, ceci veut dire que u est inversible dans A. Et, si l'on a $x = u \prod_\alpha p^{n_\alpha}$ avec u inversible dans A, le fait que les Ap_α sont des idéaux premiers minimaux distincts implique que, pour $\alpha \neq \beta$, on a $p_\beta \notin Ap_\alpha$, c'est-à-dire $v_\alpha(p_\beta)=0$, d'où $n_\alpha = v_\alpha(x)$; ceci montre l'unicité des exposants n_α.

Si, réciproquement, tout $x \in K^*$ se met, et d'une seule manière sous la forme $x = u \prod_\alpha p_\alpha^{n_\alpha}$, les p_α étant des éléments extrémaux de A, l'application v_α de K dans Z qui, à $x \in K$, fait correspondre l'exposant $n_\alpha = v_\alpha(x)$ est une valuation de K : en effet $v_\alpha(xy)=v_\alpha(x)+v_\alpha(y)$ est évidemment vérifiée à cause de l'unicité de la décomposition (1) ; d'autre part, comme x et y sont des multiples de $\prod_\alpha p_\alpha^{\min(v_\alpha(x), v_\alpha(y))}$, il en est de même de $x+y$ si $x+y \neq 0$, et l'on a $v_\alpha(x+y) \geqslant \min(v_\alpha(x), v_\alpha(y))$ puisque $v_\alpha(a) \geqslant 0$ pour tout α caractèrise les éléments de A. Ainsi A est l'intersection des anneaux des valuations discrètes V_α, et, comme les $v_\alpha(x)$ sont nuls à l'exception d'un nombre fini pour $x \in K^*$, A est un anneau normal (§ 4, déf. 1) et (V_α) une famille de définition de A. Enfin le centre de V_α sur A est l'idéal principal Ap_α puisque $v_\alpha(a) \geqslant 0$ pour tout α caractérise les éléments de A ; ainsi Ap_α est un idéal premier minimal (remarque au début du §), et les V_α sont des valuations essentielles (§ 4, cor. de la prop. 4).

Et, comme la famille (V_α) est une famille de définition de A , elle contient toutes les valuations essentielles de A ($\S$ 4,cor. de la prop.4), et tout idéal premier minimal de A est de la forme Ap_α , ce qui veut dire que A est un anneau factoriel.

La condition a) montre que le groupe ordonné Γ^* est réticulé. On peut donc appliquer aux anneaux factoriels les propriétés de Divisibilité démontrées en Algèbre, chap.VI, $\S$ 1,n , en particulier les notions de pgcd, de ppcm, d'éléments étrangers, et les résultats s'apparentant au lemme d'Euclide. En particulier, du fait que le ppcm d'une famille finie d'éléments deux à deux étrangers de A est égal à leur produit, on déduit le résultat suivant :

Proposition 1 - Dans un anneau factoriel A tout idéal principal Aa distinct de A est à la fois l'intersection et le produit d'une famille finie $(Ap_i^{n_i})$ de puissances d'idéaux premiers minimaux Ap_i .

---

§ 6 - Anneaux de Dedekind.

1 - Anneaux de Dedekind et anneaux principaux.

Définition 1 - Un anneau A est appelé un anneau de Dedekind, si c'est un anneau normal, et si toute valuation non triviale de A est essentiell

Comme les valuations essentielles d'un anneau normal sont caractérisées par le fait que leurs centres sur A sont des idéaux premiers minimaux (§ 4, cor. de la prop. 4), et comme tout idéal premier de A est le centre d'une valuation de A (§ 2, n° 3, prop. 3), on a le résultat suivant:

Proposition 1 - Pour qu'un anneau normal A soit un anneau de Dedekind il faut et il suffit que tout idéal premier non nul de A soit minimal (resp. maximal).

Proposition 2 - Si I est un idéal d'un anneau de Dedekind A, les éléments x de I sont caractérisés par la relation "$v(x) \geqslant \min_{z \in I} v(z)$ pour toute valuation V de A".

Soit J l'ensemble des $x \in A$ tels que $v(x) \geqslant \min_{z \in I} v(z)$ pour toute valuation V de A ; c'est évidemment un idéal de A qui contient I, et nous avons à montrer que $J = I$. Soit $(I:J)$ l'ensemble des $y \in A$ tels que $yJ \subset I$; c'est évidemment un idéal de A dont nous devons montrer qu'il est égal à A. S'il n'en était pas ainsi, $(I:J)$ serait contenu dans un idéal maximal P de A ; d'après la prop. 1 P est le centre d'une valuation essentielle de A, et il existe un élément u du corps des fractions de A tel que $u \in A$ et $uP \subset A$ (§ 4, prop. 1) ; on en déduit

$u(I:J) \subset A$ et $uI \subset A$.

Nous allons en déduire, par récurrence sur n, que l'on a $u^n I \subset A$ pour tout entier naturel n ; en effet, de $\min_{x \in u^n I} v(x) = \min_{x \in u^n J} v(x)$ et de $u^n I \subset A$, on déduit $u^n J \subset A$, d'où $u^n J I \subset I$, $u^n I \subset (I:J)$

et $u^{n+1}I \subset u(I:J) \subset A$. Mais, comme $v(u) < 0$ pour certaine valuation V de A , $u^n I \subset A$ entraîne, pour $a \in I$, $v(a) \geqslant nv(1/u)$ contrairement au fait que V est discrète.

Corollaire - Pour qu'un anneau A soit principal, il faut et il suffit qu'il soit à la fois anneau factoriel et anneau de Dedekind.

Si A est principal, nous avons vu qu'il est aussi factoriel (§ 5) ; et, comme tout idéal premier P de A est principal, il est minimal (remarque au début du § 5, qui mérite donc un énoncé explicite), et A est un anneau de Dedekind (prop.1). Soit, réciproquement I un idéal d'un anneau A qui est à la fois factoriel et de Dedekind ; les entiers $\min_{x \in I} v(x)$ sont nuls sauf un nombre fini ; comme A est factoriel, il existe $a \in A$ tel que $v(a) = \min_{x \in I} v(x)$ pour toute valuation V de A ; alors $a \in I$ (prop.2) et tout élément de I est multiple de a par construction ; ainsi $I = Aa$ et A est principal.

Proposition 3 - Soient K un corps de A un sous-anneau de K intersection d'un nombre fini d'anneaux de valuations discrètes V_i ; alors A est un anneau principal dont les seuls idéaux premiers non nuls sont les centres P_i des V_i .

En effet A est évidemment un anneau normal (§ 4,déf.1), et on peut supposer que les V_i sont des valuations essentielles de A (§ 4,prop.4), c'est-à-dire que les idéaux premiers P_i sont minimaux. Soit alors P un idéal premier de A distinct des P_i ; comme les P_i sont minimaux, on a $P \not\subset P_i$, et il existe $x_i \in P$, $x_i \notin P_i$; de même (les P_i étant supposés distincts) il existe, pour $i \neq j$, $y_{ij} \in P_j$, $y_{ij} \notin P_i$; alors $z_i = x_i \prod_{j \neq i} y_{ij}$ appartient à P , aux P_j pour $j \neq i$, mais non à P_i . Donc $z = \sum_i z_i$ est élément de P , mais d'aucun des P_i .

Ainsi $v_i(z)=0$ pour toutes les valuations V_i, et z est un élément inversible de A, en contradiction avec $z \in P$. Par conséquent les P_i sont les seuls idéaux premiers de A. Comme ils sont minimaux, A est un anneau de Dedekind (prop.2). Donc (prop.2) les éléments x d'un idéal I de A sont caractérisés par "$v_i(x) \geqslant \min_{z \in I} v_i(z)$ pour tout i". Or (§ 4, cor. de la prop.2) il existe un élément $a \in A$ tel que $v_i(a) = \min_{z \in I} v_i(z)$ pour tout i, ce qui montre que l'on a $I = Aa$, et que A est un anneau principal.

2 - Idéaux fractionnaires d'un anneau de Dedekind.

Définition 2 - Soient A un anneau d'intégrité et K son corps des fractions ; on appelle idéal fractionnaire de A un sous A-module I de K qui est contenu dans un module de la forme Au, $u \in K$.

Tout idéal de A est donc un idéal fractionnaire ; pour préciser on appelle parfois idéaux entiers les idéaux de A. Comme l'application $x \to ux$ $(x \in K)$ est un isomorphisme pour les structures de A-modules, les idéaux fractionnaires de A sont de la forme Ju où J est un idéal entier, et où $u \in K$. Les idéaux principaux fractionnaires (Alg., chap.VI, § 1) sont des idéaux fractionnaires.

Soient I et J deux idéaux fractionnaires de A. Le A-module M engendré par les produits xy où $x \in I$, $y \in J$ est un idéal fractionnaire car, si $I \subset Au$ et $J \subset At$, on a $M \subset Aut$. Le module M se compose des sommes de produits xy $(x \in I, y \in J)$. On dit que M est le produit des idéaux fractionnaires I et J, et on écrit $M = IJ$ par abus de notations (IJ ayant été jusqu'ici réservé pour l'ensemble des produits xy où $x \in I$ et $y \in J$). La multiplication ainsi définie dans l'ensemble des idéaux fractionnaires est évidemment associative et commutative ; si A admet un élément unité, A est élément neutre pour

cette multiplication ; l'ensemble des idéaux principaux fractionnaires est stable pour cette multiplication, et constitue un sous-groupe.

Notons enfin que l'intersection $I \cap J$ et la somme $I + J$ de deux idéaux fractionnaires I et J sont des idéaux fractionnaires : c'est évident pour $I \cap J$; et, si $I \subset Au$ et $J \subset At$ $(u \in K , t \in K)$, on peut écrire $u = a/b$ et $v = c/d$ $(a,b,c,d \in A)$, d'où $I \subset Ab^{-1}$, $J \subset Ad^{-1}$ et $I + J \subset A(bd)^{-1}$. L'ensemble $\mathfrak{J}$ des idéaux fractionnaires de A, ordonné par inclusion, est donc réticulé. Et, comme $I \subset I'$ entraîne évidemment $IJ \subset I'J$, la multiplication dans $\mathfrak{J}$ est compatible avec la relation d'ordre, et $\mathfrak{J}$ est muni d'une structure de <u>monoïde réticulé</u>.

<u>Théorème 1 - Pour qu'un anneau d'intégrité A soit un anneau de Dedekind, il faut et il suffit que le monoïde $\mathfrak{J}$ de ses idéaux fractionnaires non nuls soit un groupe. Dans ces conditions $\mathfrak{J}$ est un groupe abélien libre ayant pour générateurs les idéaux premiers non nuls de A ; autrement dit tout idéal fractionnaire I de A est, et de façon unique, produit de puissances d'idéaux premiers de A : $I = \prod_P P^{n(P)}$; on a aussi $I = \bigcap_P P^{n(P)}$, et les éléments x de I sont caractérisés par "$v_P(x) \geqslant n(P)$ pour tout P" , V_P désignant la valuation de A de centre P . Si $I = \prod_P P^{n(P)}$ et $J = \prod_P P^{m(P)}$, on a $IJ = \prod_P P^{n(P)+m(P)}$, $I \cap J = \prod_P P^{\min(n(P),m(P))}$ et $I + J = \prod_P P^{\min(n(P),m(P))}$.</u>

Supposons d'abord que A soit un anneau de Dedekind, et soit I un idéal fractionnaire non nul de A . Comme $I \subset uJ$ où $u \in K$ et où J est un idéal entier, la prop.2 montre que $x \in I$ équivaut à "$v_P(x) \geqslant n(P)$ pour toute valuation V_P ". Soient alors, I, J et IJ des idéaux

fractionnaires définis par $v_p(x) \geqslant n_p$, $v_p(y) \geqslant m_p$, et $v_p(z) \geqslant s_p$; comme $v_p(x)$ $(x \in I)$ et $v_p(y)$ $(y \in J)$ atteignent leurs minima, on a $s_p \leqslant n_p + m_p$; et, comme $v_p(xy) \geqslant n_p + m_p$, on a $v_p(\sum x_i y_i) \geqslant m_p + n_p$ $(x_i \in I,\ y_i \in J)$, d'où $s_p = n_p + m_p$. D'autre part les conditions "$v_p(x) \geqslant n_p$ pour tout P" (les n_p étant nuls à l'exception d'un nombre fini) ne peuvent entraîner $v_p(x) \geqslant n_p' > n_p$ pour au moins un indice P , en vertu de cor. de la prop.2 (§ 4). Comme les $n_p < 0$ sont en nombre fini, la condition "$v_p(x) \geqslant n_p$ pour tout P" définit un idéal fractionnaire, et il y a correspondance biunivoque entre les idéaux fractionnaires de A et les familles (n_p) d'entiers nuls à l'exception d'un nombre fini. D'après ce qui a été vu au début, si I et J correspondent aux familles (n_p) et (m_p), le produit IJ correspond à la famille $(n_p + m_p)$; donc le monoïde $\mathfrak{S}$ est isomorphe au groupe additif $Z^{(\Phi)}$, Φ étant l'ensemble des idéaux premiers distincts de A . Comme l'inclusion $I \subset J$ équivaut aux inégalités $n_p \geqslant m_p$ pour tout P , l'isomorphisme ci-dessus est aussi un isomorphisme pour les structures de groupes ordonnés de $\mathfrak{S}$ et de $Z^{(\Phi)}$ (considéré comme somme directe de groupes ordonnés). Ceci démontre aussitôt les formules relatives à la décomposition en idéaux premiers de $I \cap J$ et de $I+J$. Et l'application répétée de la formule donnant $I \cap J$ montre que, si $I = \prod_P P^{n(P)}$, on a aussi $I = \bigcap_P P^{n(P)}$.

Supposons maintenant que le monoïde $\mathfrak{S}$ des idéaux fractionnaires d'un anneau d'intégrité A soit un groupe. Soient I un idéal de A et I' son inverse ; de $II' = A$, on déduit $1 = \sum_i x_i y_i$ avec $x_i \in I$ et $y_i \in I'$; alors, pour tout $x \in I$, on a $xy_i \in A$ et $x = \sum_i (xy_i)x_i$, ce qui montre que I est engendré par la famille <u>finie</u> (x_i) .

On déduit de ceci que toute famille non vide d'idéaux de A , ordonnée par inclusion, possède un élément maximal (Alg., chap.VII, §1, lemme du th.). Par conséquent le groupe $\mathfrak{J}$, qui est réticulé, est un groupe abélien libre ayant pour base l'ensemble (P_α) des idéaux maximaux de A (alg., chap.VI, §1, n°12, th.). Ainsi, pour tout $I \in \mathfrak{J}$, on a $I = \prod_\alpha P^{n_\alpha(I)}$, les $n_\alpha(I)$ étant nuls à l'exception d'un nombre fini, et déterminés de façon unique ; et l'application $I \to n_\alpha(I)$ est un homomorphisme du groupe ordonné $\mathfrak{J}$ sur Z ; il en est donc de même de la restriction de n_α au sous-groupe $\mathfrak{P}^*$ des idéaux principaux fractionnaires de A . Donc l'application v_α de K^* dans Z définie par $v_\alpha(x) = n_\alpha((x))$ pour $x \in K^*$ satisfait aux conditions (V_I) et (V_{II}) du §2, n°1, et définit donc une valuation discrète V_α de A . Comme les idéaux entiers sont caractérisés par $n_\alpha(I) \geqslant 0$ pour tout α , A est l'intersection des anneaux des valuations V_α . Et, comme les $n_\alpha(I)$ sont nuls à l'exception d'un nombre fini, on a, pour tout $x \in K^*$, $v_\alpha(x) = 0$ sauf pour un nombre fini d'indices α . Ainsi A est un anneau normal, et la famille Φ des valuations V_α est une famille de définition de A (§4, déf.1). Comme P_α est le centre de V_α sur A , et comme Φ contient toutes les valuations essentielles de A (§4, cor. de la prop.4), tous les idéaux premiers minimaux de A sont des P_α , et sont donc maximaux ; donc tout idéal premier de A est minimal, et A est un anneau de Dedekind (prop.1).

Corollaire 1 - Tout idéal d'un anneau de Dedekind admet un système fini de générateurs.

Ceci a été montré en cours de démonstration.

Corollaire 2 - Si I et J sont des idéaux fractionnaires d'un anneau de Dedekind A , le quotient IJ^{-1} est l'ensemble $(I:J)$ des éléments x du corps des fractions K de A tels que $xJ \subset I$.

On a en effet $(I:J)J \subset I$, donc $(I:J) \subset IJ^{-1}$, -et d'autre part $IJ^{-1}J = I$, donc $IJ^{-1} \subset (I:J)$.

§ 2 - Congruences dans un anneau de Dedekind.

Théorème 2 - Soient A un anneau de Dedekind, $(V_i)(1 \leqslant i \leqslant h)$ une famille finie de valuations normées distinctes de A , $(x_i)(1 \leqslant i \leqslant h)$ une famille d'éléments du corps des fractions K de A , et $(m_i)(1 \leqslant i \leqslant h)$ une famille d'entiers rationnels ; il existe alors un élément x de K tel que $v_i(x-x_i) = m_i$ pour $1 \leqslant i \leqslant h$, et $w(x) \geqslant 0$ pour toute valuation W de K distincte des V_i .

Il n'y a qu'un nombre fini de valuations V' de K telles que l'un au moins des $v'(x_i)$ soit < 0 ; en adjoignant à l'ensemble $(V_1,\dots,V_h)$ celles de ces valuations V' qui n'y figurent pas, on obtient un ensemble $(V_1,\dots,V_h,\dots,V_{h+k})$; pour $h < i \leqslant h+k$, nous poserons $x_i = 0$ et $m_i = 0$. Soit m un entier positif tel que $m + v_i(x_j) \geqslant m_s + 1$ pour tous i,j,s compris entre 1 et h+K . Si P_i désigne le centre de V_i sur A , il résulte de la dernière formule du th.1 que l'on a $P_i^m + \prod_{j \neq i} P_j^m = A$, c'est-à-dire qu'il existe des éléments $y_i \in \prod_{j \neq i} P_j^m$, $y'_i \in P_i^m$ tels que $y_i + y'_i = 1$; on a alors $v_i(y_i - 1) \geqslant m$, $v_j(y_i) \geqslant m$ pour $j \neq i$. Posons $x' = \sum_{i=1}^{h+k} x_i y_i$; on a $x' - x_i = x_i(y_i - 1) + \sum_{j \neq i} x_j y_j$, d'où $v_i(x' - x_i) \geqslant \min(v_i(x_i) + v_i(y_i - 1),\ v_i(x_j) + v_i(y_j)) \geqslant m + \min_{1 \leqslant i,j \leqslant h+k} v_i(x_j) \geqslant m_i + 1$. Si $i > h$ on a donc $v_i(x') > 0$; si W est une valuation normée de A distincte des $V_1,\dots,V_{h+k}$, on a $w(x_i) \geqslant 0$, d'où $w(x') \geqslant 0$. Par ailleurs il existe $x'' \in K$ tel que $v_i(x'') = m_i$ pour $1 \leqslant i \leqslant h$, et $w(x'') \geqslant 0$ pour toute autre valuation normée de A (§ 4, cor. de la prop.2). Alors l'élément $x = x' + x''$ possède les propriétés requises (§ 2, prop.1) .

Corollaire - Soient A un anneau qui soit intersection d'un nombre fini d'anneaux de valuations normées V_i d'un corps K , x_i des éléments de K, et m_i des entiers ; il existe un élément $x \in K$ tel que $v_i(x-x_i)=m_i$ pour tout i.

En effet A est un anneau principal (prop.3), donc un anneau de Dedekind.

Proposition 3 ("théorème chinois") - Soient A un anneau de Dedekind, $I_1,\dots,I_h$ des idéaux non nuls de A , et $x_1,\dots,x_h$ des éléments de A . Pour qu'il existe $x \in A$ tel que $x \equiv x_i \pmod{I_i}$ pour $1 \leqslant i \leqslant h$, il faut et il suffit que l'on ait $x_i \equiv x_j \pmod{I_i+I_j}$ pour $1 \leqslant i,j \leqslant h$.

Les conditions sont évidemment nécessaires. Supposons-les remplies. Soient $P_1,\dots,P_k$ tous les idéaux premiers non nuls de A contenant au moins un des idéaux I_i . Pour chaque j $(1 \leqslant j \leqslant k)$ choisissons un indice i(j) tel que l'exposant n(j,i) de P_j dans la décomposition de I_i soit le plus grand possible, et posons $y_j = x_{i(j)}$. Pour $1 \leqslant i \leqslant h$, $x_i - x_{i(j)}$ appartient à $I_i + I_{i(j)}$, donc aussi à $P_j^{n(j,i)} + P_j^{n(j,i(j))} = P_j^{n(j,i)}$. En notant V_j la valuation normée de centre P_j , il existe, en vertu du th.2, un élément $x \in A$ tel que $v_j(x-x_j) = n(j,i(j))$ pour $1 \leqslant j \leqslant k$; on a alors $v_j(x-x_i) \geqslant n(j,i)$ pour $1 \leqslant j \leqslant k$ et $1 \leqslant i \leqslant h$, d'où $x - x_i \in I_i$ pour $1 \leqslant i \leqslant h$.

Remarque - Nous avons vu, en Alg., chap.VI, § 1, exerc. , que la prop.3 reste vraie toutes fois que, dans le monoide réticulé des idéaux de l'anneau A , les opérations de somme et d'intersection sont distributives l'une par rapport à l'autre. Ceci nous donne une nouvelle démonstration de la prop.3 car, si A est un anneau de Dedekind, le monoïde réticulé des idéaux entiers de A est l'ensemble des éléments positifs du groupe réticulé $\mathcal{J}$ des idéaux fractionnaires de A (th.1), et car, dans un groupe réticulé, les opérations sup et inf sont distributives l'une par rapport à l'autre (Alg., chap.VI, § 1, n° 11, cor.2 de la prop.) .

---

§ 7 - Théorèmes de permanence.

Nous allons, dans ce § , montrer que, étant donnés un anneau A et un anneau B construit à partir de A en employant certains procédés, l'anneau B possède certaines propriétés (comme d'être intégralement clos, normal, factoriel, ou de Dedekind) dès que l'anneau A les possède.

1 - Anneaux de fractions.

Proposition 1 - Soient A un anneau d'intégrité et S une partie multiplicativement stable de A ; si A est un anneau normal (resp. factoriel, de Dedekind, principal), il en est de même de l'anneau de fractions A_S.

Soit (V_α) une famille de définition (§ 4, déf. 1) de l'anneau normal A. L'anneau A_S est évidemment contenu dans l'intersection B des anneaux des valuations (V_β) dont le centre sur A ne rencontre pas S . Si $x \in B$, soient (V_i) les valuations, en nombre fini, de la famille de définition donnée, et telles que $v_i(x) < 0$; alors le centre P_i de V_i rencontre S ; soit s_i un élément de $S \cap P_i$. Supposons les (V_i) normées, et soit $v_i(x) = -n_i$, $s = \prod_i s_i^{n_i}$. On a alors $v_i(sx) = 0$ pour tout i . Et, comme on a par hypothèse $v_\beta(xs) \geqslant v_\beta(x) \geqslant 0$ pour tout β , il en résulte que l'on a $xs \in A$, d'où $B = A_S$. Ainsi A_S est un anneau normal admettant (V_β) pour famille de définition. Comme les idéaux premiers de A_S sont tous de la forme PA_S où P est un idéal premier de A ne rencontrant pas S (§ 1, prop. 3), PA_S sera minimal, ou principal, avec P ; donc (§ 5, déf. 1, et § 6, prop. 1) A_S sera factoriel, ou de Dedekind, avec A .

2 - Trace d'un anneau sur un sous-corps.

Proposition 2 - Soient A un anneau d'intégrité, et L un sous-corps du corps des fractions K de A ; si A est un anneau normal, il en est de même de l'anneau $A \cap L$.

Soit $\Phi = (V_\alpha)$ une famille de définition de l'anneau normal A . Alors la famille Ψ des restrictions (W_α) à L des valuations (V_α) de K et l'anneau $A \cap L$ satisfont évidemment aux conditions de la déf.1 (§ 4) ; ainsi $A \cap L$ est un anneau normal.

Mais on notera que, si A est factoriel, il n'en est pas forcément de même de $A \cap L$: exemple $L = Q(\sqrt{-5})$, A = anneau des entiers de l'extension abélienne non ramifiée maximale de L ; A est principal (corps de classes), mais non $A \cap L$. Même histoire si A est de Dedekind: soient k un corps, u,v,x des éléments algébriquement indépendants sur K ; on prend $A = k(u,v)[x]$ et $L = k(x,u+vx)$; un élément de $A \cap L$ est de la forme $P(x,u+vx)/Q(x,u+vx)$ où P et Q sont des polynomes à coefficients dans k , et où $P(x,u+vx)$ est multiple de $Q(x,u+vx)$ dans $k(u,v)[x]$; mais le contenu de $Q(x,u+vx)$, considéré comme élément de $k[u,v][x]$, est égal à 1 , car son terme constant est un polynome en u , et son coefficient dominant un polynome en v ; donc $P(x,u+vx)/Q(x,u+vx)$ est un élément de $k[u,v,x] = k[x,u+vx,v]$; comme il ne dépend que de x et $u+vx$, c'est un polynome en x et $u+vx$; ainsi on a $A \cap L = k[x,u+vx]$ où x et $u+vx$ sont algèbriquement indépendants sur k , et $A \cap L$ n'est pas un anneau de Dedekind à cause des idéaux premiers emboités (x) et $(x,u+vx)$. Naturellement ces exemples ne peuvent être qu'annoncés ici.

Mais voici un contre exemple plus simple, relatif au premier canular : On prend pour A l'anneau de polynomes $K[x,y]$ et pour L le sous-corps $K(x^2,xy,y^2) = K(x^2,y/x)$ de $K(x,y)$; le degré de $K(x,y)$ sur L est 2 . Tout élément de $K[x,y]$ se met sous la forme $P(x^2,xy,y^2) + xQ(x^2,xy,y^2) + yR(x^2,xy,y^2)$ où P,Q,R sont des polynomes, car c'est évident pour un monôme $x^a y^b$. De $P + xQ + yR \in L$, on déduit $xQ+yR = x(Q+(y/x)R) \in L$.

Comme $x \notin L$ et $(Q + (y/x)R) \in L$, ceci implique $Q + (y/x)R = 0$, d'où $xQ + yR = 0$. Par conséquent $A \cap L$ est l'anneau $K[x^2, xy, y^2]$ qui n'est pas factoriel puisque l'on a $(xy)^2 = x^2y^2$ bien que x^2, xy et y^2 soient des éléments extrémaux de $K[x^2, xy, y^2]$.

Ce n°, écrit pour l'édification de Bourbaki (et pour celle personnelle du rédacteur), semble mûr pour le rejet en exercices.

3 - Anneaux de polynomes.

Théorème 1 - Si l'anneau A est normal, l'anneau $A[X]$ des polynomes à une indéterminée sur A est normal. Si A est un anneau factoriel, il en est de même de $A[X]$.

Soit K le corps des fractions de A, et Ψ la famille des valuations essentielles normées de $K[X]$, qui est un anneau principal, donc normal. D'autre part, on a le lemme suivant :

Lemme - Etant donnée une valuation v d'un corps K, on peut prolonger v en une valuation v' du corps K(X) des fractions rationnelles à une indéterminée sur K telle que $v'(\sum_{i=0}^{n} a_i X^i) = \min_{0 \leqslant i \leqslant n} v(a_i)$ où $a_i \in K$ $(1 \leqslant i \leqslant n)$.

En effet posons $v'(f) = \min_{0 \leqslant i \leqslant n} v(a_i)$ si f est le polynome $\sum_{i=0}^{n} a_i X^i$. Si $f \in K[X]$ et $g \in K[X]$, on a évidemment $v'(f+g) \leqslant \min(v'(f), v'(g))$. Pour montrer que $v'(fg) = v'(f)+v'(g)$, f et g étant des polynomes non nuls, remarquons qu'il existe des éléments a et b de K tels que $v'(f) = v(1/a)$ et $v'(g) = v(1/b)$; alors les polynomes af et bg ont leurs coefficients dans l'anneau B de V, et chacun a au moins un coefficient en dehors de l'idéal P de V ; ainsi les polynomes f' et g' de $(B/P)[X]$ obtenus à partir de af et bg par rédaction des coefficients mod.P sont non nuls. Par conséquent leur produit f'g' est non nul ; comme il est obtenu à partir de abfg par

par réduction des coefficients mod.P , ceci montre que les coefficients de abfg sont tous dans B , l'un au moins étant en dehors de P . Autrement dit on a $v'(abfg) = 0$, d'où $v'(fg) = v(1/ab) = v(1/a)+v(1/b) = v'(f)+ v'(g)$. On peut alors prolonger v' en une valuation (notée aussi v') du corps des fractions $K(X)$ de $K[X]$ (§ 2,prop.2).

Considérons alors la famille Φ des valuations essentielles normées de A , et la famille Φ' des valuations V' de $K(X)$ obtenues à partir des $V \in \Phi$ par la méthode du lemme. L'anneau $A[X]$ est évidemment contenu dans l'intersection C des anneaux des valuations de la famille $\Phi' \cup \Psi$. Inversement, si $f \in C$, on a $f \in K[X]$ puisque Ψ est une famille de définition de $K[X]$; et si a est un coefficient de f , on a $v(a) \geqslant v'(f) \geqslant 0$ pour toute $V \in \Phi$, d'où $a \in A$ puisque Φ est une famille de définition de A ; ainsi $C = A[X]$. D'autre part toutes les valuations de $\Phi' \cup \Psi$ sont discrètes. Enfin si $f \in A[X]$, les valuations $w \in \Psi$ telles que $w(f) > 0$ sont en nombre fini par définition, et les valuations $v' \in \Phi'$ telles que $v'(f) > 0$ sont aussi en nombre fini, puisque, si a est un coefficient de f, on a $v(a) \geqslant v'(f) \geqslant 0$. Par conséquent (§ 4,déf.1) l'anneau $A[X]$ est normal et $\Phi' \cup \Psi$ est une famille de définition de $A[X]$.

Supposons maintenant que A soit un anneau factoriel. Si le centre de $V \in \Phi$ sur A est l'idéal principal Ap, il est clair que le centre de $V' \in \Phi'$ sur $A[X]$ est aussi engendré par p . Si $W \in \Psi$ le centre de W sur $K[X]$ est engendré par un polynome irréductible g , que, par multiplication par un élément convenable de K , nous pouvons supposer avoir tous ses coefficients dans A et étrangers dans leur ensemble ; on a alors $v'(g)=0$ pour toute $v' \in \Phi'$, $u(g)=0$ pour

toute $u \in \Psi$ distincte de w, et $w(g)=1$; et ceci montre que le centre de W sur $A[X]$ est engendré par g. Comme les valuations essentielles de $A[X]$ sont toutes contenues dans la famille de définition $\Phi' \cup \Psi$ (§ 4, cor. de la prop.4), les idéaux premiers minimaux de $A[X]$ sont tous principaux, et $A[X]$ est un anneau factoriel (§ 5, déf.1).

La dernière partie de la démonstration nous donne les compléments suivants :

Proposition 3 - Soit $A[X]$ l'anneau des polynomes à une indéterminée sur un anneau factoriel A ; un élément extrémal de $A[X]$ est, ou bien un élément extrémal de A, ou bien un polynome irréductible de $K[X]$ (K désignant le corps des fractions de A) dont les coefficients sont des éléments étrangers dans leur ensemble de A.

Etant donné un polynome $f \in K[X]$, nous appellerons contenu de f (par rapport à A) un pgcd (par rapport à A) des coefficients de f. Il résulte aussitôt de la définition des valuations $V' \in \Phi'$ que l'on a le résultat suivant :

Proposition 4 - Soient A un anneau factoriel, K son corps des fractions, et f un élément de $K[X]$; si $f = u \prod_{v \in \Phi} p_v^{r(v)} \prod_{w \in \Psi} g_w^{r(w)}$ est la décomposition de f en produit d'éléments extrémaux de $A[X]$ (u étant un élément inversible de A, les p_v des éléments extrémaux de A, et les g_w les polynomes irréductibles de contenu 1 de $K[X]$), alors $\prod p_v^{n(v)}$ est un contenu de f.

Corollaire 1 ("lemme de Gauss") - Si f et g sont des éléments de $K[X]$ de contenus c et d, cd est un contenu de fg.

Ceci résulte aussitôt de l'unicité de la décomposition en facteurs extrémaux dans $A[X]$.

Corollaire 2 - Pour que f soit multiple de g par rapport à l'anneau $A[X]$, il faut et il suffit que f soit multiple de g par rapport à $K[X]$ et que le contenu de f soit multiple du contenu de g par rapport à A.

Corollaire 3 - Pour que des polynomes de $A[X]$ soient étrangers dans $A[X]$, il faut et il suffit qu'ils le soient dans $K[X]$, et que leurs contenus soient étrangers dans A.

Théorème 2 - Si A est un anneau factoriel, il en est de même de l'anneau de polynomes $A[X_\iota]$ $(\iota \in I)$.

Ceci est évident par récurrence lorsque I est un ensemble fini (th.1). Dans le cas général remarquons qu'un élément $f \in A[X_\iota]$ ne contient effectivement qu'un nombre fini d'indéterminées $(X_{\iota_1},..,X_{\iota_n})$, et qu'un diviseur g de f ne contient effectivement d'autres indéterminées que celles-ci. Il en résulte d'abord que tout ensemble non vide d'idéaux principaux de $A[X_\iota]$, ordonné par inclusion, contient un élément maximal, puisqu'il en est ainsi dans $A[X_{\iota_1},\ldots,X_{\iota_n}]$ (§ 5, th.1). D'autre part deux éléments f et g de $A[X_\iota]$ sont contenus dans un même anneau de polynomes à un nombre fini d'indéterminées $A[X_{\nu_1},\ldots,X_{\nu_m}]$, et y admettent un pgcd puisque l'anneau en question est factoriel ; et ce pgcd est évidemment un pgcd de f et g dans $A[X_\iota]$. Par conséquent le groupe ordonné $\mathcal{P}^*$ des idéaux fractionnaires principaux de $K(X_\iota)$ (par rapport à $A[X_\iota]$) répond aux conditions du th., n°12, §1, chap.VI d'Algèbre, et $A[X_\iota]$ est un anneau factoriel (§ 5, th.1).

Corollaire 1 - Si K est un corps, l'anneau de polynomes $K[X_\iota]$ $(\iota \in I)$ est factoriel.

Corollaire 2 - L'anneau de polynomes à coefficients entiers $Z[X_\iota]$ ($\iota \in I$) est factoriel.

On remarquera que, ni $K[X_\iota]$ si I a au moins 2 éléments, ni $Z[X_\iota]$ si I n'est pas vide, ne sont des anneaux principaux (cf.exerc.).

Proposition 5 - Soient K un corps, L un surcorps de K , f et g deux polynomes de $K[X_\iota]$ ($\iota \in I$) ; alors un pgcd de f et g dans $K[X_\iota]$ est encore un pgcd de f et g dans $L[X_\iota]$.

On se ramène, comme dans le th.2, au cas où I est un ensemble fini. Dans ce cas nous procèderons par récurrence sur le nombre d'éléments de I . Nous sommes ainsi amenés à montrer que, si A est un sous-anneau factoriel d'un anneau factoriel B tel que deux éléments quelconques de A aient même pgcd dans A et B , alors deux éléments f et f de $A[X]$ ont même pgcd dans $A[X]$ et $B X$. Comme les contenus de f (resp.g) par rapport à A et B sont égaux, nous sommes, en vertu de la prop.4, ramenés à montrer que f et g ont même pgcd dans $K' X$ et dans $L' X$, L' désignant le corps des fractions de B , et K' le sous-corps de L' engendré par A . Or ceci a été démontré dans l'étude des anneaux principaux (Alg.,chap.VII, 1, prop.).

Proposition 6 - Si K est un corps, et f un polynome homogène non nul de degré m de $K[X_1,\ldots,X_n]$, alors tout polynome g qui divise f est homogène.

Soit, en effet $f = gh$. Désignons par g' et h' (Resp.g" et h") les formes de plus haut (resp. plus bas) degré de g et h . Alors g'h' (resp. g"h") est la forme de plus haut (resp. plus bas) degré de gh . Comme gh est homogène, on a donc $g'h' = g"h"$; en comptant les degrés on en déduit $g'=g"$ et $h'=h"$. (Ceci reste vrai avec un anneau intègre à la place du corps K ; ça n'a d'ailleurs rien à voir avec les anneaux factoriels ; il est vrai que Chevalley en donne une démonstration

différente, se servant des résultats de ce n° , mais plus compliquée).

Les propriétés analogues des anneaux de séries formelles sont plus compliquées à démontrer (quand on sait les démontrer). Le rédacteur est prêt à faire un rapport sur la question, si ça intéresse Bourbaki.

4 - Anneaux d'entiers algèbriques.

Théorème 3 - Soient A un anneau d'intégrité, et B la fermeture intégrale de A dans une extension algèbrique L de degré n du corps des fractions K de A ; l'espace vectoriel engendré par B sur K est égal à L ; si A est intégralement clos et L séparable B est contenu dans un A-module de type fini ; si A est un anneau normal (resp. de Dedekind) il en est de même de B .

Si $x \in L$, il satisfait à $x^n + a_1 x^{n-1} + \ldots + a_n = 0$, avec $a_i \in K$; si c est un dénominateur commun des a_i , soit $a = b_i/c$ avec $c \in A$ et $b_i \in A$, on a $(xc)^n + b_1 (xc)^{n-1} + \ldots + b_n c^{n-1} = 0$, ce qui montre que xc est entier sur A et appartient à B . Supposons maintenant A intégralement clos et L séparable ; soient (x_i) une base de L sur K $(1 \leqslant i \leqslant n)$, et $(x_i^{(j)})$ $(1 \leqslant j \leqslant n)$ les conjugués de x_i sur K ; alors la matrice carrée $(x_i^{(j)})$ est inversible, et soit c_{ij} le cofacteur de $x_i^{(j)}$; si on multiplie tous les x_i par un même élément $a \in K$, les c_{ij} sont multipliés par $1/a$; on peut donc supposer que les c_{ij} sont tous entiers sur A ; alors, si $b \in B$, on a $b = \sum_{i=1}^{n} a_i x_i$, d'où , en prenant les conjugués $b^{(j)} = \sum_{i=1}^{n} a_i x_i^{(j)}$, et, par résolution de ce système de n équations linéaires, $a_i = \sum_{j=1}^{n} c_{ij} b^{(j)}$; or les $b^{(j)}$ sont entiers sur A , puisqu'il en est ainsi de b ; donc les a_i sont aussi entiers sur A , et on a $a_i \in A$ puisque A est intégralement clos ; ainsi B est contenu dans le A-module de base (x_i) .

Supposons maintenant que A soit un anneau normal, et soit Φ une famille de définition de A . Les valuations $W(V)$ de L prolongeant $V \in \Phi$ sont toutes discrètes (§ 2, n°4, prop.8) et en nombre fini $\leqslant n$ (§ 2, n°5, cor. de la prop.15). Soit Ψ la famille de ces valuations $W(V)$ où $V \in \Phi$. Si x est un élément de L non contenu dans B , un au moins a_i des coefficients de son polynome minimal $X^n + \sum_{i=1}^{n} a_i X^{n-i}$ est en dehors de A (§ 3, prop.7), et il existe $V \in \Phi$ telle que $v(a_i) < 0$; ceci veut dire que x n'est pas entier sur l'anneau C de V (§ 3, prop.7) ; il existe alors une valuation non triviale U de L dont l'anneau contient C, mais non x ; la restriction U' de U à K est non triviale (§ 2, remarque à la prop.8) ; donc l'anneau de U' est égal à C , puisque C est un sous-anneau propre maximal de K (§ 2, n°5, prop.14), et U appartient à Ψ ; ainsi B est l'intersection des anneaux des valuations $W \in \Psi$. Enfin, si $y \in B$ est d'ordre > 0 pour $W \in \Psi$, le terme constant b de son polynome minimal est d'ordre > 0 pour la restriction de W à K ; comme ceci ne peut se produire que pour un nombre fini de valuations $V \in \Phi$, et comme toute $V \in \Phi$ n'a qu'un nombre fini de prolongements à L , il n'y a qu'un nombre fini de $W \in \Psi$ telles que $w(y) > 0$. Ainsi B est un anneau normal (§ 4, déf.1).

Si B n'est pas un anneau de Dedekind, il existe deux idéaux premiers non nuls et distincts P' et Q' tels que $P' \supset Q'$ (§ 6, prop.1). Alors les idéaux $P' \cap A$ et $Q' \cap A$ sont premiers, non nuls, et distincts (§ 4, prop.5), ce qui montre que A n'est pas anneau de Dedekind. Donc B est anneau de Dedekind s'il en est de même de A .

<u>Corollaire</u> - <u>Si K est une extension de degré fini du corps Q des nombres rationnels, l'anneau B des entiers de K est de Dedekind.</u>

En effet l'anneau Z des entiers rationnels est principal, donc de Dedekind. Les valuations non triviales de B correspondent (§ 6, th.1) aux idéaux premiers P de B ; la valuation correspondant à l'idéal P est appelée valuation P-adique. Remarquons que toute valuation V de K est une valuation P-adique, puisque son anneau contient Z et donc B .

Remarque - Les notations étant celles du th.3, si V est une valuation essentielle de l'anneau normal A , toute valuation W de B prolongeant V est essentielle : si, en effet, le centre P' de W sur B n'était pas un idéal premier minimal, il en serait de même de $P' \cap A$, qui est centre de V (§ 3, prop.5).

5 - Degré local ; indice de ramification.

Définition 1 - Soient W une valuation d'un corps L et V sa restriction à un sous-corps K de L , L' et K' les corps des valeurs de W de V , Γ et Δ les groupes des ordres de W et V ; si L' est de degré fini sur K' on appelle ce degré $[L' : K']$ le degré local de W sur V (ou le degré local de L sur K en W) ; si Δ est d'indice fini dans Γ , on appelle cet indice $(\Gamma : \Delta)$ l'indice de ramification de W par rapport à K .

Lorsque L est algèbrique, ou de degré fini, sur K , L' possède la propriété correspondante sur K' , comme on le voit en se souvenant qu'une valuation définit une spécialisation.

Théorème 4 - Soient K un corps, V une valuation discrète de K , et L une extension algèbrique de degré fini n de K ; les valuations de L prolongeant V sont alors discrètes, et en nombre fini s ; si $V_1, \ldots, V_s$ sont toutes les valuations normées de L prolongeant V , chaque V_i est de degré local fini d_i et d'indice de ramification fini e_i sur V ; on a l'inégalité $\sum_{i=1}^{s} d_i e_i \leqslant n$.

Que les V_i soient discrètes et en nombre fini a déjà été démontré (§ 2, prop.8 et cor.de la prop.15). Alors (en excluant le cas trivial où V est discrète) le groupe des ordres de V_i est Z, et celui de V est un sous-groupe non nul, donc de la forme $e_i\mathbb{Z}$ de Z ; donc V_i est d'indice de ramification fini e_i sur V .

Considérons l'anneau A de V, et l'intersection B des anneaux des valuations V_i . L'anneau B est principal, et a pour seuls idéaux premiers les centres $P_1,\dots,P_s$ des V_i sur B (§ 6, prop.3). L'idéal de la valuation V est un idéal principal Ap de A (§ 2, prop.7). Mettons l'idéal Bp de B sous la forme $\prod_{i=1}^{s} P_i^{a_i} = \bigcap_{i=1}^{s} P_i^{e_i}$, où $a_i = \min_{x \in Bp} v_i(x)$; il est clair que $a_i = v_i(p)$ est le plus petit élément > 0 du groupe des ordres de la restriction de V_i à K ; on a donc $a_i = e_i$. Comme l'anneau de V_i est l'anneau de fractions Bp_i (§ 4, prop.1), le corps des valeurs de V_i est identique à $S_i = B/P_i$. Les S_i sont des espaces vectoriels sur le corps $R = A/Ap$ des valeurs de V . Nous allons montrer que, pour les structures d'espaces vectoriels sur R , B/Bp est isomorphe au produit $\prod_{i=1}^{s} (S_i)^{e_i}$: en effet la structure des idéaux de l'anneaux principal B montre qu'il existe une suite de $e_1+\dots+e_s+1$ idéaux I_j de B , dont le premier est B et le dernier Bp , et telle que $I_j \supset I_{j+1}$, et que $I_j I_{j-1}^{-1}$ soit premier, et égal, par exemple à Bp_i ; comme $x \to xp_i$ est un isomorphisme pour les structures de B-modules, I_{j-1}/I_j est isomorphe à $B/Bp_i = S_i$; et il est clair que S_i figure e_i fois parmi les I_{j-1}/I_j .

Il ne nous reste donc plus qu'à montrer que B/Bp est de dimension $\leqslant n$ sur R , c'est-à-dire que, si $z_1,\dots,z_m$ sont des éléments de B dont les classes $\bar{z}_i$ sont linéairement indépendantes sur R , les z_i sont linéairement indépendants sur K . Dans le cas contraire on aurait $\sum_{i=1}^{m} a_i z_i = 0$, où les a_i sont des éléments non tous nuls de K , que,

par multiplication par un élément convenable de K , nous pouvons supposer tous dans A , l'un au moins étant en dehors de Ap ; en réduisant alors mod.p on obtient une contradiction.

On remarquera que nous avons redémontré la finitude du nombre de prolongements de V (raisonner sur un anneau B intersection d'une famille finie d'anneaux de valuations prolongeant V) .

Proposition 7 - Les notations étant celles du th.3, une condition nécessaire et suffisante pour que l'on ait la "relation des degrés" $\sum_{i=1}^{r} d_i e_i = n$, est que la fermeture intégrale B de l'anneau A de V dans L soit un A-module de type fini ; c'est alors un A-module libre de rang n

Si on a la relation des degrés, la dernière partie de la démonstration du th.4 montre qu'il existe une base $(z_1,\dots,z_n)$ de L sur K telle que $z_i \in B$, et que $(\bar{z}_1,\dots,\bar{z}_n)$ soit une base de B/Bp sur R . Si $x = \sum x_i z_i$ $(x_i \in K)$ appartient à B , les x_i sont dans A , sinon, par multiplication par une puissance positive convenable de p , on aurait $xp^g \in B$ et $xp^g \notin Bp$, contrairement à $x \in B$. Alors $(z_1,\dots,z_n)$ est une base du A-module B .

Si réciproquement B est un A-module de type fini, c'est un A-module libre de rang n puisque A est un anneau principal (Alg.,chap.VII) ; il admet donc une base $(z_1,\dots,z_n)$ sur A , telle que le sous-module Bp ait $(a_1z_1,\dots,a_nz_n)$ avec $a_i \in A$ pour base (Alg.,chap.VII) ; on a évidemment $a_i = p$ pour tout i , et B/Bp est somme directe de n sous-modules isomorphes à A/Ap . Comme $\sum d_i e_i$ est la dimension de l'espace vectoriel B/Bp sur A/Ap , on a donc $\sum_i d_i e_i = n$.

Corollaire - Avec les mêmes notations, on a la relation des degrés $\sum d_i e_i = n$ lorsque L est extension séparable de K .

En effet, le th.3 montre alors que B est contenu dans un A-module de type fini, et est donc lui-même de type fini (et libre) puisque A est un anneau principal.
