Rédaction

COTE : PSMS 003

AUTEUR : Claude Chevalley

TITRE : **(Aucun. Valuations)**
Manuscrit autographe de C. Chevalley
Fragments, pièce unique

FONDS : PIERRE SAMUEL

Nombre de pages numérisées	**049**
Nombre de feuilles prises en compte	**049**

I

1. La relation de divisibilité

~~On rappelle qu'étant donné un anneau σ, un~~ Soit σ un anneau commutatif. On rappelle qu'on dit qu'un élément x de σ est divisible (à droite) par un élément y ~~si~~ s'il existe un élément z de σ tel que $x = yz$.

Cette notion de divisibilité est sans intérêt dans le cas où σ est un corps parce qu'alors, si $y \neq 0$, tout élément est divisible par y. ~~Par~~ Par contre nous avons déjà rencontré deux exemples d'anneaux dans lesquels la notion de divisibilité est du plus haut intérêt ; à savoir celui des entiers rationnels et celui des polynômes en une lettre à coefficients dans un corps. Et l'on peut même dire que la connaissance que nous avons ~~Etant donné~~ du corps des nombres rationnels ou de celui des fractions rationnelles en une lettre à coefficients dans un corps baigne dans une large mesure des propriétés de divisibilité de l'anneau des entiers et de ceux des polynômes dans les corps en question sont les corps des coefficients.

On peut donc se proposer, étant donné un corps K, d'en étudier les sous-anneaux et de ~~déduire~~ faire usage de cette étude pour obtenir des propriétés structurales du corps K lui-même.

Soit donc σ un sous-anneau d'un corps K. On peut généraliser la notion de divisibilité entre ceux des éléments de σ en convenant de dire qu'un élément x de K sera divisible (à droite) par un élément y s'il existe un $z \in \sigma$ tel que $x = yz$ (relativement à l'anneau σ)

(La différence avec la définition préalable est que l'on ne demande pas ici que x et y appartiennent à σ).

• Désignons par $D(x,y)$ la relation "x est divisible (à droite) par y (relativement à σ)". Il est clair que la relation D

est toujours transitive : $D(x,y)$ et $D(y,z)$ entraînent $D(x,z)$. Par ailleurs, ~~si, comme nous le supposerons à part~~ si l'anneau o contient l'élément unité 1 de K, ce que nous supposerons à partir de maintenant, la relation D est réflexive, i.e. $D(x,x)$ est toujours vraie.

~~Les relations transitives et réflexives~~ La relation D est donc d'un type que nous avons déjà rencontré, celui des relations transitives et réflexives — Nous avons vu que ces relations permettent, par passage aux quotients, de construire des relations d'ordre.

Plus précisément, introduisons la relation $A(x,y)$ qui est la conjonction de $D(x,y)$ et de $D(y,x)$. La relation $A(x,y)$ est donc vraie quand chacun des éléments x et y est divisible par l'autre (relativement à l'anneau o). On sait alors que la relation A est une relation ~~équivalence~~ d'équivalence, et que la relation D définit dans l'ensemble quotient $K/A = \overline{K}$ une relation d'ordre $\overline{D}$: si ξ et η sont des éléments de $\overline{K}$, $\overline{D}(\xi,\eta)$ signifie que tout représentant x de la classe ξ est divisible par tout représentant y de la classe η.

Par ailleurs, ~~la relation D est compatible avec la multiplication dans K. En effet~~, si x est divisible par y et x' par y', il est clair que xx' est divisible par yy'. Il en résulte immédiatement que la relation A est ~~elle-même~~ compatible avec la multiplication, donc que l'ensemble $\overline{K}$ se trouve muni d'une loi de composition ~~multiplicative~~, déduite de la multiplication dans K par passage aux quotients.

Le seul élément x tel que $A(x,0)$ soit vrai est 0 (car 0 est déjà le seul élément divisible par 0). L'ensemble $\{0\}$ est donc un élément de $\overline{K}$. Désignons par $\overline{K}^*$ l'ensemble des éléments $\neq 0$ de K et par $\overline{K}^*$ l'ensemble des éléments $\neq \{0\}$ de $\overline{K}^*$. Il en résulte

3

P≥ns 003 4

clair que $\overline{K}^* = K^*/A^*$, où A^* est la restriction de A à K^*. ~~Or, puisque K est un corps, K^* est un groupe multiplicatif ; puisque A^* est compatible avec la multiplication dans K^*, $\overline{K}^*$ est un gr~~ l'ensemble K^* est stable par rapport à la multiplication dans K ; $\overline{K}^*$ est donc stable par rapport à la loi de composition dans $\overline{K}$. Puisque K est un corps, K^* est un groupe multiplicatif. Puisque la relation A^* est compatible avec la multiplication dans K^*, $\overline{K}^*$ contribue un groupe par rapport à la multiplication qu'y est définie. ~~L'ensemble~~

~~Définition~~ Remarque la loi de composition dans K^* sont ~~multi~~ notée multiplicativement, nous noterons additivement la loi de composition qu'on en déduit dans $\overline{K}^*$. Je est clair que la restriction $\overline{D}^*$ de $\overline{D}$ à $\overline{K}^*$ est compatible avec l'addition dans $\overline{K}^*$: i.e. les relations $\overline{D}^*(x,y)$ et $\overline{D}^*(x',y')$ entraînent $\overline{D}^*(x+x', y+y')$.

Changer.

Définition 1.

Changer. Appeler ~~sont~~ $x-y$

On appelle groupe ordonné un groupe additif ~~abe~~ abélien ~~de~~ muni d'une relation d'ordre compatible avec la loi de composition de groupe.

Soit Γ un groupe ordonné, et soient γ, δ des éléments de Γ. Si $\delta \geq \gamma$, on a, puisque $-\gamma \geq -\gamma$, $\delta - \gamma \geq \gamma - \gamma = 0$; inversement, $\delta - \gamma \geq 0$ implique $\delta = \delta - \gamma + \gamma \geq 0 + \gamma = \gamma$. On voit donc que la structure d'ordre de Γ est entièrement déterminée dès qu'on connaît l'ensemble des éléments ≥ 0. Par ailleurs, les conditions $\gamma \geq 0$, $-\gamma \leq 0$ sont équivalentes, et il en est de même des conditions $\gamma > 0$, $-\gamma < 0$.

~~Il résulte de ce que nous avons dit~~ On voit donc que la donnée d'un ~~sous~~-anneau o (contenant l'élément unité) d'un corps K ~~le groupe associé~~ permet de construire un groupe ordonné Γ, dont nous disons que c'est le groupe ordonné associé à o. De plus, on a un homomorphisme φ du groupe multiplicatif K^* des éléments $\neq 0$ de ~~K~~ K sur le groupe additif Γ. ~~Enfin on notera~~

~~Exemples~~

~~Considérons le cas où K est le corps $\mathbb{Q}$ des nombres rationnels, désignons o par l'anneau $\mathbb{Z}$ des entiers. A chaque nombre premier p faisons correspondre l'élément $\varphi(p) = p^*$ du groupe ordonné associé Γ. Les éléments p^* forment alors un système de générateurs~~

??

les éléments $x \in K^*$ tels que $\varphi(x) = 0$ sont ceux pour lesquels $D(x,1)$ et $D(1,x)$ sont tous deux vrais. Or $D(x,1)$ signifie que $x \in \sigma$ et on voit tout de suite que $D(1,x)$ signifie que $x^{-1} \in \sigma$.

Définition 2. On appelle unité d'un anneau σ pourvu d'un élément unité tout élément de σ qui a un inverse dans σ.

On voit donc que $\bar{\varphi}^{-1}(0)$ On voit donc que, si σ est un sous-anneau de K contenant l'élément unité de K, le sous-groupe $\bar{\varphi}^{-1}(0)$ de K^* est le groupe des unités.

4

~~que~~, si x, y, z sont des éléments $\neq 0$ de K tels que $x+y$ soit aussi $\neq 0$, les conditions $\varphi(x) \geq \varphi(z)$, $\varphi(y) \geq \varphi(z)$ entraînent $\varphi(x+y) \geq \varphi(z)$ (en désignant par le signe "$\geq$" la relation d'ordre dans Γ). En effet, ~~dire que $\varphi(t)$~~ si $x = zu$, $y = zv$, avec u et v dans o, on a $x+y = z(u+v)$, et $u+v \in o$.

Enfin, on remarquera que la donnée du groupe ordonné Γ et de l'application φ détermine entièrement l'anneau o. En effet, pour qu'un élément $x \in K$ appartienne à o, il est évidemment nécessaire et suffisant que x soit divisible par 1 relativement à o, i.e. que $\varphi(x) \geq \varphi(1) = 0$. Nous avons donc démontré la

Proposition 1.

Soient K un corps et o un sous-anneau de K contenant l'élément unité. L'anneau o définit alors un homomorphisme φ du groupe multiplicatif K^* des éléments $\neq 0$ de K sur un groupe ordonné Γ. Si x, y, z sont des éléments $\neq 0$ de K et si $x+y \neq 0$, les conditions $\varphi(x) \geq \varphi(z)$, $\varphi(y) \geq \varphi(z)$ entraînent $\varphi(x+y) \geq \varphi(z)$. L'anneau o ~~est l'ensemble des x~~ se compose de 0 et de ceux des éléments $x \in K$ pour lesquels $\varphi(x) \geq 0$. Le sous-groupe $\varphi^{-1}(0)$ ~~démontrons maintenant la~~ de K^* est le groupe des unités de o.

~~Proposition 2~~

2. Valuations.

On dira qu'un groupe ordonné Γ est <u>totalement ordonné</u> s'il est totalement ordonné par sa relation d'ordre.

<u>Definition 3</u>.

<u>On dit qu'un sous-anneau o du corps K est un anneau à valuation</u> si son <u>groupe ordonné associé Γ est totalement ordonné</u>. <u>L'homomorphisme φ du groupe multiplicatif des éléments $\neq 0$ de K sur Γ est alors appelé une valuation du corps K</u>; <u>on dit que o est l'anneau de cette valuation</u>, <u>et que Γ est son groupe de valeurs</u>.

Si on prend par exemple pour ~~k~~ o le corps K lui-même, le groupe ordonné associé se réduit à son élément nul et est totalement ordonné. La valuation correspondante de K s'appelle la <u>valuation triviale</u>.

Si φ est une valuation d'un corps K, le symbole $\varphi(0)$ n'est pas défini. ~~Il est commode d'introduire~~ Soit Γ le groupe des valeurs. Il est commode d'introduire un ensemble Γ_1 ~~(...)~~ composé des éléments de Γ et d'un nouvel élément, que l'on note ∞, et de prolonger la valuation φ en posant $\varphi(0) = \infty$. On étend ~~la~~ à Γ_1 la loi de composition additive de Γ en posant

$$(1) \quad \begin{cases} \infty + \gamma = \infty & \text{pour tout } \gamma \in \Gamma \\ \infty + \infty = \infty \end{cases}$$

et on étend aussi à Γ_1 la relation d'ordre de Γ en convenant que $\infty \geq \infty$ ~~et que~~ $\infty \geq \gamma$ pour tout $\gamma \in \Gamma$, on (2) vérifie tout de suite que la relation ~~ainsi étendue~~ "$\geq$" dans Γ_1 est encore une relation d'ordre et que Γ_1 est totalement ordonné. En vertu des conventions faites, ~~il reste~~ la formule $\varphi(xy) = \varphi(x) + \varphi(y)$ reste vraie même si x ~~ou~~ y

~~seul~~ est nul ; de plus, $\varphi(x) \geq 0$ est la condition nécessaire et suffisante pour que x appartienne à l'anneau de la valuation.

Proposition 2.

$(\varphi(-x) = \varphi(x)$, et Soit φ une valuation d'un corps K. Si x, y sont des éléments de K, on a $\varphi(x+y) \geq \min\{\varphi(x), \varphi(y)\}$. Si de plus $\varphi(x) \neq \varphi(y)$, on a $\varphi(x+y) = \min\{\varphi(x), \varphi(y)\}$. Plus généralement, si $x_1, \dots, x_m$ sont des éléments de K, $(m \geq 1)$ on a $\varphi(\sum_{i=1}^m x_i) \geq \min_{1 \leq i \leq m}\{\varphi(x_i)\}$, et les deux membres de la cette dernière formule sont égaux s'il n'y a qu'un seul indice i pour lequel $\varphi(x_i) = \min_{1 \leq i \leq m}\{\varphi(x_i)\}$.

(relativement à l'anneau de la valuation) ~~On a évidemment $\varphi(1) = 0$~~ Puisque chacun des éléments $x, -x$ est divisible par l'autre, on a $\varphi(-x) = \varphi(x)$. ~~D'où $\varphi(0) = \varphi(1)$~~ L'inégalité $\varphi(x+y) \geq \min\{\varphi(x), \varphi(y)\}$ est évidemment vraie si l'un des éléments x, y ou $x+y$ est nul ; sinon elle résulte de la Prop. 1, § 1 en prenant pour z celui des éléments x, y qui est tel que $\varphi(z) = \min\{\varphi(x), \varphi(y)\}$. ~~L'inégalité $\varphi(\sum_{i=1}^m x_i) \geq \min \sum_{i=1}^m (\varphi(x_i))$ $\min_{1 \leq i \leq m}\{\varphi(x_i)\}$ se démontre immédiatement par récurrence sur m si $m \geq 2$ et est évidente si $m < 2$ $m = 1$.~~ ~~Soient maintenant x, y tels que $\varphi(x) \neq \varphi(y)$, supposons par exemple $\varphi(x) < \varphi(y)$. On a alors $x \neq 0$, $x+y = x(1+y/x)$.~~ Supposons maintenant que ~~$\varphi(x) \neq \varphi(y)$~~ $\varphi(x) < \varphi(y)$. On a $x = x+y+(-y)$, d'où $\varphi(x) \geq \min\{\varphi(x+y), \varphi(-y)\} = \min\{\varphi(x+y), \varphi(y)\}$; ~~Si on avait $\varphi(x+y) \geq \varphi(x)$,~~ il est donc impossible que $\varphi(x+y)$ et $\varphi(y)$ soient tous deux $> \varphi(x)$, d'où $\varphi(x+y) \leq \varphi(x)$. On a aussi $\varphi(x+y) \geq \min\{\varphi(x), \varphi(y)\} = \varphi(x)$, d'où $\varphi(x+y) = \varphi(x) = \min\{\varphi(x), \varphi(y)\}$. On voit de même que, si $\varphi(y) < \varphi(x)$, on a $\varphi(x+y) = \min\{\varphi(x), \varphi(y)\}$; cette dernière formule est donc vraie toutes les fois que $\varphi(x) \neq \varphi(y)$.

L'inégalité $\varphi(\sum_{i=1}^m x_i) \geq \min_{1 \leq i \leq m}\{\varphi(x_i)\}$ est évidente si $m = 1$. Dans le cas où $m = 2$, elle a été démontrée plus haut. Dans le cas où $m > 2$, elle se démontre aisément par récurrence sur m. Supposons qu'il n'y ait qu'un seul indice i_0 pour lequel $\varphi(x_{i_0}) = \min_{1 \leq i \leq m}\{\varphi(x_i)\}$. On a alors $\varphi(\sum_{i \neq i_0} x_i) \geq \min_{i \neq i_0}\{\varphi(x_i)\} > \min_{1 \leq i \leq m}\{\varphi(x_i)\}$

$> \varphi(x_{i_0})$, d'où $\varphi(\sum_{i=1}^m x_i) = \varphi(x_{i_0} + \sum_{i \neq i_0} x_i) = \varphi(x_{i_0})$, et la prop. 2 est démontrée.

Corollaire. Soit φ une valuation d'un corps K, et soient $x_1, \dots, x_m$ des éléments de K tels que $\sum_{i=1}^m x_i = 0$. Si $m \geq 2$, il existe des indices i, j distincts l'un de l'autre tels que $\varphi(x_i) = \varphi(x_j) = \min_{1 \leq k \leq m} \{\varphi(x_k)\}$.

L'existence des indices i et j est évidente si tous les x_i sont nuls. S'il n'en est pas ainsi, on a $\infty = \varphi(\sum_{i=1}^m x_i) > \min_{1 \leq i \leq m} \{\varphi(x_i)\}$ et le corollaire résulte immédiatement de la Prop. 2.

Proposition 3

Soient K un corps, Γ un groupe totalement ordonné et φ un homomorphisme sur Γ du groupe multiplicatif K^* des éléments $\neq 0$ de K. Supposons que la formule $\varphi(x+y) \geq \min\{\varphi(x), \varphi(y)\}$ soit vraie toutes les fois que $x, y, x+y$ sont dans K^*. Il existe alors une valuation φ_0 de K et un isomorphisme h de Γ sur le groupe des valeurs de φ_0 tels que $\varphi_0(x) = h(\varphi(x))$ pour tout $x \in K^*$.

Désignons par σ l'ensemble composé de 0 et des éléments $x \in K^*$ tels que $\varphi(x) \geq 0$. Les conditions $\varphi(x) \geq 0$, $\varphi(y) \geq 0$ entraînent $\varphi(x) + \varphi(y) \geq 0$; puisque $\varphi(xy) = \varphi(x) + \varphi(y)$, on voit que σ est stable par rapport à la multiplication dans K. Soient x, y des éléments de σ; si l'un des éléments $x, y, x+y$ est nul, il est clair que $x+y \in \sigma$; sinon, la conclusion subsiste cependant, puisque l'on a $\varphi(x+y) \geq \min\{\varphi(x), \varphi(y)\} = 0$. Donc σ est stable par rapport à l'addition dans K.

Si u est une unité de σ, on a $u^{-1} \in \sigma$, $\varphi(u) \geq 0$, $\varphi(u^{-1}) = -\varphi(u) \geq 0$, d'où $\varphi(u) = 0$. En particulier on a $\varphi(-1) = 0$. La condition $x \in \sigma$ entraîne donc $\varphi(-x) = \varphi(-1) + \varphi(x) = \varphi(x) \geq 0$, soit $-x \in \sigma$.

On voit donc que σ est un sous-anneau de K; il est clair que ce sous-anneau possède un élément unité. Il correspond à l'anneau σ un homomorphisme φ_0 de K^* sur un groupe ordonné Γ_0.

~~si~~ ~~Si x est une unité de σ, on a~~ d'ensemble $\varphi_0(0)$ est le groupe U des unités de σ (Prop. 1, §1.1) et on a vu que $\varphi(U) = \{0\}$. Inversement, si $u \in K^*$ est tel que $\varphi(u) = 0$, on a $\varphi(u^{-1}) \geq 0$, d'où $u^{-1} \in \sigma$, $u \in U$. On voit donc que $\varphi_0(0) = \bar{\varphi}(0)$. On en conclut qu'il existe un isomorphisme h de la structure de groupe de Γ sur celle de Γ_0 tel que ~~$\varphi_0(x) = h(\varphi(x))$ pour tout~~ $\varphi_0 = h \circ \varphi$. Il reste à montrer que h est aussi un isomorphisme pour la structure d'ordre. Si ~~$x, y \in K^*$~~ x et y sont dans K^*, la condition $\varphi(x/y) \geq 0$ $\varphi(x) \geq \varphi(y)$ équivaut à $\varphi(x/y) \geq 0$, i.e. à $x/y \in \sigma$; elle signifie que x est divisible par y relativement à σ, donc que $\varphi_0(x) \geq \varphi_0(y)$, ce qui achève la démonstration de la proposition 3.

Si φ est un homomorphisme du groupe K^* dans un groupe totalement ordonné Δ, ~~et si la condition formule $\varphi(x+y) \geq \min\{\varphi(x), \varphi(y)\}$~~ l'ensemble $\varphi(K^*) = \Gamma$ est un sous-groupe de Δ sur lequel la structure d'ordre dans Δ induit une structure de groupe totalement ordonné. Si la formule $\varphi(x+y) \geq \min\{\varphi(x), \varphi(y)\}$ est vraie toutes les fois que $x, y, x+y$ sont dans K^*, l'ensemble σ composé de 0 et des $x \in K^*$ tels que $\varphi(x) \geq 0$ est un anneau de valuation. Par extension, on dit encore dans ce cas que φ est une valuation du corps K, que σ est l'anneau de la valuation φ et que Γ est son groupe des valeurs. Deux valuations φ, φ' du corps K sont dites <u>équivalentes</u> quand elles ~~admet~~ ont le même anneau de valuation. Une condition nécessaire et suffisante pour qu'il en soit ainsi est qu'il existe un isomorphisme h de la structure de groupe ordonné du groupe des valeurs Γ de φ sur celle du groupe des valeurs Γ' de φ' tel que $\varphi' = h \circ \varphi$. Si φ est une valuation quelconque, on convient (comme nous l'avons fait plus haut) d'étendre φ en posant $\varphi(0) = \infty$, où ∞ est un symbole soumis aux règles (2) ci-dessus. Il est clair que la proposition 2 reste valable sans modification.

<u>Proposition 3</u>.

<u>Soient φ une valuation d'un corps K et L un sous-corps de K. La restriction de φ à L est alors une valuation de L.</u>

C'est évident.

PSTS 003 11

3. ~~Exemples de valuations~~.

Nous allons maintenant ~~chercher à~~ caractériser les sous-anneaux d'un corps K qui sont des anneaux de valuation.

Proposition 4

Une condition nécessaire et suffisante pour qu'un sous-anneau σ d'un corps K soit un anneau de valuation est que l'inverse de tout élément ~~n'appartenant~~ de K n'appartenant pas à σ soit dans σ.

Supposons d'abord que σ soit l'anneau d'une valuation φ. Si x n'appartient pas à σ, on a $\varphi(x) < 0$, d'où $\varphi(x^{-1}) = -\varphi(x) > 0$ et $x^{-1} \in \sigma$. Supposons maintenant que σ satisfasse à la condition énoncée. Il est d'abord évident que $1 = 1^{-1} \in \sigma$. Soit Γ le groupe ordonné associé à σ, et ~~soit~~ φ l'homomorphisme ~~sur~~ Γ du groupe multiplicatif (K^*) des éléments $\neq 0$ de K (cf. Prop. 1, § 1), γ, δ soient des éléments de Γ tels que γ ne soit pas $\leqslant \delta$, on peut écrire $\gamma = \varphi(x)$, $\delta = \varphi(y)$, où $x \in K^*$, $y \in K^*$, et y n'est pas divisible par x relativement à σ. Donc $y/x \notin \sigma$, d'où $x/y = (y/x)^{-1} \in \sigma$; x est donc divisible par y relativement à σ, et on a $\delta \leqslant \gamma$; donc Γ est totalement ordonné et σ est un anneau de valuation.

~~Le groupe additif $\mathbb{Z}$ des entiers, muni de sa structure d'ordre, est évidemment un groupe totalement ordonné~~.

Définition

Une valuation φ d'un corps K est dite simple si son groupe de valeurs Γ est isomorphe au groupe additif $\mathbb{Z}$ des entiers ; ~~cette~~ la valuation simple φ est dite normée si Γ est le groupe $\mathbb{Z}$ lui-même muni de la relation d'ordre qui existe dans $\mathbb{Z}$.

Il convient d'observer qu'il revient au même de postuler l'existence d'un isomorphisme de la structure de groupe de Γ sur celle de $\mathbb{Z}$ ou d'un isomorphisme de la structure de groupe ordonné de Γ sur celle de $\mathbb{Z}$. Supposons en effet qu'il existe un isomorphisme h de la structure de groupe de Γ sur celle de $\mathbb{Z}$; ~~et~~ Soit γ l'élément de Γ ~~qui corr~~ tel que $h(\gamma) = 1$. On a donc pour tout entier z, $h(z\gamma) = z$. Si $\gamma > 0$, h est un isomorphisme de la structure

~~de groupe ordonné de Γ sur celle de $\underline{Z}$; sinon, si~~ ~~application isomorphisme $\gamma \to -\gamma$ est un isomor~~ On obtient un isomorphisme de la structure de groupe ordonné de Γ sur celle de $\underline{Z}$ en prenant l'application h dans le cas où $\gamma > 0$ et l'application $-h$ (définie par $(-h)(\delta) = -h(\delta)$) si $\gamma < 0$.

Toute valuation simple est équivalente à une valuation normée et à une seule. Si on observe que tout sous-groupe $\neq \{0\}$ de $\underline{Z}$ est isomorphe à $\underline{Z}$, on voit que la restriction φ à un sous-corps K d'un corps L d'une valuation simple ψ de L est ou bien triviale ou bien une valuation simple de K. Par contre, si ψ est normée, φ n'est pas en général normée (même si φ n'est pas triviale).

Proposition.

Pour qu'un sous-anneau o d'un corps K soit l'anneau d'une valuation simple de K, il faut et suffit qu'il satisfasse aux conditions suivantes : 1) o contient 1, est $\neq K$ et ~~K~~ est le corps des quotients de o ~~est K~~ ; 2) les éléments de o qui ne sont pas des unités forment un idéal dans o ; 3) tout idéal de o est principal.

Les conditions 1), 2) sont évidemment nécessaires. Supposons que o soit l'anneau d'une valuation simple φ de K que nous pouvons supposer normée, et soit $\mathfrak{r}$ un idéal ~~de o~~ $\neq \{0\}$ de o. Posons $a = \min_{x \in \mathfrak{r}} \varphi(x)$, et soit x_0 un élément de $\mathfrak{r}$ tel que $\varphi(x) = a$. Si $x \in \mathfrak{r}$, on a $\varphi(x x_0^{-1}) \geq 0$, d'où $x x_0^{-1} \in o$, et $x \in x_0 o$, d'où $\mathfrak{r} = x_0 o$.

Supposons inversement les conditions 1), 2), 3) satisfaites. Soit op ($p \in o$) l'idéal des non-unités de o, et soit ~~XXX~~ oq l'idéal $\bigcap_{n=1}^{\infty} op^n$. Puisque $o \neq K$, on a $p \neq 0$; puisque $q \in op^{n+1}$, on a $p^{-1} q \in op^n$ pour tout entier n, d'où $p^{-1} q \in oq$, et $q = apq$, $a \in o$. Si on avait $q \neq 0$, on aurait $ap = 1$, ce qui est impossible puisque p est une non-unité. On a donc $\bigcap_{n=1}^{\infty} op^n = \{0\}$. Si x est un élément $\neq 0$ de o, il existe donc un

DSMS 003 13

~~entier $m \geq 0$ tel que $x \in \mathfrak{o}\mathfrak{p}^m$, $x \notin \mathfrak{o}\mathfrak{p}^{m+1}$~~ plus grand entier m tel que $x \in \mathfrak{o}\mathfrak{p}^m$. Si $x, y, x+y$ sont des éléments $\neq 0$ de $\mathfrak{o}$, on a évidemment $\varphi(x+y) \geq \min\{\varphi(x), \varphi(y)\}$. Par ailleurs on a $x = p^{\varphi(x)} x_1$, $y = p^{\varphi(y)} y_1$, où x_1, y_1 sont des unités, d'où $xy = p^{\varphi(x)+\varphi(y)} x_1 y_1$, $x_1 y_1$ étant une unité. Il est donc impossible que $xy \in \mathfrak{p}^n \mathfrak{o}$ si $n > \varphi(x) + \varphi(y)$, d'où $\varphi(xy) = \varphi(x) + \varphi(y)$. L'application φ de $\mathfrak{o}$ dans $\underline{Z}$ peut se prolonger par une valuation φ du corps des quotients K de $\mathfrak{o}$. Si x/y est un élément de K tel que $\varphi(x/y) \geq 0$ (où $x, y \in \mathfrak{o}$), on a $\varphi(x) \geq \varphi(y)$, d'où (en utilisant les mêmes notations que plus haut) $xy^{-1} = p^{\varphi(x)-\varphi(y)} x_1 y_1^{-1} \in \mathfrak{o}$; $\mathfrak{o}$ est donc l'anneau de la valuation φ.

16

PSMS 003 14

Un théorème d'existence pour les valuations.

Au paragraphe précédent, nous avons établi par des considérations spéciales l'existence de certaines valuations du corps des rationnels ou d'un corps qui est donné comme extension transcendante simple d'un sous-corps. ~~Dans ce paragraphe~~, Nous allons maintenant donner un théorème qui garantit l'existence de valuations dans des cas beaucoup plus généraux.

~~Définition~~ Introduisons d'abord la notion suivante. Soit φ une valuation d'un corps K, et soit o l'anneau de la valuation φ. ~~L'ensemble des éléments~~ L'ensemble p des ~~anneau~~ éléments ~~de~~ x de K tels que $\varphi(x) > 0$ est ~~evidemment~~ un idéal dans o, car les conditions $\varphi(x) > 0$, $\varphi(y) > 0$, $\varphi(z) \geq 0$ entraînent $\varphi(x-y) \geq \min\{\varphi(x), \varphi(y)\} > 0$ et $\varphi(zx) = \varphi(z) + \varphi(x) > 0$. Les éléments u tels que $\varphi(u) = 0$ sont les unités de o ; les éléments de p sont donc les ~~non-unités~~ éléments de o qui ne sont pas des unités ; c'est pourquoi on appelle p l'idéal des non-unités de o. Si x, y sont des éléments de o tels que $xy \in p$, l'un au moins des éléments $\varphi(x), \varphi(y)$ est > 0 ; il en résulte que p est un idéal premier. Ceci dit nous allons démontrer le

(ou de φ)

Théorème 1.

Soient K un corps, o un sous-anneau de K et p un idéal premier de o, distinct de l'anneau o. Il existe alors une valuation φ dont l'anneau contient o et telle que p soit l'intersection de o et de l'idéal des non-unités de φ.

~~Nous aurons besoin au cours de la démonstration d'utiliser~~

~~la notion~~ Soit o un anneau commutatif sans diviseurs de zéro, et soit S une partie de o qui possède les propriétés suivantes :

1. S est stable par rapport à la multiplication dans o
2. S n'est pas vide, mais ne contient pas 0.

Considérons alors l'ensemble o_S des éléments des corps des quotients de o

qui peuvent se mettre sous la forme $s^{-1}a$, $s \in S$, $a \in \sigma$. Les formules

$$s_1^{-1}a_1 + s_2^{-1}a_2 = (s_1 s_2)^{-1}(a_1 s_2 + a_2 s_1) \; ; \; (s_1^{-1}a_1)(s_2^{-1}a_2) = (s_1 s_2)^{-1}(a_1 a_2)$$

montrent que σ_S est un anneau. Il en découle que $\sigma_S \supset \sigma$, car, si $a \in \sigma$, $s \in S$, on a $a = s^{-1}(sa)$. De plus, si $p \in S$, on a $s^{-1} = s^2(s^2)^{-1} \in \sigma_S$.

On notera que, si $\mathfrak{p}$ est un idéal premier $\neq \sigma$ de σ, le complément S de $\mathfrak{p}$ par rapport à σ possède les propriétés 1) et 2) ci-dessus.

Définition.

Soient σ un anneau commutatif sans diviseurs de zéro et S une partie de σ qui possède les propriétés 1), 2) ci-dessus. L'anneau σ_S s'appelle alors l'anneau des quotients de S par rapport à σ. Si S est le complément par rapport à σ d'un idéal premier $\mathfrak{p} \neq \sigma$, σ_S s'appelle aussi l'anneau des quotients de $\mathfrak{p}$ et se désigne plus $\sigma_{\mathfrak{p}}$.

Lemme 1. Soient σ un anneau commutatif sans diviseurs de zéro, $\mathfrak{m}$ un idéal dans σ et S une partie de σ qui possède les propriétés 1), 2) ci-dessus. Désignons par $\mathfrak{m}'$ l'idéal engendré par $\mathfrak{m}$ dans l'anneau des quotients σ_S de S; si $\mathfrak{m} \cap S \neq \emptyset$, on a $\mathfrak{m}' = \sigma_S$. Si $\mathfrak{m} \cap S = \emptyset$, on a $\mathfrak{m}' \neq \sigma_S$; si de plus $\mathfrak{m}$ est premier, on a $\mathfrak{m}' \cap \sigma = \mathfrak{m}$ et $\mathfrak{m}'$ est premier. Inversement, si $\mathfrak{m}$ est un idéal quelconque de σ_S, $\mathfrak{m}$ est engendré par les éléments de $\mathfrak{m} \cap \sigma$.

Les éléments de $\mathfrak{m}'$ sont les produits d'éléments de $\mathfrak{m}$ par des éléments de σ_S.

Soit $\mathfrak{m}''$ l'ensemble des produits de $\mathfrak{m}$ par des éléments de σ_S. Il est clair que $\mathfrak{m}''$ contient $\mathfrak{m}$ et que le produit d'un élément de $\mathfrak{m}''$ par un élément de σ_S est dans $\mathfrak{m}''$. Soient $m_1 a_1 s_1^{-1}$ et $m_2 a_2 s_2^{-1}$ des éléments de $\mathfrak{m}''$ ($m_i \in \mathfrak{m}$, $a_i \in \sigma$, $s_i \in S$; $i = 1, 2$); on a $m_2 a_2 s_2^{-1} - m_1 a_1 s_1^{-1} = (m_2 a_2 s_1 - m_1 a_1 s_2)(s_1 s_2)^{-1}$. Or $m_2 a_2 s_1 - m_1 a_1 s_2$ est dans $\mathfrak{m}$ et $(s_1 s_2)^{-1}$ dans σ_S, d'où $m_2 a_2 s_2^{-1} - m_1 a_1 s_1^{-1} \in \mathfrak{m}''$. On voit que $\mathfrak{m}''$ est un idéal dans σ_S, d'où $\mathfrak{m}'' = \mathfrak{m}'$. Si $m \in \mathfrak{m} \cap \sigma_S$, on a $1 = mm^{-1} \in \mathfrak{m}'$, d'où $\mathfrak{m}' = \sigma_S$. Inversement, si $\mathfrak{m}' = \sigma_S$, on peut écrire $1 = m\, as^{-1}$ avec $m \in \mathfrak{m}$, $a \in \sigma$, $s \in S$, d'où $s = am \in \mathfrak{m}$ et $\mathfrak{m} \cap S \neq \emptyset$. Supposons que $\mathfrak{m}$ soit premier et que $\mathfrak{m} \cap S = \emptyset$; soit q un élément de $\mathfrak{m}' \cap \sigma$. On a donc $q = mas^{-1}$, $m \in \mathfrak{m}$, $a \in \sigma$, $s \in S$, d'où $qs = ma \in \mathfrak{m}$. Puisque $s \notin \mathfrak{m}$, on en déduit que $q \in \mathfrak{m}$. Soient enfin $a_1 s_1^{-1}$ et $a_2 s_2^{-1}$ des éléments de σ_S dont le produit est égal à un élément mas^{-1} de $\mathfrak{m}'$ ($a, a_1, a_2 \in \sigma$, $s, s_1, s_2 \in S$,

$m \in w$). On a $a_1 a_2 s = m a_1 s_1 s_2 \in w$ et $s \notin w$; on en conclut, puisque w est premier, que l'un des éléments a_1, a_2 appartient à w, donc que l'un des éléments $a_1 s_1^{-1}$, $a_2 s_2^{-1}$ appartient à w'. ~~Le lemme 1 est donc démontré~~.

Soit $\mathfrak{M}$ un idéal de $\mathfrak{o}_S$, et soit as^{-1} un élément de $\mathfrak{M}$ (avec $a \in \mathfrak{o}$, $s \in S$) ; on a alors $a = as^{-1} s \in \mathfrak{M} \cap \mathfrak{o}$ et $s^{-1} \in \mathfrak{o}_S$, ce qui montre que $\mathfrak{M}$ est engendré par les éléments de $\mathfrak{M} \cap \mathfrak{o}$. Le lemme 1 est démontré.

Ceci dit, revenons aux notations du Théorème 1. Formons l'anneau des quotients $\mathfrak{o}'$ de $\mathfrak{o}_{\mathfrak{p}}$ de l'idéal premier $\mathfrak{p}$, et soit $\mathfrak{p}'$ l'idéal engendré par $\mathfrak{p}$ dans $\mathfrak{o}'$. Il ~~est clair~~ résulte du lemme 1 que $\mathfrak{p}'$ est premier et que $\mathfrak{p}' \cap \mathfrak{o}' = \mathfrak{p}$, d'où $1 \notin \mathfrak{p}'$.

Considérons la famille $\mathfrak{F}$ des sous-anneaux A de K qui possèdent les propriétés suivantes :

a) A contient $\mathfrak{o}'$

b) l'idéal engendré par $\mathfrak{p}'$ dans A ne contient pas 1.

Nous allons montrer que la famille $\mathfrak{F}$ est inductive. Soit $\mathfrak{F}_0$ une ~~famille~~ sous-famille de $\mathfrak{F}$ totalement ordonnée par inclusion, et soit A_0 l'union de tous les anneaux appartenant à $\mathfrak{F}_0$. Si x, y sont des éléments de A_0, il existe des anneaux A_1, A_2 appartenant à $\mathfrak{F}_0$ tels que $x \in A_1$, $y \in A_2$. L'un des anneaux A_1, A_2, soit A_2, contient l'autre ; les éléments $x-y$, xy sont alors tous deux dans A_2, donc aussi dans A_0, ce qui montre que A_0 est un anneau. Soient $p_1, \dots, p_h$ des éléments de $\mathfrak{p}'$ et $a_1, \dots, a_h$ des éléments de A_0. Il existe des anneaux $A_i \in \mathfrak{F}_0$ ($1 \leq i \leq h$) tels que $a_i \in A_i$; puisque $\mathfrak{F}_0$ est totalement ordonné, les A_i sont tous contenus dans l'un d'entre eux, soit A_k, et $\sum_{i=1}^{h} p_i a_i$ est ~~contenu~~ dans l'idéal engendré par $\mathfrak{p}'$ dans A_k, d'où $\sum_{i=1}^{h} a_i p_i \neq 1$, ce qui montre que l'idéal engendré par $\mathfrak{p}'$ dans A_0 ne contient pas 1. On a donc $A_0 \in \mathfrak{F}$, ce qui montre que $\mathfrak{F}$ est inductive.

~~Soit~~ Il résulte du théorème de Zorn que la famille $\mathfrak{F}$ possède au moins un ~~anneau~~ élément maximal V. On va montrer que V est un anneau de valuation.

L'idéal engendré par $\mathfrak{p}'$ dans V, ne contenant pas 1, est contenu dans au moins un idéal premier maximal ~~$\mathfrak{v}$ de V~~ (ne contenant pas 1) $\mathfrak{v}$ de V. Formons l'anneau des quotients $V_{\mathfrak{v}}$ de $\mathfrak{v}$; il résulte immédiatement du lemme 1 que l'idéal engendré par $\mathfrak{p}'$ dans $V_{\mathfrak{v}}$ (qui est contenu dans l'idéal engendré par $\mathfrak{v}$) ne contient pas 1. On a donc $V_{\mathfrak{v}} \in \mathfrak{F}$, d'où $V_{\mathfrak{v}} = V$ puisque V est maximal. L'inverse

l'un élément de V non contenu dans $\mathfrak{v}$ est donc dans V.

Soit x un élément de K non contenu dans V. Donc $V[x] \neq V$, d'où $V[x] \notin \mathfrak{F}$, ce qui montre que 1 appartient à l'idéal engendré par $\mathfrak{p}'$ dans $V[x]$. Or les éléments de cet idéal sont évidemment les éléments de la forme $\sum_{i=0}^{m} p_i x^i$, $p_i \in \mathfrak{p}'$ $(1 \leq i \leq m)$; on a donc une égalité de la forme

$$1 = \sum_{i=0}^{m} p_i x^i \qquad (p_i \in \mathfrak{p}',\ 0 \leq i \leq m)$$

L'élément $1 - p_0$ est $\equiv 1 \pmod{\mathfrak{v}}$, donc n'est pas dans $\mathfrak{v}$, d'où $(1-p_0)^{-1} \in V$. Posons $v_i = (1-p_0)^{-1} p_i$; on a alors

$$1 = \sum_{i=1}^{m} v_i x^i \qquad v_i \in \mathfrak{v} \quad (1 \leq i \leq m)$$

Parmi toutes les représentations de 1 sous la forme précédente, nous supposons que nous en avons choisi une pour laquelle l'entier m soit le plus petit possible.

Si on avait $1/x \notin V$, on aurait de même

$$1 = \sum_{i=1}^{n} v'_i \left(\tfrac{1}{x}\right)^i \qquad v'_i \in \mathfrak{v} \quad (1 \leq i \leq n)$$

et nous supposons encore que, parmi toutes les représentations de 1 sous la forme précédente, nous en avons choisi une pour laquelle l'entier n est le plus petit possible. On a $v_m x^m = \sum_{i=1}^{n} v'_i x^{m-i}$, d'où

$$1 = \sum_{i=1}^{m-1} v_i x^{m-i} + \sum_{i=1}^{n} v_m v'_i x^{m-i}$$

Si on avait $m \geq n$, 1 pourrait être écrit comme combinaison linéaire de $x, \ldots, x^{m-1}$ à coefficients dans $\mathfrak{v}$, ce qui est impossible puisque m a été choisi le plus petit possible. Donc Echangeant les rôles joués par x et par $1/x$, on voit de même que l'hypothèse $n \geq m$ conduit à une contradiction. On voit donc que l'hypothèse que $1/x \notin V$ est intenable. Nous avons démontré que l'inverse d'un élément $x \notin V$ appartient à V, ce qui montre que V est une anneau de valuation. On a $\mathfrak{o} \subset \mathfrak{o}' \subset V$ et $\mathfrak{p} \subset \mathfrak{p}' \subset \mathfrak{v}$, ce qui montre que $\mathfrak{p}$ est contenu dans l'idéal des non-unités de V. D'autre part tout élément de $\mathfrak{o}$ non contenu dans $\mathfrak{p}$ devient une unité dans $\mathfrak{o}'$ et *a fortiori* dans V ; on voit donc que $\mathfrak{p}$ est l'intersection de $\mathfrak{o}$ et de l'idéal des non unités de V. Le théorème 1 est donc démontré.

Corollaire 1.

Soient K un corps, φ une valuation de K et L un sur-corps de K.

Il existe alors une valuation ψ de L dont la restriction à K est équivalente à φ.

Soient en effet o l'anneau de la valuation φ et $\mathfrak{p}$ l'idéal des non-unités de o. Il existe une valuation ψ de L dont l'anneau O contient o et tel que $\mathfrak{p}$ soit l'intersection de o avec l'idéal des non-unités de O. L'anneau de valuation de la restriction de ψ à K est évidemment $O \cap K$; cet anneau contient o. D'autre part, si x est un élément de K non contenu dans o, il est clair que $1/x$ est dans $\mathfrak{p}$, donc aussi dans l'idéal des non-unités de O, d'où $x \notin O$; on a donc bien $O \cap K = o$.

~~Soient φ une valuation d'un corps K et désignons par o l'idéal l'anneau de la valuation φ et par $\mathfrak{p}$ l'idéal des non-unités de o. Il est évident que $\mathfrak{p}$ est un idéal maximal de o, donc que l'anneau $o/\mathfrak{p}$ est un corps.~~

(d'un corps K)

~~Définition. Soient o l'anneau d'une valuation φ et $\mathfrak{p}$ l'idéal des non-unités de o. Le corps $o/\mathfrak{p}$ s'appelle alors le corps des résidus de la valuation φ.~~

~~Soient L un sur-corps de K et ψ une valuation de L dont la restriction à K soit équivalente à φ. Désignons par O l'anneau de la valuation ψ et par $\mathfrak{P}$ l'idéal des non-unités de O. On a par hypothèse $O \cap K = o$; si $x \in K$, les conditions $\varphi(x) > 0$, $\psi(x) > 0$ sont équivalentes, d'où $\mathfrak{P} \cap o = \mathfrak{p}$. Le corps $o/\mathfrak{p}$ est donc canoniquement isomorphe à $o + \mathfrak{P}/\mathfrak{P}$, qui est un sous-corps de $O/\mathfrak{P}$. On peut donc identifier le corps des résidus de φ avec un sous-corps de celui de ψ.~~

Corollaire 2. Soient o un sous-anneau d'un corps K, contenant l'élément-unité de K. Si x est un élément de o qui n'est pas une unité, il existe une valuation φ de K dont l'anneau contient o et qui est telle que $\varphi(x) > 0$.

L'idéal ox, ne contenant pas 1, est contenu dans au moins un idéal premier $\mathfrak{p}$ de o. Si φ est une valuation ~~telle~~ de K dont l'anneau ~~V~~ contient o et telle que l'idéal des non-unités de V contienne $\mathfrak{p}$, on a $\varphi(x) > 0$.

III

Anneaux normaux

Définition

Soient o un domaine d'intégrité, et K le corps des quotients de o. On dit que l'anneau o est normal s'il existe une famille Φ de valuations de K qui possède les propriétés suivantes:
1) l'intersection des anneaux des valuations $\varphi \in \Phi$ est l'anneau o;
2) Le groupe des valeurs de chaque $\varphi \in \Phi$ est isomorphe au groupe additif des entiers ; 3) si $x \in o$, $x \neq 0$, il y a qu'un nombre fini de valuations $\varphi \in \Phi$ telles que $\varphi(x) \neq 0$.

Si o est un anneau normal, il y a en général de multiples familles Φ qui jouissent des propriétés précédentes. Dans l'ensemble de toutes ces familles, nous allons montrer qu'il y en a une qui est en un certain sens minimale et qui jouit de propriétés particulières.

nous les appellerons les familles de définition de o

Définition

Soient o un domaine d'intégrité et K le corps des quotients de o. On dit qu'un idéal $\mathfrak{p}$ de o est essentiel s'il existe un élément x de K, non contenu dans o, tel que $\mathfrak{p}x \subset o$.

Soit o un anneau normal. Nous disons qu'un idéal $\mathfrak{p}$ de o est essentiel s'il existe un élément x du corps des quotients K de o non contenu dans o mais tel que $\mathfrak{p}x \subset o$.

Lemme 1. Soient o un anneau normal et $\mathfrak{p}$ un idéal premier essentiel de o. L'anneau des quotients de $\mathfrak{p}$ est alors l'anneau d'une valuation $\varphi_{\mathfrak{p}}$ de K dont le groupe des valeurs est le groupe des entiers. Si φ est une valuation non triviale de K dont l'anneau contient o sans être telle que $\varphi(a) = 0$ pour tout $a \in \mathfrak{p}$ non contenu dans $\mathfrak{p}$,

ASTIS 003 20

~~Soit σ un anneau normal~~

Nous si φ est une valuation d'un corps K dont le groupe des valeurs est isomorphe au groupe additif $\underline{Z}$ des entiers, φ est équivalente à une valuation φ' dont le groupe des valeurs est $\underline{Z}$ lui-même. Les valuations φ' dont le groupe des valeurs est $\underline{Z}$ sont dites normées. Il est clair que tout anneau normal possède une famille de définition composée de valuations normées.

(dont l'anneau contient σ)

~~Soit σ~~ Soit σ un anneau normal. Si φ est une valuation non triviale du corps des quotients de σ, nous désignerons par $\mathfrak{p}_\varphi$ ~~l'idéal composé des~~ l'ensemble des $x \in \sigma$ tels que $\varphi(x) > 0$; il est clair que $\mathfrak{p}_\varphi$ est un idéal premier $\neq \{0\}$ de σ (si on avait $\mathfrak{p}_\varphi = \{0\}$, on aurait $\varphi(x) = 0$ pour tout $x \neq 0$ de σ, donc aussi pour tout $x \neq 0$ de K, puisque K est le corps des quotients de σ).

~~Lemme 1. Soient σ un anneau normal, et Φ une famille de définition de σ. Soit $\mathfrak{p}$ un idéal premier $\neq \{0\}$ de σ; il existe alors un $\varphi \in \Phi$ tel que $\mathfrak{p}_\varphi \subset \mathfrak{p}$. S'il existe un élément u du corps des quotients de σ tel que $u \notin \sigma$, $u\mathfrak{p} \subset \sigma$, il existe un $\varphi \in \Phi$ tel que $\varphi(u) < 0$, $\mathfrak{p}_\varphi \subset \mathfrak{p}$, $\sigma u^{-1} \cap \mathfrak{p}$, $u \notin \sigma$, on peut choisir φ~~

Lemme 1. Soient σ un anneau normal et Φ une famille de définition de σ. Soit $\mathfrak{p}$ un idéal premier de σ et u un élément du corps des quotients K de σ tel que $u \notin \sigma$, $\sigma \cap \sigma u^{-1} \subset \mathfrak{p}$. Il existe alors une valuation $\varphi \in \Phi$ telle que $\varphi(u) < 0$, et $\mathfrak{p}_\varphi \subset \mathfrak{p}$.

On peut supposer que les valuations de la famille Φ sont normées

Si nous écrivons $u = u_1/u_2$, avec $u_1, u_2 \in \sigma$, il n'y a qu'un nombre fini de valuations $\varphi \in \Phi$ telles que $\varphi(u_2) \geq 0$. Il n'y a donc qu'un nombre fini de $\varphi \in \Phi$ telles que $\varphi(u) < 0$; soient $\varphi_1, \cdots, \varphi_h$ ces valuations. Supposons pour un moment que $\mathfrak{p}$ ne contienne aucun des $\mathfrak{p}_{\varphi_i}$; soit alors x_i un élément de $\mathfrak{p}_{\varphi_i}$ non contenu dans $\mathfrak{p}$. On a $\varphi_i(x_i) \geq 1$; il existe donc un entier $n_i > 0$ tel que $\varphi_i(x_i^{n_i}) \geq \varphi_i(u)$. Posons $x = \prod_{i=1}^{n} x_i^{n_i}$, d'où $\varphi_i(ux) \geq 0$ $(1 \leq i \leq h)$. Si $\varphi \in \Phi$ est distincte de $\varphi_1, \cdots, \varphi_h$, on a $\varphi(u) \geq 0$, d'où $\varphi(ux) \geq 0$; on a donc $ux \in \sigma$, $x \in \sigma u^{-1}$, d'où $x \in \mathfrak{p}$. Or, $\mathfrak{p}$ étant premier, un produit de plusieurs facteurs ne peut appartenir à $\mathfrak{p}$ sans que l'un des facteurs y appartienne. Notre hypothèse que $\mathfrak{p}$ ne contient aucun des $\mathfrak{p}_{\varphi_i}$ est donc absurde, et le lemme 1 est démontré.

Corollaire. Si $\mathfrak{p}$ est un idéal premier $\neq \{0\}$ de σ, il existe un $\varphi \in \Phi$ tel que $\mathfrak{p}_\varphi \subset \mathfrak{p}$.

C'est évident si $\mathfrak{p} = \sigma$. Sinon, soit x un élément $\neq 0$ de $\mathfrak{p}$; on a donc $x^{-1} \notin \sigma$, $\sigma \cap (x^{-1})^{-1}$

$\subset \mathfrak{p}$, et le corollaire résulte du lemme 1.

Définition

Une valuation ~~non triviale~~ φ du corps des quotients K d'un anneau normal σ est ~~dite essentielle~~ s'il existe un élément $u \in K$ tel que $u \notin \sigma$, $u\mathfrak{p}_\varphi \subset \sigma$.

appelée une valuation essentielle de σ

Lemme 2. Soient σ un anneau normal et Φ une famille de définition de σ. ~~L'anneau σ est alors~~ la famille des valuations essentielles appartenant à Φ est alors une famille de définition de σ.

Il suffit de montrer que, si u est un élément du corps des quotients K de σ, ~~il existe une valuation~~ tel que $u \notin \sigma$, il existe une valuation essentielle $\varphi \in \Phi$ telle que $\varphi(u) < 0$. Désignons par C le complément de σ par rapport à K; si $v \in C$, désignons par $\mathfrak{v}_v$ l'~~ensemble~~ idéal $\sigma \cap v^{-1}$ de σ. Montrons qu'il n'y a qu'un nombre fini d'idéaux distincts de la forme $\mathfrak{v}_v$ ($v \in C$) qui contiennent $\mathfrak{v}_u$. Il n'y a qu'un nombre fini de valuations $\varphi \in \Phi$ telles que $\varphi(u) < 0$ (pour la démonstration du lemme 1); soient $\varphi_1, \dots, \varphi_h$ ces valuations. Si $v \in C$, posons $q_i = \min_{x \in \mathfrak{v}_v} \varphi_i(x)$ $(1 \leq i \leq h)$. L'ensemble $\mathfrak{v}_v$ est donc contenu dans l'ensemble $\mathfrak{v}'_v$ des $x \in \sigma$ tels que $\varphi_i(x) \geq q_i$ $(1 \leq i \leq h)$; montrons que, si $\mathfrak{v}_u \subset \mathfrak{v}_v$, on a $\mathfrak{v}_v = \mathfrak{v}'_v$. Soit alors en effet x' un élément de $\mathfrak{v}'_v$; puisque $u\mathfrak{v}_v \subset \sigma$, on a $q_i + \varphi_i(u) \geq 0$ $(1 \leq i \leq h)$, d'où $\varphi_i(x'u) \geq 0$ $(1 \leq i \leq h)$; d'autre part, ~~si $\varphi \in \Phi$ est différent de $\varphi_1, \dots, \varphi_h$, on a $\varphi(u) \geq 0$, d'où $\varphi(v) \geq 0$ puisque $v\mathfrak{v}_u \subset \sigma$~~ on a évidemment $u_2 \in \mathfrak{v}_u \subset \mathfrak{v}_v$, d'où $vu_2 \in \sigma$ et par suite $\varphi(v) \geq 0$ si $\varphi \in \Phi$ est distincte de $\varphi_1, \dots, \varphi_h$. On a donc $\varphi(vx') \geq 0$ pour tout $\varphi \in \Phi$, d'où $vx' \in \sigma$, $x' \in \mathfrak{v}_v$, ce qui démontre notre assertion. Parmi ~~les $\mathfrak{v}_v$~~ ceux des idéaux $\mathfrak{v}_v$ ($v \in C$) qui contiennent $\mathfrak{v}_u$, choisissons en un maximal, soit $\mathfrak{v}_w = \mathfrak{p}$ (avec $w \in C$).

Posons $u = u_1/u_2$, $u_1 \in \sigma$, $u_2 \in \sigma$.

Montrons que $\mathfrak{p}$ est premier. Soient x, y des éléments de σ tels que $x \notin \mathfrak{p}$, $xy \in \mathfrak{p}$. On a donc $xw \in C$, et, puisque $x \in \sigma$, $\mathfrak{v}_{xw} \supset \mathfrak{v}_w = \mathfrak{p}$; puisque $\mathfrak{p}$ est maximal, on a $\mathfrak{v}_{xw} = \mathfrak{p}$. Or, puisque $xy \in \mathfrak{p}$, y appartient à $\mathfrak{v}_{xw}$, d'où $y \in \mathfrak{p}$, ce qui démontre notre assertion. ~~En vertu du lemme 1, il existe un $\varphi \in \Phi$ tel que φ. Puisque $\mathfrak{v}_u \subset \mathfrak{p}$, on a $\sigma \cap u^{-1} \subset \mathfrak{p}$; en vertu du lemme 1, il existe un $\varphi \in \Phi$ tel que $\varphi(u) < 0$, $\mathfrak{p}_\varphi \subset \mathfrak{p}$. Puisque $u\mathfrak{p} \subset \sigma$, il en dans que $\mathfrak{p} \in \mathfrak{p}_\varphi$, d'où $\mathfrak{p} = \mathfrak{p}_\varphi$.~~ On a $\mathfrak{v}_u = \sigma \cap u^{-1} \subset \mathfrak{p}$; en vertu du lemme 1, il existe un $\varphi \in \Phi$ tel que $\varphi(u) < 0$, $\mathfrak{p}_\varphi \subset \mathfrak{p}$. On a donc $w\mathfrak{p}_\varphi \subset w\mathfrak{p} \subset \sigma$, et φ est essentielle, ce qui démontre le lemme 2.

PSMS 003 22

Lemme 3. *Si φ est une valuation essentielle d'un anneau normal σ, l'anneau de valuation de φ est l'anneau des quotients σ' de $\mathfrak{p}_\varphi$. Tout idéal de σ' est principal ; si u est un élément non contenu dans σ du corps des quotients de σ tel que $u\mathfrak{p}_\varphi \subset \sigma$, u^{-1} engendre l'idéal des non-unités de σ' et $\varphi(u^{-1})$ engendre le groupe des valeurs de φ ; il existe un $x \in \mathfrak{p}_\varphi$ tel que $\varphi(x) = \varphi(u^{-1})$.*

tout idéal $\neq 0$ de σ' est engendré par une puissance de u^{-1} ;

Il est clair que σ' est contenu dans l'anneau de valuation de φ. Soit maintenant y un élément $\neq 0$ de σ. Puisque $u \notin \sigma$, il existe dans une famille de définition de σ une valuation ψ, que nous pouvons supposer normée, telle que $\psi(u) < 0$. Il est donc impossible que $\psi(u^n) \leq \psi(y)$ pour tout $n > 0$; il y a donc un entier $n(y) \geq 0$ tel que $yu^{n(y)} \in \sigma$, $yu^{n(y)+1} \notin \sigma$. On a donc $yu^{n(y)} \notin \mathfrak{p}_\varphi$, d'où $\varphi(yu^{n(y)}) = 0$, $\varphi(y) = n(y)\varphi(u^{-1})$. Le groupe des valeurs de φ est donc entièrement engendré par les valeurs prises par φ sur σ, donc aussi par $\varphi(u^{-1})$, ~~Si on a de plus y appartient~~ d'où $\varphi(u^{-1}) \neq 0$. Si $y \in \mathfrak{p}_\varphi$, on a $n(y) \geq 1$, $\varphi(y) > 0$, d'où $\varphi(u^{-1}) > 0$; de plus, $n(y) = \varphi(y)/\varphi(u^{-1})$ est entièrement déterminé par y, d'où il résulte que $yu^\nu \in \sigma$ pour $0 \leq \nu \leq n(y)$. Soit $z = y/y'$ un élément de l'anneau de valuation de φ, avec y et y' dans σ. On a donc $\varphi(y) \geq \varphi(y')$, d'où $n(y) \geq n(y')$ et $z = yu^{n(y')}/y'u^{n(y')}$, avec $yu^{n(y')} \in \sigma$, $y'u^{n(y')} \in \sigma$, $y'u^{n(y')} \notin \mathfrak{p}_\varphi$, d'où $z \in \sigma'$, ce qui montre que σ' est l'anneau de valuation de φ. Si de plus $\varphi(z) > 0$, on a $yu^{n(y')+1} \in \sigma$, d'où $zu \in \sigma'$, $z \in \sigma' u^{-1}$, ce qui montre que u^{-1} engendre l'idéal des non unités de σ'. Soit σ' un idéal $\neq 0$ de σ'. Si $z \in \sigma'$, $z \neq 0$, il est impossible que $\varphi(zu^n) \geq 0$ pour tout n, puisque $\varphi(u) < 0$; il y a donc un entier $m \geq 0$ tel que $u^m \sigma' \subset \sigma'$, $u^{m+1}\sigma' \not\subset \sigma'$. On a donc $u^m \sigma' \not\subset \sigma' u^{-1}$, et $\sigma' u^m \sigma'$ contient une unité, d'où $u^m \sigma' = \sigma'$, $\sigma' = \sigma' u^{-m}$, ce qui montre que σ' est principal. Si nous écrivons $u^{-1} = x/y'$, $x \in \sigma$, $y' \in \sigma$, $y' \notin \mathfrak{p}_\varphi$, on a $\varphi(x) = \varphi(u^{-1})$.

Corollaire. *Soient σ un anneau normal, et Φ une famille de définition de σ. Toute valuation essentielle de σ est équivalente à une valuation $\varphi \in \Phi$.*

Soit en effet φ_1 une valuation essentielle de σ, et soit u un élément du corps des quotients K de σ tel que $u\mathfrak{p}_{\varphi_1} \subset \sigma$, $u \notin \sigma$. Il existe, en vertu du lemme 2, une valuation essentielle $\varphi \in \Phi$ telle que $\varphi(u) < 0$. Il en résulte que $\mathfrak{p}_{\varphi_1} \subset \mathfrak{p}_\varphi$

PSTS 003 23

Nous appellerons (par abus de langage) idéal premier minimal d'un domaine d'intégrité σ un idéal premier qui est minimal dans l'ensemble des idéaux premiers $\neq (0)$ de σ, ordonné par inclusion –

Proposition

Soit σ un anneau normal. ~~Tout idéal premier minimal~~ Si $\mathfrak{p}$ est un idéal premier minimal de σ, l'anneau des quotients de $\mathfrak{p}$ est l'anneau d'une valuation essentielle $\varphi_{\mathfrak{p}}$ de σ dont le groupe des valeurs est le groupe des entiers. Si Φ est la famille des valuations ~~obtenues~~ $\varphi_{\mathfrak{p}}$ relatives à tous les idéaux premiers minimaux de σ, σ est l'intersection des anneaux des valuations $\varphi_{\mathfrak{p}}$. Si $\varphi \in \Phi$, il existe un élément u du corps des quotients de σ tel que $\varphi(u) = -1$, $\varphi'(u) \geq 0$ pour toute $\varphi' \in \Phi$ différente de φ. Toute valuation essentielle de σ est équivalente à l'une des valuations de la famille Φ.

[composés de valuations normées]

Soit Φ_1 une famille de définition de σ, et soit Φ_0 la famille des valuations essentielles appartenant à Φ_1. Il résulte du lemme 2 que Φ_0 est encore une famille de définition. Soit $\mathfrak{p}$ un idéal premier minimal de σ ; il résulte du lemme 1, appliqué à Φ_0, qu'il existe une valuation essentielle $\varphi \in \Phi_0$ telle que ~~$\mathfrak{p} =$~~ $\mathfrak{p}_\varphi \subset \mathfrak{p}$. Puisque $\mathfrak{p}$ est minimal, on a $\mathfrak{p} = \mathfrak{p}_\varphi$, et il résulte du lemme 3 que l'anneau des valuations de φ est l'anneau des quotients de $\mathfrak{p}$. ~~Il existe donc une~~ Soit maintenant ψ une valuation essentielle quelconque de σ, ~~il est soit x un élément des corps des quotients K de σ tel que $x\mathfrak{p}_\psi \subset \sigma$~~. Soit σ' l'anneau des quotients de $\mathfrak{p}_\psi$; il résulte ~~du lemme 3 que, si $\mathfrak{q}'$ est un idéal de σ' qui est $\neq \sigma'$, on a $\varphi'(x) \geq 0$~~ immédiatement du lemme 3 que le seul idéal premier $\neq (0)$ de σ' est l'idéal $\mathfrak{p}_\psi$ des non-unités, qui est l'idéal engendré par $\mathfrak{p}_\psi$ dans σ'. Faisant usage du lemme 4, on en conclut que $\mathfrak{p}_\psi$ ~~ne peut exister~~ est minimal ; la valuation ψ, dont l'anneau est l'anneau des quotients de $\mathfrak{p}_\psi$, est donc équivalente à l'une des valuations de Φ. Appliquant ceci aux valuations $\varphi \in \Phi_0$, on en conclut que σ est l'intersection des anneaux des valuations appartenant à Φ. Soit φ un élément de Φ, et soit u un élément non contenu dans σ du corps des quotients de σ tel que $u\mathfrak{p}_\varphi \subset \sigma$. Puisque φ est normée, on a $\varphi(u) = -1$ en vertu du lemme 3. Si $\varphi' \in \Phi$, $\varphi' \neq \varphi$, on a $\mathfrak{p}_{\varphi'} \neq \mathfrak{p}_\varphi$ (~~puisque $\mathfrak{p}_\varphi \neq \mathfrak{p}_{\varphi'}$~~ parce que φ et φ' sont normées et que deux valuations normées distinctes sont inéquivalentes). Puisque $\mathfrak{p}_\varphi$ n'est pas minimal, il n'est pas contenu dans $\mathfrak{p}_{\varphi'}$. Si $x \in \mathfrak{p}_\varphi$, $x \notin \mathfrak{p}_{\varphi'}$, on a $\varphi'(x) = 0$, $\varphi'(ux) \geq 0$, d'où $\varphi'(u) \geq 0$. La proposition est donc démontrée –

PSNS 003 24

Proposition

Soient σ un anneau normal, $\varphi_1, \cdots, \varphi_h$ des valuations essentielles normées distinctes de σ et $m_1, \cdots, m_h$ des entiers. Il existe alors un élément x du corps des quotients K de σ tel que $\varphi_i(x) = m_i$ $(1 \leq i \leq h)$, $\varphi(x) \geq 0$ pour toute valuation essentielle φ de σ qui n'est équivalente à aucune des valuations $\varphi_1, \cdots, \varphi_h$.

Supposons d'abord que $m_i < 0$ $(1 \leq i \leq h)$. Soit u_i un élément de K tel que $u_i \notin \sigma$, $u_i \mathfrak{p}_{\varphi_i} \subset \sigma$. Il résulte alors immédiatement de la prop. que $x = u_1^{-m_1} + u_2^{-m_2} + \cdots + u_h^{-m_h}$ a les propriétés requises. Pour passer au cas général, déterminons des entiers $n_i > 0$ $(1 \leq i \leq h)$ tels que $n_i > m_i$; soit, pour chaque i, $x_i \neq 0$, y_i un élément de $\mathfrak{p}_{\varphi_i}$, tel que $\varphi_i(\pi_{i=1}^{h} y_i^{n_i}) > m_i$; on pourra prendre $x = \pi_{i=1}^{h} y_i^{n_i} x'$, où x' est tel que $\varphi_i(x') = m_i - \varphi_i(\pi_{i=1}^{h} y_i^{n_i})$, $\varphi^*(x') \geq 0$ pour toute valuation essentielle φ de σ qui n'est équivalente à aucune des valuations $\varphi_1, \cdots, \varphi_h$.

Remarque. Les notations étant celles de la Prop., il n'est en général pas possible de trouver un élément x du corps des quotients K de σ tel que $\varphi_i(x) = m_i$ $(1 \leq i \leq h)$, et $\varphi(x) = 0$ pour toute valuation essentielle φ qui n'est équivalente à aucune des valuations $\varphi_1, \cdots, \varphi_h$. Les anneaux pour lesquels ce problème est toujours possible sont les anneaux arithmétiques que nous étudierons plus loin.

Par ailleurs, un anneau normal possède en général des valuations non essentielles (autres que la valuation triviale). Des anneaux normaux ~~qui n'en possèdent pas forment une autre catégorie d'anneaux normaux~~, dont toutes les valuations non triviales sont essentielles sont les anneaux de Dedekind, que nous étudierons également plus loin.

Enfin, nous verrons que les anneaux qui sont à la fois anneaux arithmétiques et anneaux de Dedekind sont les anneaux dont tous les idéaux sont principaux.

Anneaux arithmétiques

Définition.

On appelle anneau arithmétique un anneau normal dont les idéaux premiers minimaux sont principaux. Les éléments de l'anneau qui engendrent les idéaux premiers minimaux sont dits irréductibles.

Soit o un anneau arithmétique, et soit Φ l'ensemble des valuations essentielles normées de o. A chaque $\varphi \in \Phi$ associons un élément $q_\varphi \in o$ qui engendre l'idéal premier $\mathfrak{p}_\varphi$ composé des $x \in o$ tels que $\varphi(x) > 0$. Si φ' est un élément de Φ distinct de φ, $\mathfrak{p}_\varphi$ n'est pas contenu dans $\mathfrak{p}_{\varphi'}$, d'où $\varphi'(q_\varphi) = 0$. Donnons nous pour chaque $\varphi \in \Phi$ un entier m_φ de telle manière que l'on n'ait $m_\varphi \neq 0$ que pour un nombre fini d'éléments φ. Si nous formons $y = \prod_{\varphi \in \Phi} q_\varphi^{m_\varphi}$, on a évidemment $\varphi(y) = m_\varphi$ pour tout $\varphi \in \Phi$. Inversement, si x est un élément quelconque $\neq 0$ du corps des quotients K de o, et si nous posons $m_\varphi = \varphi(x)$, il n'y a qu'un nombre fini d'éléments $\varphi \in \Phi$ pour lesquels $\varphi(x) \neq 0$.

On a donc

$$(1) \qquad x = u \prod_{\varphi \in \Phi} q_\varphi^{\varphi(x)}$$

où u est un élément tel que $\varphi(u) = 0$ pour tout $\varphi \in \Phi$, donc une unité de o. On dit que la formule (1) donne la décomposition de x en facteurs irréductibles (relative au choix des q_φ). On notera que, si $x = u' \prod_{\varphi \in \Phi} q^{m_\varphi}$, où u' est une unité et $m_\varphi = 0$ sauf pour un nombre fini de valuations φ, on a $m_\varphi = \varphi(x)$ pour tout $\varphi \in \Phi$, d'où $u' = u$. C'est ce qui exprime en disant que la décomposition de x en facteurs irréductibles est unique. - Si Φ' est une partie de Φ telle que $\varphi'(x) = 0$ pour tout φ

Si o est un anneau normal, tout idéal premier principal $\mathfrak{p}$ de o, autre que $\{0\}$ ou o, est minimal ; car Soit en effet $\mathfrak{q}$ un idéal premier $\neq \{0\}$ contenu dans $\mathfrak{p}$, et soit $\mathfrak{p}'$ l'idéal $p^{-1}\mathfrak{q}$. Puisque $\mathfrak{p}$ n'est pas une unité, il existe une valuation essentielle φ de o telle que $\varphi(p) > 0$. On a $\min_{x \in \mathfrak{q}} \varphi(x) < \min_{x \in \mathfrak{p}} \varphi(x)$, d'où $\mathfrak{q} \neq \mathfrak{p}$. Soit x un élément de $\mathfrak{q}$ non contenu dans $\mathfrak{p}$; on a $xp \in \mathfrak{q}$, d'où $p \in \mathfrak{q}$ et $\mathfrak{q} = \mathfrak{p}$.

$\varphi \in \Phi$ non contenu dans Φ', on a aussi $x = u \prod_{\varphi \in \Phi'} q_\varphi^{\varphi(x)}$; par abus de langage on dit encore que cette formule donne ~~aussi~~ la décomposition de x en facteurs irréductibles.

(q ne sert pas une unité et que)

Proposition.

Pour qu'un élément q d'un anneau arithmétique σ soit irréductible, il faut et suffit que, dans toute représentation $q = xy$ de q comme un produit de deux éléments de σ, l'un des facteurs x ou y soit une unité.

($q = xy$)

Supposons q irréductible. Puisque σq est premier, l'un des facteurs x ou y est dans σq ; si $x = qz$, on a $zy = 1$, et y est une unité. Inversement, supposons la condition satisfaite. ~~Puisque~~ Écrivons $q = u \prod_{\varphi \in \Phi} q_\varphi^{\varphi(q)}$; l'un au moins des $\varphi(q)$ est ≥ 1, et, si $\varphi_1(q) \geq 1$, on $q = q_{\varphi_1} \cdot \left(u \prod_{\varphi \in \Phi} q_\varphi^{m_\varphi} \right)$ où ~~$\psi(q) = \varphi(q)$~~ $\cdot$ $m_{\varphi_1} = \varphi(q) - 1$, $m_\varphi = \varphi(q)$ si $\varphi \neq \varphi_1$. Le second facteur étant une unité, on a $m_\varphi = 0$ pour tout $\varphi \in \Phi$, d'où $q = u q_{\varphi_1}$, et q est irréductible.

Soit E une partie non vide ~~$\neq \{0\}$~~ ~~d'un anneau arithmétique σ~~ de σ. Posons, pour tout $\varphi \in \Phi$, ~~$m_\varphi = \varphi$~~ $m_\varphi = \min_{x \in E} \varphi(x)$, et soit d un élément de σ tel que $\varphi(x) = m_\varphi$ pour tout $\varphi \in \Phi$. Il en résulte que d divise tous les éléments de σ ; inversement, tout élément de σ qui divise tous les éléments de E divise d. Un élément d qui possède ces propriétés est appelé un plus grand commun diviseur des éléments de E ; les p.g.c.d. des éléments de E sont tous les éléments du, où u parcourt l'ensemble des unités de σ. Si E se compose d'un nombre fini d'éléments $x, y, \ldots$ donnés explicitement, ~~un p~~ un p.g.c.d. des éléments de E s'appelle aussi un p.g.c.d. des éléments $x, y, \ldots$.

(p.g.c.d.)

~~Définition~~.

~~Des éléments d'une partie~~

Proposition.

Soit E une partie non vide $\neq \{0\}$ d'un anneau arithmétique σ et soit z un élément $\neq 0$ de σ. Si d est un p.g.c.d. des éléments de E, ~~zd~~ zd est un p.g.c.d. des éléments de zE.

~~Cela résulte immédiatement des définitions. En effet, si $\varphi \in \Phi$,~~ on a ~~$\min_{x \in zE} \varphi(x) = \min_{y \in E} \{\varphi(y) + \varphi(z)\} = \varphi(z) + \min_{y \in E} \varphi(y)$ et~~ zd étant $z \prod_{\varphi \in \Phi} q_\varphi^{\varphi(d)}$ ~~est un~~ $= \prod_{\varphi \in \Phi} q_\varphi^{\varphi(z)}$

PSMS 007 27

Il en dcoule que zd divise tous les éléments de E. Inversement, supposons que δ divise tous les éléments de zE. On a alors $\varphi(e) \leq \varphi(z) + \varphi(x)$ pour tout $\varphi \in \Phi$ et $x \in E$, d'où $\varphi(e) \leq \varphi(z) + \varphi(d) = \varphi(zd)$, et e divise zd.

Définition.

On dit que les éléments d'une partie non vide $\neq \{0\}$ d'un anneau arithmétique σ sont premiers entre eux dans leur ensemble si 1 est un p.g.c.d. de ces éléments.

Si E se compose d'un nombre fini d'éléments $x, y, z, \ldots$, on dit alors aussi que $x, y, z, \ldots$ sont premiers entre eux dans leur ensemble. Si $E = \{x, y\}$ et si x, y sont premiers entre eux dans leur ensemble, on dit aussi que x, y sont premiers entre eux, ou que chacun d'eux est relativement premier à l'autre.

Soit d un p.g.c.d. des éléments d'une partie non vide $E \neq \{0\}$ de σ. On a alors $d^{-1}E = F$ ~~contenue dans σ~~ $\subset \sigma$, et, si δ est un p.g.c.d. des éléments de F, δd est un pgcd des éléments de E, ce qui montre que δ est une unité et que les éléments de $d^{-1}E$ sont premiers entre eux dans leur ensemble.

Proposition.

Soient x, y, z des éléments $\neq 0$ d'un anneau arithmétique σ tels que x divise yz et soit premier à y; x divise alors z.

En effet, 1 ~~étant~~ est un p.g.c.d. de x et de y, z est un p.g.c.d. de xz et de yz; x divisant xz et yz doit diviser z.

~~Définition~~ Proposition.

Soit z un élément $\neq 0$ du corps des quotients d'un anneau arithmétique σ. On peut alors mettre z sous la forme x/y, où x, y sont des éléments de σ premiers entre eux. Cette condition étant satisfaite, si on a aussi $z = x'/y'$, $x' \in \sigma$, $y' \in \sigma$, x' est divisible par x et y' par y.

Mettons en effet z sous la forme x_1/y_1, $x_1 \in \sigma$, $y_1 \in \sigma$, et soit d un p.g.c.d. de x_1 et de y_1. On a $z = x_1 d^{-1} / y_1 d^{-1}$; $x_1 d^{-1}$ et $y_1 d^{-1}$ sont des éléments de σ premiers entre eux. Si $x/y = x'/y'$, on a $y'x = x'y$; x, étant ~~pre~~ relativement premier à y, et divisant $x'y$, divise x', et on voit de même que y divise y'.

~~Représenter un élément z du corps des quotients de σ sous la forme x/y~~ On dit que la représentation $z = x/y$ d'un élément ~~du cor~~ $\neq 0$ du corps des quotients de σ comme quotient de deux éléments de σ premiers entre eux est une forme réduite de z.

PSNS 003 28

Soit E une partie non vide d'un anneau arithmétique σ dont les éléments possèdent un multiple commun m (i.e. m est divisible par tous les éléments de E). Il existe alors un multiple commun e des éléments de E qui ~~est divisible par~~ divise tous les autres multiples communs : il suffit en effet de choisir un $e \in \sigma$ tel que $\varphi(e) = \max_{x \in E} \varphi(x)$ pour tout $\varphi \in \mathfrak{F}\sigma$. Un multiple commun qui possède cette propriété s'appelle alors un plus petit commun multiple (p.p.c.m.) des éléments de E. Si e, e' sont des p.p.c.m. des éléments de E, on a $e' = ue$, où u est une unité.

Si E se compose d'un nombre fini d'éléments $x, y, z, \ldots$ de σ donnés explicitement, on dit aussi que e est un p.p.c.m. de $x, y, z, \ldots$.

Proposition.

~~Soit E un ensemble ne contenant pas 0, d'éléments $\neq 0$ d'un anneau arithmétique σ et d un p.g.c.d. des éléments de E. Si p est le produit des éléments de E, $d^{-1}p$ est un p.p.c.m.~~

Soient x, y des éléments $\neq 0$ d'un anneau arithmétique σ et d un p.g.c.d. de x et y. L'élément $d^{-1}xy$ est alors un p.p.c.m. de x et y.

Il est clair que $d^{-1}xy$ est un multiple commun de x et y. Soit m un multiple commun de x et y ; puisque 1 est un p.g.c.d. de $\frac{x}{d}$ et $\frac{y}{d}$, $\frac{m}{xy}$ est un p.g.c.d. de $\frac{m}{d}$ et de $\frac{my}{xy}$, qui sont tous deux divisibles par y/d ; m est donc divisible par xy/d.

Théorème.

Tout domaine d'intégrité σ dans lequel tous les idéaux sont principaux est un anneau arithmétique.

Il suffit de montrer que σ est normal. Soit $\mathfrak{p} = \sigma p$ un idéal premier de σ, distinct de (0) et de σ. ~~Mais soit q un élément de $\bigcap_{n=1}^{\infty} \mathfrak{p}^n$, et soit $\mathfrak{a}$ l'idéal engendré par les qp^{-n} $(1 \leq n < \infty)$. On a $\mathfrak{a} = \sigma a$, $a \in \sigma$, et on peut écrire $a = \sum_{i=1}^{m} x_i q p^{-i}$, $x_i \in \sigma$. On a $qp^{-(m+1)} = u \sum_{i=1}^{m} q p^{-i}$, d'où $q = qu \sum_{i=1}^{m} x_i p^{m+1-i}$. Si on avait $q \neq 0$, on en conclurait $1 = u \sum_{i=1}^{m} x_i p^{m+1-i} \in p\sigma = \mathfrak{p}$, ce qui n'est pas. Donc $\bigcap_{n=1}^{\infty} \mathfrak{p}^n = (0)$. Si donc x est un élément $\neq 0$ de σ, il est impossible que $x p^{\ldots} \in \mathfrak{p}^n$ pour tout entier $n > 0$, soit $\varphi(x)$ le plus grand entier $n \geq 0$ tel que $x \in \mathfrak{p}^n$. Si $x, y, x+y$ sont des éléments $\neq 0$ de σ, on a évidemment $\varphi(x+y) \geq \min\{\varphi(x), \varphi(y)\}$,~~

Soit $\sigma_{\mathfrak{p}}$ l'anneau des quotients de $\mathfrak{p}$. Il résulte alors immédiatement du lemme, que tout idéal de $\sigma_{\mathfrak{p}}$ est principal. Faisant usage de la Prop., on en conclut que $\sigma_{\mathfrak{p}}$ est l'anneau d'une valuation normée φ du corps des quotients K de σ.

~~$\varphi(xy) \geq \varphi(x)+\varphi(y)$. D'autre part, on a $x = p^{\varphi(x)}x'$, $y = p^{\varphi(y)}y'$ où x', y' sont dans o mais non plus dans $\mathfrak{p}$. L'idéal $\mathfrak{p}$ étant premier, $x'y'$ n'est pas dans $\mathfrak{p}$, d'où $\varphi(xy) = \varphi(x)+\varphi(y)$. Enfin on a $\varphi(p) \neq 1$; on peut donc prolonger φ en une valuation du corps des quotients K de o dont le groupe des valeurs est le groupe additif des entiers~~ - Montrons que σ est l'intersection des anneaux des valuations φ obtenues de cette manière. Soit $z = x/y$ un élément $\neq 0$ de K, avec $x \in o$, $y \in o$. Soit z un générateur de l'idéal $ox+oy$; on a donc $xz^{-1} \in o$, $yz^{-1} \in o$, $z = (xz^{-1})/(yz^{-1})$ et $oxz^{-1}+oyz^{-1} = o$. Supposons que ~~l'on ait $\varphi(z) \geq 0$ pour toute valuation φ obtenue de la manière indiquée plus haut~~. Alors yz^{-1} n'est pas une unité, et par suite ~~il serait~~ contenu dans un idéal premier $\mathfrak{p} \neq o$; puisque $oxz^{-1}+oyz^{-1} = o$, $\mathfrak{p}$ ne contient pas xz^{-1}. Si φ est la valuation qui correspond à $\mathfrak{p}$, on a $\varphi(xz^{-1}) = 0$, $\varphi(yz^{-1}) > 0$, d'où $\varphi(z) < 0$, ce qui démontre notre assertion. ~~Reste à~~ Il reste à montrer qu'un élément $x \neq 0$ de o n'est contenu que dans un nombre fini d'idéaux premiers. Soit E un ensemble infini d'idéaux premiers, et soit q un élément de l'intersection des idéaux premiers de E. ~~Pour chaque $\mathfrak{p} \in E$ form~~ Représentons chaque $\mathfrak{p} \in E$ sous la forme $o\mathfrak{p}_{\mathfrak{p}}$, et soit $\mathfrak{r}$ l'idéal engendré par les $q/p_{\mathfrak{p}}$ ($\mathfrak{p} \in E$). On $\mathfrak{r} = oa$, $a \in \mathfrak{r}$; on a $a = \sum_{i=1}^{n} x_i\, q/p_{\mathfrak{p}_i}$, $x_i \in o$, $\mathfrak{p}_i \in E$. Soit $\mathfrak{p}$ un idéal de E distinct de $\mathfrak{p}_1, \dots, \mathfrak{p}_n$; on a $q/p_{\mathfrak{p}} = yq \sum_{i=1}^{n} x_i/p_{\mathfrak{p}_i}$, $y \in o$, d'où il résulte que $qp_{\mathfrak{p}}$ divise $p_{\mathfrak{p}_1} \cdots p_{\mathfrak{p}_n} q$. ~~Si on avait $\mathfrak{p} \subset \mathfrak{p}_i$ pour~~ ~~avait $q \neq 0$, $p_{\mathfrak{p}_1} \cdots p_{\mathfrak{p}_n}$ serait multiple de $p_{\mathfrak{p}}$, donc contenu dans $\mathfrak{p}$; $\mathfrak{p}$ étant premier, l'un des $\mathfrak{p}_i$ serait contenu dans $\mathfrak{p}$, et on aurait $\mathfrak{p}_i = \mathfrak{p}$, avec $\mathfrak{p}_i \in o$~~ Or, $\mathfrak{p}$ étant distinct de $\mathfrak{p}_1, \dots, \mathfrak{p}_n$, aucun des $p_{\mathfrak{p}_i}$ n'est dans $\mathfrak{p}$; $\mathfrak{p}$ étant premier, $p_{\mathfrak{p}_1} \cdots p_{\mathfrak{p}_n}$ n'est pas dans $\mathfrak{p}$ et n'est par suite pas divisible par $p_{\mathfrak{p}}$; $qp_{\mathfrak{p}_1} \cdots p_{\mathfrak{p}_n}$ étant divisible par $qp_{\mathfrak{p}}$, on a $q = 0$, $\bigcap_{\mathfrak{p} \in E} \mathfrak{p} = \{o\}$. Le théorème est donc démontré.

x ne sort pas dans σ

Remarquons d'abord que si $\mathfrak{p} = o\mathfrak{p}$ et $\mathfrak{q} = oq$ sont des idéaux premiers différents de $\{o\}$ et de o, l'inclusion $\mathfrak{q} \subset \mathfrak{p}$ implique $\mathfrak{q} = \mathfrak{p}$. On a en effet $q = pr$, $r \in o$; l'un des éléments p, r est donc dans $\mathfrak{q}$. Si on avait $p \in o\mathfrak{q}$, p serait une unité, ce qui n'est pas. Donc $p \in \mathfrak{q}$ et $\mathfrak{p} = \mathfrak{q}$.

Corollaire 1.

L'anneau $\underline{Z}$ des entiers rationnels est un anneau ~~euclidien~~ arithmétique.

En effet, un idéal de $\underline{Z}$, étant un sous-groupe du groupe additif de $\underline{Z}$, est composé de tous les multiples d'un certain entier et est donc principal.

Les unités de l'anneau $\underline{Z}$ sont $+1$ et -1. Il résulte tout de suite de la Prop. que les éléments irréductibles de $\underline{Z}$ sont les nombres $\pm p$, où p est premier. La décomposition d'un entier >0 en facteurs premiers est donc un cas particulier de la décomposition en facteurs irréductibles dans un anneau arithmétique.

Corollaire 2. L'anneau $K[X]$ des polynomes en une lettre X à coefficients dans un corps K est un anneau ~~est~~ arithmétique

On sait en effet que tout idéal de $K[X]$ est principal. Les éléments irréductibles de $K[X]$ sont les polynomes que nous avons déjà appelés irréductibles au Chapitre . Les unités de $K[X]$ sont évidemment les éléments $\neq 0$ de K; chaque idéal premier $\mathfrak{p}$ de $K[X]$, différent de $\{0\}$ et de $K[X]$, est donc engendré par un polynome irréductible unitaire et par un seul. ~~Nous obtenons donc le théorème suivant~~

Par ailleurs on remarquera que nous avons établi dans le cours de la démonstration du théorème que tout idéal premier $\neq \{0\}$ et de σ d'un anneau à idéaux tres principaux est maximal.

~~Théorème~~

~~Tout polynome $\neq 0$ en une lettre X à coefficients dans un~~

Théorème

Soit σ un anneau normal. L'anneau $\sigma[X]$ des polynomes en une lettre X à coefficients dans σ est alors normal. Si σ est un anneau arithmétique, il en est de même de $\sigma[X]$.

Désignons par K le corps des quotients de σ, par Φ la famille des valuations essentielles normées de σ et par Ψ la famille des valuations essentielles normées de l'anneau $K[X]$. Soit φ un élément de Φ. ~~Si $f \in \sigma[X]$~~ Soit $f = \sum_{i=0}^{n} a_i X^i$ un élément de $\sigma[X]$; posons $\varphi^*(f) = \min_{0 \le i \le n} \varphi(a_i)$. Il est clair que, si $f, g \in \sigma[X]$, on a $\varphi^*(f+g) \ge \min\{\varphi^*(f), \varphi^*(g)\}$;

Si $f = \sum_{i=0}^{n} a_i X^i$, $g = \sum_{j=0}^{m} b_j X^j$, les coefficients de fg sont des sommes de produits $a_i b_j$, d'où $\varphi^*(fg) \geq \varphi^*(f) + \varphi^*(g)$.

Montrons que l'égalité a lieu. On peut supposer que $f \neq 0$, $g \neq 0$. Soient a, b des éléments de σ tels que $\varphi^*(f) = \varphi(a)$, $\varphi^*(g) = \varphi(b)$, et soit $f' = a^{-1} f$, $g' = b^{-1} g$. Les coefficients de f', g' appartiennent donc à l'anneau σ' de la valuation φ. Soit $\mathfrak{p}'$ l'idéal des non unités de σ'; l'homomorphisme canonique de σ' sur $\sigma'/\mathfrak{p}'$ se prolonge en un homomorphisme h de $\sigma'[X]$ sur $(\sigma'/\mathfrak{p}')[X]$ tel que $h(X) = X$. L'un au moins des coefficients de chacun des polynomes f', g' est une unité de σ', d'où $h(f') \neq 0$ et $h(g') \neq 0$. L'anneau $\sigma'/\mathfrak{p}'$ étant un domaine d'intégrité, on a $h(f'g') = h(f')h(g') \neq 0$, ce qui montre que l'un au moins des coefficients de $f'g'$ est une unité de σ'. Or $f'g' = (ab)^{-1} fg$; il existe donc un coefficient c de fg tel que $\varphi(c) = \varphi(ab) = \varphi^*(f) + \varphi^*(g)$, et on a $\varphi^*(fg) = \varphi^*(f) + \varphi^*(g)$. L'application φ^* peut donc se prolonger en une valuation que nous désignerons aussi par φ^*, de $K(X)$. Soit Φ^* la famille des valuations φ^*. L'anneau $\sigma[X]$ est évidemment contenu dans l'intersection $\mathfrak{J}$ des anneaux des valuations de la famille $\Phi^* \cup \Psi$. Soit inversement f un élément de $\mathfrak{J}$. Puisque $K[X]$ est normal, on a $f \in K[X]$; si a est un coefficient de f, on a $\varphi(a) \geq \varphi^*(f) \geq 0$ pour tout $\varphi \in \Phi$, d'où $a \in \sigma$ et $f \in \sigma[X]$. On a donc $\mathfrak{J} = K[X]$. Si $f \neq 0$, il n'y a qu'un nombre fini de valuations $\psi \in \Psi$ telles que $\psi(f) > 0$; si a est un coefficient $\neq 0$ de f, $\varphi^*(f) > 0$ implique $\varphi(a) > 0$; il n'y a donc qu'un nombre fini de $\varphi^* \in \Phi^*$ tels que $\varphi^*(f) > 0$. L'anneau $\sigma[X]$ est donc normal. Supposons maintenant que σ soit un anneau arithmétique. Si $\varphi \in \Phi$, l'idéal des $x \in \sigma$ tels que $\varphi(x) > 0$ est engendré par un élément p, d'où il résulte immédiatement que l'idéal des $f \in \sigma[X]$ tels que $\varphi^*(f) > 0$ est engendré par p. Si $\psi \in \Psi$, l'idéal $\mathfrak{P}$ des éléments $g \in K[X]$ tels que $\psi(g) > 0$ est engendré par un polynome f_1. Multipliant tous les éléments de f_1 par un élément convenable de σ, on obtient un générateur f_2 de $\mathfrak{P}$ situé dans $\sigma[X]$. Divisant les coefficients de f_2 par un

p.g.c.d. de ces coefficients, on voit que $\varphi = K[X] f$, où f est un polynome de $\sigma[X]$ dont les coefficients sont premiers entre eux dans leur ensemble. Il en résulte que $\varphi^*(f) = 0$ pour tout $\varphi \in \Phi$; on a aussi $\psi'(f) = 0$ pour tout $\psi' \in \Psi$ distinct de ψ. De plus on a $\psi(f) = 1$; on en conclut que f est un générateur de l'idéal des $x \in \sigma[X]$ tels que $\psi(x) > 0$. Nous avons donc démontré que $\sigma[X]$ est un anneau arithmétique.

Par ailleurs, nous avons obtenu au cours de la démonstration les résultats suivants.

Proposition.

Soit φ une valuation d'un corps K. On peut alors ~~étendre~~ prolonger φ par une valuation φ^* du corps des fractions rationnelles en une lettre X à coefficients dans K telle que $\varphi^*(\sum_{i=0}^{n} a_i X^i) = \min_{0 \le i \le n} \varphi(a_i)$ si $a_i \in K$ $(0 \le i \le n)$

La démonstration qu'on a donnée plus haut de ce fait ne dépendait en effet pas de ce que la valuation φ considérée était une valuation essentielle normée d'un anneau normal.

Proposition.

Soit $\sigma[X]$ l'anneau des polynomes ~~irréductible~~ en X à coefficients dans un anneau arithmétique σ. Un élément irréductible de $\sigma[X]$ est ou bien un élément irréductible de σ ou bien un polynome irréductible dans $K[X]$. Tout polynome irréductible dans $K[X]$ se met sous la forme af, où $a \in K$ et f est un ~~polynome~~ élément irréductible de $\sigma[X]$; pour que f soit lui-même irréductible dans $\sigma[X]$, il faut et suffit que ses coefficients soient premiers entre eux dans leur ensemble.

Si p est un élément irréductible de σ, l'~~élément~~ idéal engendré par p dans $\sigma[X]$ est premier.

Raisonnant par récurrence sur n, on déduit immédiatement du Théorème le résultat suivant :

Proposition.

Si σ est un anneau arithmétique, l'anneau des polynomes en n lettres à coefficients dans σ est un anneau arithmétique. En particulier, l'anneau des polynomes en n lettres à coefficients dans un corps est un anneau arithmétique.

On remarquera que, si $n \geq 2$, l'anneau $K[X_1, \dots, X_n]$ des polynomes en n lettres $X_1, \dots, X_n$ à coefficients dans un corps K n'est pas un anneau à idéaux tous principaux. Soit en effet $\mathfrak{p}$ l'idéal engendré par $X_1, \dots, X_n$; il est clair que $1 \notin \mathfrak{p}$. D'autre part, $X_1, \dots, X_n$ sont évidemment irréductibles et engendrent des idéaux qui sont $\neq \mathfrak{p}$; $\mathfrak{p}$ n'est donc pas un idéal premier minimal, ~~et ne peut par suite être principal~~ ce qui montre que $K[X_1, \dots, X_n]$ n'est pas un anneau à idéaux tous principaux.

et que $\mathfrak{p}$ se compose des éléments f tels que $f(X_1, \dots, X_n) = 0$ et est par suite premier.

Proposition.

Soit f un polynome homogène $\neq 0$ en n lettres $X_1, \dots, X_n$ à coefficients dans un corps K. ~~Soit~~ Tout polynome qui divise f est aussi homogène.

Considérons $K[X_1, \dots, X_n]$ comme sous-anneau de $K[X_1, \dots, X_n, T]$, où T est une nouvelle lettre. On a donc $f(X_1 T, \dots, X_n T) = T^m f(X_1, \dots, X_n)$ où m est le degré de f. Soit g un élément de $K[X_1, \dots, X_n]$ qui divise f. Il est alors clair que $g(X_1 T, \dots, X_n T)$ divise $f(X_1 T, \dots, X_n T)$ dans $K[X_1, \dots, X_n, T]$ et, à fortiori, dans $K(X_1, \dots, X_n)[T]$. Donc $g(X_1 T, \dots, X_n T)$, considéré comme polynome en T à coefficients dans $K(X_1, \dots, X_n)$, divise T^m. Le polynome T étant irréductible, les diviseurs de T^m dans $K(X_1, \dots, X_n)[T]$ sont les $T^a u$, $0 \leq a \leq m$, $u \in K(X_1, \dots, X_n)$. On a donc $g(X_1 T, \dots, X_n T) = T^a h(X_1, \dots, X_n)$, h étant une fraction rationnelle. Si on remplace T par 1, on voit que $h = g$; g est donc homogène.

On voit donc que, si on décompose un polynome homogène $\neq 0$ en facteurs irréductibles, les polynomes irréductibles qui interviendront dans cette décomposition seront tous homogènes.

Anneaux de Dedekind.

Définition

On appelle anneau de Dedekind un anneau normal dont toutes les valuations non triviales sont essentielles.

Proposition

Pour qu'un anneau normal o soit un anneau de Dedekind, il faut et suffit que tout idéal ~~minimal de o soit~~ premier ~~$\neq (0)$~~ de o autre que (0) ou o soit minimal.

Supposons que o soit un anneau de Dedekind, et soit $\mathfrak{p}$ un idéal premier de o distinct de (0) et de o. Il existe alors une valuation φ du corps des quotients de o telle que $\mathfrak{p}$ soit l'ensemble des $x \in o$ tels que $\varphi(x) > 0$ (Théorème , §); o étant un anneau de Dedekind, φ en essentielle, d'où il résulte que $\mathfrak{p}$ est minimal. Supposons inversement la condition satisfaite, et soit φ une valuation non triviale de o. Soit $\mathfrak{p}_\varphi$ l'idéal des $x \in o$ tels que $\varphi(x) > 0$; on sait que $\mathfrak{p}_\varphi \neq (0)$ (cf. §) et on a évidemment $\mathfrak{p}_\varphi \neq o$; $\mathfrak{p}_\varphi$ est donc minimal. Or il existe une valuation essentielle φ' de o telle que $\mathfrak{p}_{\varphi'} \subset \mathfrak{p}_\varphi$ (Lemme 1, §), d'où $\mathfrak{p}_{\varphi'} = \mathfrak{p}_\varphi$. Il existe donc un élément $u \notin o$ du corps des quotients de o tel que $u\mathfrak{p}_\varphi \subset o$, et φ est essentielle.

~~Observons que, dans un dom~~

Proposition.

Un domaine d'intégrité o dont tous les idéaux sont principaux est un anneau de Dedekind.

En effet, on sait que o est normal (Théorème , §), et les idéaux premiers ~~$\neq (0)$~~ autres que (0) ou o de o, étant principaux, sont minimaux.

PSTS003 35

Définition

Soit o un domaine d'intégrité, et soit K le corps des quotients de o. On appelle idéal fractionnaire pour o un sous-module $\mathfrak{a}$ de la structure de module par rapport à o de K ~~tel qu'il existe un $x \in K$ tel que $x\mathfrak{a} \subset o$~~ qui est contenu dans un module de la forme $o\alpha$, $\alpha \in K$.

Les idéaux de o sont donc les idéaux fractionnaires contenus dans o.

m/ Soient $\mathfrak{a}$ et $\mathfrak{a}'$ des idéaux fractionnaires pour o. Le module engendré par les produits xx', $x \in \mathfrak{a}$, $x' \in \mathfrak{a}'$ (module qui se compose des sommes de semblables produits) est alors un idéal fractionnaire, car si $x\mathfrak{a} \subset o\alpha$, $x'\mathfrak{a}' \subset o\alpha'$, on a $\mathfrak{m} \subset o\alpha\alpha'$. On dit que $\mathfrak{m}$ est le produit des idéaux fractionnaires $\mathfrak{a}$ et $\mathfrak{a}'$, et on écrit $\mathfrak{m} = \mathfrak{a}\mathfrak{a}'$ (Il faut cependant se garder de confondre le produit ainsi défini avec l'ensemble des produits d'éléments de $\mathfrak{a}$ par des éléments de $\mathfrak{a}'$, ensemble que l'on notait jusqu'ici aussi $\mathfrak{a}\mathfrak{a}'$). La multiplication ainsi définie dans l'ensemble des idéaux fractionnaires est évidemment associative et commutative ; si o possède un élément unité, l'idéal o est élément unité pour cette multiplication.

~~Proposition~~

~~Soient o un anneau de Dedekind, et Φ la famille des valuations normées de o. Soit $\mathfrak{a}$ un idéal fractionnaire $\neq (0)$ pour o ; si $\varphi \in \Phi$, posons $\varphi(\mathfrak{a}) = \min_{x \in \mathfrak{a}} \varphi(x)$. L'idéal $\mathfrak{a}$ est alors fractionnaire et est alors l'ensemble des éléments x du corps des quotients K de o tels que $\varphi(x) \geq \varphi(\mathfrak{a})$ pour tout $\varphi \in \Phi$. Il n'y a qu'un nombre fini de $\varphi \in \Phi$ tels que $\varphi(\mathfrak{a}) \neq 0$; si on se donne pour chaque $\varphi \in \Phi$ un entier m_φ de telle manière qu'il n'y ait qu'un nombre fini de $\varphi \in \Phi$ pour lesquels $m_\varphi \neq 0$, il existe un idéal fractionnaire $\mathfrak{a}$ tel que $\varphi(\mathfrak{a}) = m_\varphi$ pour tout $\varphi \in \Phi$.~~

~~Nous démontrerons d'abord la dernière assertion~~

Théorème

L'ensemble des idéaux fractionnaires $\neq (0)$ relatifs à un anneau de Dedekind ~~constitue un~~, muni de la loi de composition multiplicative définie ci-dessus, constitue un groupe.

Désignons par $\mathfrak{a}$ un idéal fractionnaire $\neq (0)$ relatif à un anneau de Dedekind o, et par $\mathfrak{a}'$ l'ensemble des éléments x du corps des quotients K

de σ tels que $x\mathfrak{a}\subset\sigma$. Il en dérive que $\mathfrak{a}'$ est un module par rapport à σ; si a est un élément $\neq 0$ de $\mathfrak{a}$, on a $\mathfrak{a}'\subset\sigma a^{-1}$, ce qui montre que $\mathfrak{a}'$ est un idéal fractionnaire. Montrons que $\mathfrak{a}'\mathfrak{a}=\sigma$. Tout idéal $\neq\sigma$ étant contenu dans au moins un idéal premier $\neq\sigma$, il suffit de montrer qu'un idéal premier $\mathfrak{p}\neq\sigma$ ne peut contenir $\mathfrak{a}'\mathfrak{a}$. Si $\mathfrak{p}\neq\{0\}$, $\mathfrak{p}$ est maximal, et il existe un $u\in K$ non contenu dans σ tel que $u\mathfrak{p}\subset\sigma$; il existe ainsi une valuation normée φ de K telle que $\varphi(u)<0$. Si on avait $\mathfrak{a}'\mathfrak{a}\subset\mathfrak{p}$, on aurait $u\mathfrak{a}'\mathfrak{a}\subset\sigma$, d'où $u\mathfrak{a}'\subset\mathfrak{a}$, et $\mathfrak{a}$ contient un élément $b\neq 0$, car, si $\mathfrak{a}\subset\sigma b$, on a $b\neq 0$ et $b^{-1}\in\mathfrak{a}'$; on a donc $\min_{v\in\mathfrak{a}}\varphi(v)<\infty$, d'où $\min_{v\in\mathfrak{a}}\varphi(uv)<\min_{v\in\mathfrak{a}}\varphi(v)$ et $u\mathfrak{a}'\neq\mathfrak{a}'$.

L'inverse d'un idéal fractionnaire $\mathfrak{a}\neq\{0\}$ dans le groupe des idéaux fractionnaires se note $\mathfrak{a}^{-1}$; il convient de ne pas confondre l'idéal fractionnaire $\mathfrak{a}^{-1}$ avec l'ensemble des x^{-1}, pour $x\in\mathfrak{a}$, $x\neq 0$.

Il résulte de la démonstration du théorème que, si $\mathfrak{a}$ est un idéal fractionnaire $\neq\{0\}$, $\mathfrak{a}^{-1}$ est l'ensemble des x tels que $x\mathfrak{a}\subset\sigma$.

Proposition.

Le groupe des idéaux fractionnaires $\neq\{0\}$ pour un anneau de Dedekind σ est engendré par les idéaux premiers autres que $\{0\}$ ou σ.

Soient $\mathfrak{a}=\prod_{\mathfrak{p}}\mathfrak{p}^{a(\mathfrak{p})}$, $\mathfrak{b}=\prod_{\mathfrak{p}}\mathfrak{p}^{b(\mathfrak{p})}$ des idéaux fractionnaires $\neq\{0\}$ (les produits sont étendus à l'ensemble des idéaux premiers $\mathfrak{p}$ autres que $\{0\}$ ou σ; on a $a(\mathfrak{p})=b(\mathfrak{p})=0$ excepté pour un nombre fini d'idéaux premiers). On a alors $a(\mathfrak{p})=\min_{x\in\mathfrak{a}}\varphi_{\mathfrak{p}}(x)$, où $\varphi_{\mathfrak{p}}$ est la valuation normée dans l'anneau des quotients de $\mathfrak{p}$. Si on pose $c(\mathfrak{p})=\min\{a(\mathfrak{p}),b(\mathfrak{p})\}$, $d(\mathfrak{p})=\max\{a(\mathfrak{p}),b(\mathfrak{p})\}$, on a

$\mathfrak{a}\mathfrak{b}=\prod_{\mathfrak{p}}\mathfrak{p}^{a(\mathfrak{p})+b(\mathfrak{p})}$; $\mathfrak{a}+\mathfrak{b}=\prod_{\mathfrak{p}}\mathfrak{p}^{c(\mathfrak{p})}$; $\mathfrak{a}\cap\mathfrak{b}=\prod_{\mathfrak{p}}\mathfrak{p}^{d(\mathfrak{p})}$

Soit Φ l'ensemble des idéaux fractionnaires valuations normées de σ. Si $\mathfrak{a}$ est un idéal fractionnaire pour σ Soit P l'ensemble des idéaux premiers autres que $\{0\}$ ou σ. Si $\mathfrak{a}$ est un idéal fractionnaire $\neq\{0\}$, et $\mathfrak{p}\in P$, nous poserons $\varphi_{\mathfrak{p}}(\mathfrak{a})=\min_{x\in\mathfrak{a}}\varphi_{\mathfrak{p}}(x)$. Si $\mathfrak{b}$ est un autre idéal fractionnaire $\neq\{0\}$, on a $\varphi_{\mathfrak{p}}(\mathfrak{a}\mathfrak{b})=\varphi_{\mathfrak{p}}(\mathfrak{a})+\varphi_{\mathfrak{p}}(\mathfrak{b})$. En effet, il est clair que les conditions $x_i\in\mathfrak{a}$, $y_i\in\mathfrak{b}$ $(1\leq i\leq h)$ entraînent $\varphi_{\mathfrak{p}}(\sum_{i=1}^{h}x_iy_i)\geq\varphi_{\mathfrak{p}}(\mathfrak{a})+\varphi_{\mathfrak{p}}(\mathfrak{b})$; par ailleurs, il existe des éléments $x\in\mathfrak{a}$, $y\in\mathfrak{b}$ tels que $\varphi_{\mathfrak{p}}(x)=\varphi_{\mathfrak{p}}(\mathfrak{a})$, $\varphi_{\mathfrak{p}}(y)=\varphi_{\mathfrak{p}}(\mathfrak{b})$, d'où $xy\in\mathfrak{a}\mathfrak{b}$, $\varphi_{\mathfrak{p}}(xy)=\varphi_{\mathfrak{p}}(\mathfrak{a})+\varphi_{\mathfrak{p}}(\mathfrak{b})$. Si $\mathfrak{a}\subset\mathfrak{c}\subset\sigma$, on a $\varphi_{\mathfrak{p}}(v)\leq\varphi_{\mathfrak{p}}(\mathfrak{c})\leq\varphi_{\mathfrak{p}}(\mathfrak{a})$ pour tout $\mathfrak{p}\in P$; il n'y a donc qu'un nombre fini d'idéaux $\mathfrak{p}\in P$ tels que $\varphi_{\mathfrak{p}}(\mathfrak{a})\neq 0$. Si $\mathfrak{p}\in P$, on a évidemment $\varphi_{\mathfrak{p}}(\mathfrak{p})=1$, $\varphi_{\mathfrak{q}}(\mathfrak{p})=0$ pour $\mathfrak{q}\in P$, $\mathfrak{q}\neq\mathfrak{p}$; si on fait correspondre à chaque $\mathfrak{p}\in P$ un exposant $a(\mathfrak{p})$ entier tel qu'il n'y ait qu'un

Si $\mathfrak{a}$ se compose de tous les éléments x du corps des quotients K de σ tels que $\varphi_{\mathfrak{p}}(x)\geq a(\mathfrak{p})$ pour tout idéal premier $\mathfrak{p}$ autre que $\{0\}$ ou σ.

l'ensemble des $\varphi_{\mathfrak{p}}(x)$, $x\in\mathfrak{a}$, est borné inférieurement, car, si $\mathfrak{a}\subset\sigma$, on a $\varphi_{\mathfrak{p}}(x)\geq\varphi_{\mathfrak{p}}(\mathfrak{a})$ pour tout $x\in\mathfrak{a}$;

PSMS 003 37

Théorème. ~~Soit~~ Soient o un anneau de Dedekind, $\varphi_1, \cdots, \varphi_h$ des valuations normées distinctes de o, $x_1, \cdots, x_h$ des éléments du corps des quotients K de o et $m_1, \cdots, m_h$ des entiers. Il existe alors un élément x de K tel que $\varphi_i(x - x_i) \geq m_i$ $(1 \leq i \leq h)$ et $\varphi(x) \geq 0$ pour toute valuation normée φ de o distincte de $\varphi_1, \cdots, \varphi_h$.

Il n'y a qu'un nombre fini de valuations normées ψ de o telles que l'un au moins des $\psi(x_i)$ soit < 0 ; ~~soit $\{\varphi_1, \cdots, \varphi_h, \cdots, \varphi_{h+k}\}$~~ adjoignant à l'ensemble $\{\varphi_1, \cdots, \varphi_h\}$ celle de ces valuations ψ que n'y figurent pas, on obtient un ensemble $\{\varphi_1, \cdots, \varphi_h, \cdots, \varphi_{h+k}\}$. ~~Nous poserons~~ Si $h < i \leq h+k$, nous poserons $x_i = 0$, $m_i = 0$.

$\Rightarrow$ Désignons par $\mathfrak{p}_i$ l'idéal premier de o composé des $x \in o$ tels que $\varphi_i(x) > 0$, et soit m un entier tel que $m + \varphi_i(x_j) \geq \max\{m_1, \cdots, m_{h+k}\} + 1$ $(1 \leq i, j \leq h+k)$. Il résulte de la Prop. que $\mathfrak{p}_i^m + \prod_{j \neq i} \mathfrak{p}_j^m = o$. ~~Il y a donc~~ Il y a donc des éléments $y_i \in \prod_{j \neq i} \mathfrak{p}_j^m$, $y_i' \in \mathfrak{p}_i^m$ tels que $y_i + y_i' = 1$, d'où $\varphi_i(y_i - 1) \geq m$, $\varphi_j(y_i) \geq m$ si $j \neq i$. Posons $x' = \sum_{i=1}^{h+k} x_i y_i$; on a $\varphi_i(x' - x_i) = \varphi_i(x_i(y_i - 1)) + \varphi_i(\sum_{j \neq i} x_j y_j) \geq m + \min_{1 \leq j \leq h+k} \varphi_i(x_j) \geq m_i + 1$ Si $i > h$, on a donc $\varphi_i(x') \geq 0$; si φ est une valuation normée de o qui ne figure pas parmi $\varphi_1, \cdots, \varphi_{h+k}$, on a $\varphi(x_i) \geq 0$ $(1 \leq i \leq h+k)$, d'où $\varphi(x') \geq 0$. Par ailleurs, il existe un $x'' \in K$ tel que $\varphi_i(x'') = m_i$ $(1 \leq i \leq h)$, $\varphi(x'') \geq 0$ pour toute valuation normée φ de o distincte de $\varphi_1, \cdots, \varphi_h$ (Théorème 2 . .). L'élément $x = x' + x''$ possède les propriétés requises.

~~nombre fini d'idéaux $\mathfrak{p} \in P$ pour lesquels $a(\mathfrak{p}) \neq 0$, on a de~~
~~$\varphi_{\mathfrak{p}}\left(\prod_{\mathfrak{p}} \mathfrak{p}^{a(\mathfrak{p})}\right) = a(\mathfrak{p})$. Soit a_1 l'ensemble des éléments x du corps~~
~~des quotients de o tels que $\varphi_{\mathfrak{p}}(x) \geq \varphi_{\mathfrak{p}}(a)$ pour tout $\mathfrak{p} \in P$; on a~~
~~donc $a \subset a_1$, a_1 est un module par rapport à o contenu dans~~
~~o, donc un idéal fractionnaire, et $\varphi_{\mathfrak{p}}(a_1) = \varphi_{\mathfrak{p}}(a)$ pour tout $\mathfrak{p} \in P$,~~
~~d'où $\varphi_{\mathfrak{p}}(a^{-1} a_1)$~~ Posons $a' = a^{-1}$, d'où $\varphi_{\mathfrak{p}}(a') = -\varphi_{\mathfrak{p}}(a)$ pour tout $\mathfrak{p} \in P$; on a donc $a = a'^{-1}$, et a est l'ensemble des x tels que $xa' \subset o$. Il en résulte immédiatement que tout x tel que $\varphi_{\mathfrak{p}}(x) \geq \varphi_{\mathfrak{p}}(a)$ pour tout $\mathfrak{p} \in P$ est dans a, donc que a est l'ensemble des x satisfaisant à cette condition. Ceci montre que a est entièrement déterminé par la donnée des entiers $\varphi_{\mathfrak{p}}(a)$. Si $\mathfrak{p} \in P$, on a évidemment $\varphi_{\mathfrak{p}}(\mathfrak{p}) = 1$, $\varphi_{\mathfrak{q}}(\mathfrak{p}) = 0$ pour $\mathfrak{q} \in P$, $\mathfrak{q} \neq \mathfrak{p}$, d'où $\varphi_{\mathfrak{p}}\left(\prod_{\mathfrak{p}} \mathfrak{p}^{\varphi_{\mathfrak{p}}(a)}\right) = \varphi_{\mathfrak{p}}(a)$ pour tout $\mathfrak{p} \in P$, et $a = \prod_{\mathfrak{p}} \mathfrak{p}^{\varphi_{\mathfrak{p}}(a)}$. Pour que $a \subset b$, il est évidemment nécessaire et suffisant que $\varphi_{\mathfrak{p}}(a) \geq \varphi_{\mathfrak{p}}(b)$ pour tout $\mathfrak{p} \in P$; les formules données pour $a+b$ et $a \cap b$ résultent alors immédiatement du fait que $a+b$ est le plus petit idéal fractionnaire contenant a et b tandis que $a \cap b$ est le plus grand idéal fractionnaire contenu dans a et b.

<u>~~Théorème~~ Proposition</u>.

<u>Soient o un anneau de Dedekind, $a_1, \dots, a_h$ des idéaux fractionnaires $\neq \{0\}$ de o et $x_1, \dots, x_h$ des éléments de o. Pour qu'il existe un $x \in o$ tel que $x \equiv x_i \pmod{a_i}$ $(1 \leq i \leq h)$, il est nécessaire et suffisant que $x_i \equiv x_j \pmod{a_i + a_j}$ $(1 \leq i, j \leq h)$.</u>

Les conditions sont évidemment nécessaires. Supposons les remplies. Gardant les notations de la démonstration de la Prop., désignons par $\mathfrak{p}_1, \dots, \mathfrak{p}_k$ tous les idéaux premiers autres que $\{0\}$ ou o qui contiennent au moins un des idéaux a_i. Pour chaque ℓ $(1 \leq \ell \leq k)$, choisissons un $i(\ell)$ tel que $\varphi_{\mathfrak{p}_\ell}(a_{i(\ell)})$ soit le plus grand des entiers $a_{\ell,1} = \varphi_{\mathfrak{p}_\ell}(a_1), \dots, a_{\ell,h} = \varphi_{\mathfrak{p}_\ell}(a_h)$, et posons $y_\ell = x_{i(\ell)}$. Si $1 \leq i \leq h$, $x_i - x_{i(\ell)}$ appartient à $a_i + a_{i(\ell)}$ donc aussi à $\mathfrak{p}_\ell^{a_{\ell,i}} + \mathfrak{p}_\ell^{a_{\ell,i(\ell)}} = \mathfrak{p}_\ell^{a_{\ell,i}}$. En vertu du Théorème, il existe un $y \in o$ tel que $\varphi_{\mathfrak{p}_\ell}(y - y_\ell) \geq a_{\ell,i(\ell)}$ $(1 \leq \ell \leq k)$, d'où $\varphi_{\mathfrak{p}_\ell}(y - x_i) \geq a_{\ell,i}$ $(1 \leq \ell \leq k, 1 \leq i \leq h)$ et $y - x_i \in a_i$ $(1 \leq i \leq h)$.

<u>Proposition</u>.

<u>Soient $\varphi_1, \dots, \varphi_k$ des valuations mutuellement inéquivalentes d'un corps K dont les groupes de valeurs sont isomorphes au groupe additif des entiers. L'intersection o des anneaux de ces valuations est alors un anneau à idéaux tous principaux. Soit donné pour chaque i $(1 \leq i \leq h)$ un élément $x_i \in K$</u>

et un élément γ_i du groupe des valeurs de φ_i ; il existe alors un $x \in K$ tel que $\varphi_i(x - x_i) \geq \gamma_i$ $(1 \leq i \leq h)$.

On peut évidemment supposer les valuations φ_i normées. Il en résulte que o est un anneau normal. Toute valuation essentielle normée de o est équivalente à l'une des valuations φ_i, donc est identique à l'une de ces valuations. ~~Soient $\varphi_1, \dots, \varphi_k$ celles des valuations essen~~ On peut supposer que $\varphi_1, \dots, \varphi_k$ sont celles des valuations φ_i $(1 \leq i \leq h)$ qui sont essentielles pour o. Il existe donc des éléments $p_1, \dots, p_k$ de o tels que $\varphi_{p_i}(p_i) = 1$, $\varphi_{p_i}(p_j) = 0$ si $1 \leq i, j \leq k$, $i \neq j$. Soit $\mathfrak{r}$ un idéal $\neq \mathfrak{r}o$ de o ; posons $a_i = \min_{x \in \mathfrak{r}} \varphi_i(x)$, $u = \prod_{i=1}^{k} p_i^{a_i}$; on a donc $u^{-1}\mathfrak{r} \subset o$. D'autre part, $\mathfrak{r}$ contient pour chaque i $(1 \leq i \leq k)$ un élément x_i tel que $\varphi_i(x_i) = a_i$; posons $u' = \sum_{i=1}^{k} x_i \prod_{j \neq i, 1 \leq j \leq k} p_j$. On voit tout de suite que $\varphi_i(u') = a_i$ $(1 \leq i \leq j)$; puisque $\varphi_1, \dots, \varphi_k$ sont toutes les valuations essentielles normées de o, on a $u'u^{-1} \in o$, $ou' \subset ou$. Or on a $u' \in \mathfrak{r}$; donc $ou \subset \mathfrak{r}$, et par suite $\mathfrak{r} = \mathfrak{a}u$, ce qui montre que tout idéal de o est principal. Il en résulte que o est un anneau de Dedekind (Théorème), donc que $k = h$, et la dernière assertion de la Prop. résulte du Théorème .

Fin

PSNS003 40

Extensions de valuations.

Soient K un corps, L une extension de K et φ une valuation de K. Il existe alors au moins une valuation ψ de L dont la restriction à K est une valuation équivalente à φ. Soient en effet $\mathcal{O}$ l'anneau de la valuation φ et $\mathfrak{p}$ l'idéal des non-unités de $\mathcal{O}$. Il existe alors une valuation ψ de K dont l'anneau ~~est~~ $\mathcal{O}$ contient $\mathcal{O}$ et telle que $\mathfrak{p}$ soit l'intersection avec $\mathcal{O}$ de l'idéal $\mathfrak{P}$ des non-unités de $\mathcal{O}$. Si x est un élément de K non contenu dans $\mathcal{O}$, on a $x^{-1} \in \mathfrak{p} \subset \mathfrak{P}$, d'où $x^{-1} \notin \mathcal{O}$; il en résulte que $\mathcal{O} \cap K = \mathcal{O}$ et que la restriction de ψ à K est équivalente à φ.

Soy Supposons à présent maintenant que φ soit la restriction de ψ à K. Désignons par Γ et Δ les groupes de valeurs de φ et de ψ respectivement; il est clair que Γ est un sous-groupe de Δ.

Définition.

Soient ψ une valuation d'une extension L d'un corps K et φ sa restriction à K. Si le groupe des valeurs Γ de φ est un sous-groupe d'indice fini de celui Δ de ψ, on dit que l'indice de ramification de ψ par rapport à K est fini et ~~on appelle indice de ramif égal à~~ on appelle indice de ramification de ψ par rapport à K ~~le nombre~~ l'ordre du groupe Δ/Γ.

Gardons les mêmes notations que plus haut, observons que, puisque $\mathfrak{p}$ est un idéal maximal de $\mathcal{O}$, l'anneau $\mathcal{O}/\mathfrak{p}$ est un corps. Il en est de même de $\mathcal{O}/\mathfrak{P}$. On a $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}$; il existe donc un isomorphisme canonique de $\mathcal{O}/\mathfrak{p}$ sur $\mathcal{O}+\mathfrak{P}/\mathfrak{P}$, qui est un sous-corps de $\mathcal{O}/\mathfrak{P}$. Nous pouvons donc identifier $\mathcal{O}/\mathfrak{p}$ avec un sous-corps de $\mathcal{O}/\mathfrak{P}$.

Définition.

Soient φ une valuation d'un corps K, $\mathcal{O}$ l'anneau de valuation de φ et $\mathfrak{P}$ l'idéal premier maximal de $\mathcal{O}$. Le corps $\mathcal{O}/\mathfrak{P}$ s'appelle ~~encore~~ alors le corps des résidus de la valuation φ.

PSAS 003 41

Définition

Soient ψ une valuation d'une extension L d'un corps K, S le corps des restes de ψ et R celui de la restriction de ψ à K. Si S est de degré fini par rapport à R, on dit que ψ est de degré fini par rapport à K et on appelle degré relatif de ψ par rapport à K le degré de S par rapport à R.

Théorème

Soient K un corps, φ une valuation simple de K et L une extension algébrique de degré fini de K. Les valuations de L dont les restrictions à K sont équivalentes à φ sont alors simples ; ~~leurs indices de ramification et~~ si on les suppose normées, il n'y en a qu'un nombre fini ; ~~leurs indices de ramification et degrés relatifs par rapport à K sont finis~~. Si $\psi_1, \dots, \psi_g$ sont toutes les valuations normées de L dont les restrictions à K sont équivalentes à φ, chaque ψ_i est d'indice de ramification e_i fini et de degré relatif fini d_i, et on a $\sum_{i=1}^{g} d_i e_i \leq [L:K]$.

Soit Γ le groupe des valeurs de φ ; désignons par ψ une valuation de L dont la restriction à K est équivalente à φ (et par Γ celui de sa restriction à K) et par Δ le groupe des valeurs de ψ. Soit x un élément $\neq 0$ de L ; si d est le degré de x par rapport à K (on pose $n = [L:K]$), on a une relation de la forme $a_0 x^n + a_1 x^{n-1} + \dots + a_n = 0$, où $a_0, a_1, \dots, a_n$ ne sont pas tous nuls tous des éléments non tous nuls de K. Il existe donc des indices i, j distincts ($0 \leq i < j \leq n$) tels que $\psi(a_i x^{n-i}) = \psi(a_j x^{n-j}) \neq \infty$, d'où $(j-i)\psi(x) = \psi(a_j a_i^{-1}) \in \Gamma$. Puisque $j-i$ divise $n!$, on voit que $n!\,\Delta \subset \Gamma$. ~~Pour chaque $\delta \in \Delta$, désignons par $I(\delta)$ le plus petit entier $m > 0$ tel que $m\delta \in \Gamma$, on a donc toujours $I(\delta) \leq n!$, Pour achever il en résulte que la condition $\delta \equiv \delta'$ (mod Γ) entraîne $I(\delta) = I(\delta')$, et que $I(-\delta) = I(\delta)$. Parmi les éléments $\delta > 0$ de Δ choisissons-en un soit δ_1, pour lequel $I(\delta)$ soit maximum, et soit $e = I(\delta_1)$. On a $e\delta_1 = q\gamma$. On a donc $\delta_1 \leq q\gamma$; soit r le plus grand entier tel que $r\gamma \leq \delta_1$, et posons $\delta = \delta_1 - r\gamma$, d'où $I(\delta) = e$, $0 \leq \delta \leq \gamma$. Si $\delta = 0$, on a $I(\delta_i) = 1$, $\Delta = \Gamma$. Supposons donc $\delta > 0$. Nous allons voir que $e\delta = \gamma$. et posons $I(\delta)\,\delta = f(\delta)\,\gamma$, où γ est le générateur positif de~~

Le groupe Γ, étant engendré isomorphe au groupe $\mathbb{Z}$, est

engendré par un élément γ que l'on peut supposer >0. Si $\delta \in \Delta$, on a $(n!)\delta = z(\delta)\gamma$, où $z(\delta) \in \mathbf{Z}$. Il en résulte que l'application $\delta \to z(\delta)$ est un homomorphisme de Δ dans $\mathbf{Z}$; si $\delta > 0$, on a $n!\,\delta > 0$, d'où $z(\delta) > 0$, et, si $z(\delta) \leq 0$, $z(\delta) < 0$. Il en résulte que notre application est un isomorphisme de Δ sur un sous-groupe de $\mathbf{Z}$, qui contient le groupe $z(\Phi)$ engendré par $n!$. On en conclut que Δ est isomorphe à $\mathbf{Z}$ et que Φ est d'indice fini dans Δ, ce qui signifie que ψ est d'indice de ramification fini par rapport à K.

Désignons par $\psi_1, \dots, \psi_h$ un nombre fini de valuations simples normées distinctes de L dont les restrictions à K sont équivalentes à φ. Soient o l'anneau de valuation de φ et J l'intersection des anneaux de valuation de $\psi_1, \dots, \psi_h$; J est donc un anneau à idéaux principaux ; si $\mathfrak{P}_i$ est l'ensemble des $x \in J$ tels que $\psi_i(x) > 0$, $\mathfrak{P}_1, \dots, \mathfrak{P}_h$ sont tous les idéaux premiers de J (autres que (0) et J). Par ailleurs l'idéal $\mathfrak{p}$ des non-unités de o est principal, soit $\mathfrak{p} = po$; l'idéal pJ engendré par $\mathfrak{p}$ dans J se met sous la forme $\prod_{i=1}^{h} \mathfrak{P}_i^{a_i}$, où $a_i = \min_{x \in pJ} \psi_i(x) = \psi_i(P)$. ~~On a $\psi_i(P) > 0$, et $\psi_i($~~ Or il est clair que $\psi_i(P)$ est le générateur positif du groupe des valeurs de la restriction de ψ_i à K ; $a_i = \psi_i(P)$ est donc égal à l'indice de ramification e_i de ψ_i par rapport à K. Chaque $\mathfrak{P}_i$ est un idéal maximal ; $J/\mathfrak{P}_i$ est donc un corps S_i. On sait que l'anneau de valuation O_i de ψ_i est l'anneau des quotients de $\mathfrak{P}_i$; ~~et que l'idéal est non-unité de $\mathfrak{P}_i$ de~~ il en résulte que S_i est identique au corps des restes de ψ_i. Posons $e = \sum_{i=1}^{h} e_i$; on peut former une suite $(\mathfrak{A}_0, \mathfrak{A}_1, \dots, \mathfrak{A}_e)$ de $e+1$ idéaux de J qui possède les propriétés suivantes : $\mathfrak{A}_0 = J$; si $1 \leq k \leq e$, $\mathfrak{A}_k$ est le produit de $\mathfrak{A}_{k-1}$ par un des idéaux premiers $\mathfrak{P}_1, \dots, \mathfrak{P}_h$, soit par $\mathfrak{P}_{i(k)}$; $\mathfrak{A}_e = pJ$. Pour chaque $k \geq 1$, $\mathfrak{A}_{k-1}/\mathfrak{A}_k$ possède une structure de module par rapport à J. Nous allons voir que ce module est isomorphe à $J/\mathfrak{P}_{i(k)}$. En effet, l'idéal $\mathfrak{A}_{k-1}$ est principal, soit $\mathfrak{A}_{k-1} = J a_{k-1}$; l'application $x \to x a_{k-1}$ donne un isomorphisme de la structure de module par rapport à J de J sur celle de $\mathfrak{A}_{k-1}$, et, puisque

PSPS 003 43

$\mathfrak{o}_k = \mathfrak{o}_{k-1}\mathfrak{p}_{i(k)}$, cet isomorphisme applique $\mathfrak{p}_{i(k)}$ dans $\mathfrak{o}_k$. Inversement, on a $\mathfrak{p}_{i(k)} = a_{k-1}^{-1}\mathfrak{o}_k$; les $x \in J$ tels que $xa_{k-1} \in \mathfrak{o}_k$ sont donc exactement ceux de $\mathfrak{p}_{i(k)}$, ce qui montre que $\mathfrak{o}_{k-1}/\mathfrak{o}_k$ est isomorphe en tant que J-module à $J/\mathfrak{p}_{i(k)}$. J/pJ

La structure de module par rapport à J de ~~$\mathfrak{o}_{k-1}/\mathfrak{o}_k$~~ induit sur cet ensemble une structure de module par rapport à $\mathfrak{o}$; ~~donc~~ or on a $(p\mathfrak{o})\mathfrak{o}_{k-1} \subset \mathfrak{o}_k$; nous avons donc aussi sur ~~$\mathfrak{o}_{k-1}/\mathfrak{o}_k$~~ une structure de module par rapport au corps des restes $R = \mathfrak{o}/p\mathfrak{o}$ de la valuation φ, Nous rappelant que $\mathfrak{o}_{k-1}/\mathfrak{o}_k$ est isomorphe (en tant que J-module) à $J/\mathfrak{p}_{i(k)}$, qui est lui-même le corps des restes de $\psi_{i(k)}$, on voit que $\mathfrak{o}_{k-1}/\mathfrak{o}_k$, en tant qu'espace vectoriel sur R, est isomorphe à la structure d'espace vectoriel sur R du corps des restes $S_{i(k)}$ de $\psi_{i(k)}$.

J/pJ

(Cette structure est évidemment une structure d'espace vectoriel sur R, et les $\mathfrak{o}_k/pJ$ sont des sous-espaces de cet espace vectoriel.)

~~Observ~~ Montrons maintenant que J/pJ est de dimension finie $\leq [L:K]$ par rapport à R. Il suffira de montrer que, si $z_1, \dots, z_m$ sont des éléments de J dont les classes $\bar{z}_1, \dots, \bar{z}_m$ modulo pJ sont linéairement indépendantes sur R, les éléments $z_1, \dots, z_m$ sont linéairement indépendants par rapport à K. Soient $x_1, \dots, x_m$ des éléments ~~de K tels que $\sum_{i=1}^m x_i z_i = 0$~~ non tous nuls de K, et soit x un élément de K tel que $\varphi(x) = \min_{1 \leq i \leq m} \varphi(x_i)$. On a donc $x \neq 0$, $\varphi(x_i^m x^{-1}) \geq 0$. Désignons par ξ_i la classe de $x_i x^{-1}$ modulo p ; par hypothèse, l'un au moins des ξ_i est $\neq 0$, d'où $\sum_{i=1}^m \xi_i \bar{z}_i \neq 0$, et par suite $x^{-1}\sum_{i=1}^m x_i z_i \notin pJ$, ce qui démontre notre assertion et prouve en même temps que si $\sum_{i=1}^m x_i z_i$ ne peut appartenir à J que si $x_1, \dots, x_m$ sont tous dans $\mathfrak{o}$ (car sinon, on aurait $\varphi(x^{-1}) \geq 0$, $x^{-1} \in p\mathfrak{o}$ et $x^{-1}\sum_{i=1}^m x_i z_i \in pJ$).

~~Ceci dit, il existe pour chaque~~ On conclut immédiatement de là que les $\mathfrak{o}_{k-1}/\mathfrak{o}_k$ sont des espaces vectoriels de dimensions finies par rapport à R, donc que chaque $S_{i(k)}$ est algébrique de degré fini par rapport à R. Or, pour chaque i $(1 \leq i \leq h)$, il y a exactement e_i (≥ 1) indices k tels que $i(k) = i$; donc chaque S_i est de degré fini d_i par rapport à R, et on a la formule

$$\sum_{i=1}^{h} d_i e_i = \dim_R J/pJ \leq [L:K].$$

En particulier on a $h \leq [L:K]$. Il ne peut donc pas exister plus de $[L:K]$ valuations normées distinctes de L dont les restrictions à K soient équivalentes à φ, et on peut appliquer le raisonnement précédent en supposant cette fois que $\psi_1, \dots, \psi_h$ sont toutes les valuations normées de L dont les restrictions sont équivalentes à φ. Le théorème est donc démontré.

On peut se demander s'il est possible que le nombre $\sum_{i=1}^{g} d_i e_i$ soit $< [L:K]$; des exemples montrent ~~qu'il est~~ que la réponse à cette question est affirmative. Une valuation φ pour laquelle le nombre $\sum_{i=1}^{g} d_i e_i$ est égal à $[L:K]$ est dite satisfaire à la relation des degrés (par rapport à L)

Proposition

Soient φ une valuation ~~de~~ simple de un corps K, $\mathfrak{o}$ l'anneau de la valuation φ, L une extension algébrique finie de K et J l'anneau des éléments de L entiers par rapport à $\mathfrak{o}$ et $\{y_1, \dots, y_n\}$ une base de L par rapport à K. Pour que φ satisfasse à la relation des degrés par rapport à L, il est nécessaire et suffisant ~~que~~ qu'il existe un élément $c \neq 0$ de K tel que $cJ \subset \mathfrak{o} y_1 + \dots + \mathfrak{o} y_n$

Supposons d'abord que φ satisfasse à la relation des degrés. Utilisant les notations de la démonstration du théorème précédent, observons que l'entier m (égal à la dimension de J/pJ par rapport à R) est égal à $n = [L:K]$, et que les éléments $z_1, \dots, z_n$ sont linéairement indépendants par rapport à K. Tout $z \in J$ peut donc s'écrire sous la forme $\sum_{i=1}^{n} x_i z_i$, $x_i \in K$ $(1 \leq i \leq n)$, et nous avons vu que cela entraîne $x_i \in \mathfrak{o}$ $(1 \leq i \leq n)$; on a donc $J = \mathfrak{o} z_1 + \dots + \mathfrak{o} z_n$. Ecrivons $z_i = \sum_{j=1}^{n} a_{ij} y_j$, $a_{ij} \in K$; il existe alors un $c \neq 0$ de K tel que tous les ca_{ij} soient dans $\mathfrak{o}$, d'où $cJ \subset \sum_{i=1}^{n} \mathfrak{o} y_i$.

Supposons réciproquement la condition satisfaite. Incluons les éléments $z_1, \dots, z_m$ de la démonstration du théorème dans une base $\{z_1, \dots, z_n\}$ de L par rapport à K. Posant $y_i = \sum_{j=1}^{n} b_{ij} z_j$, ~~soit c' un~~ $b_{ij} \in K$, soit c' un élément $\neq 0$ de K tel

que les $c'b_{ij}$ soient tous dans K ; on a alors $c'c\,J \subset \sum_{i=1}^{n} o z_i$. Supposons pour un moment que $m < n$. Il existe évidemment ~~une puit~~ un entier $a > 0$ tel que $p^a z_n = \zeta_1 \in J$. Nous allons construire par récurrence une suite (ζ_k) d'éléments de J. L'élément ζ_1 est déjà construit. Si ζ_k est déterminé, il résulte immédiatement de la manière dont $z_1, \dots, z_m$ ont été définis qu'il existe m éléments $u_{k,1}, \dots, u_{k,m}$ de o tels que $\zeta_k \equiv \sum_{i=1}^{m} u_{ki} z_i \pmod{pJ}$; nous poserons alors $\zeta_{k+1} = p^{-1}(\zeta_k - \sum_{i=1}^{m} u_{ki} z_i)$. Écrivons $\zeta_k = \sum_{i=1}^{n} x_{k,i} z_i$, $x_{k,i} \in K$. ~~On voit alors que~~ Puisque $m < n$, on a évidemment $x_{ki}\, x_{k+1,n} = p^{-1} x_{k,n}$, d'où $x_{k,n} = p^{-k+1} x_{1,n} = p^{a-k+1}$. Par ailleurs on a $c'c\, x_{k,n} \in o$, $c'c \neq 0$, d'où une contradiction puisqu'on devrait avoir $\varphi(c'c) \geqslant (k-a-1)\varphi(p)$ pour tout entier k.

Corollaire. ~~Si φ est une v~~ ~~Si φ est une valuation simple d'un corps K~~ Si L est une extension algébrique séparable ~~d'un corps K~~ de degré fini d'un corps K, toute valuation simple φ de K satisfait à la relation des degrés par rapport à L.

Nous utiliserons les notations de la Proposition . Soit M une extension galoisienne de degré fini de K qui contient L ; il existe alors n isomorphismes distincts $\sigma_1, \dots, \sigma_n$ de L dans M qui coïncident avec l'identité sur K. Soit $y = \sum_{i=1}^{n} x_i y_i$ un élément de J. Il est clair que les éléments ~~$\sigma_j y$ $(1 \leq j \leq n)$~~

$$(1) \qquad \sigma_j y = \sum_{i=1}^{n} x_i (\sigma_j y_i) \qquad (1 \leq j \leq n)$$

sont entiers par rapport à o. Par ailleurs le déterminant D de la matrice $(\sigma_j y_i)$ est $\neq 0$, et la résolution des relations (1) par rapport à $x_1, \dots, x_n$ conduit à des expressions de la forme

$$x_i = \sum_{j=1}^{n} A_{ij}\, \sigma_j y$$

où les A_{ij} sont des éléments de M qui ne dépendent pas de y. Or il est clair que, pour tout $A \in M$, il existe un entier a ~~$\neq 0$~~ tel que $p^a A$ soit entier par rapport à o. Choisissons donc un entier $a \geq 0$ tel que les $p^a A_{ij}$ soient tous entiers par rapport à o. Les $p^a x_i$ seront alors entiers par rapport à o et contenus dans K, donc contenus dans o,

d'où $p^a J \subset o y_1 + \dots + o y_n$.

Remarque 1. Les éléments u_{ij}, v_{ik} ayant été choisis comme indiqué, nous avons en réalité établi que si des éléments x_{ijk} de K sont tels que $\varphi_i(x_{ijk}) \geq 0$ pour tous appartenant tous à l'anneau de φ, on ne peut avoir $\varphi_i(\sum_{jk} x_{ijk} u_j v_{ik}) > \varphi_i(\gamma)$ pour $1 \leq i \leq g$ que si tous les $\varphi(x_{ijk})$ sont > 0. Cette remarque nous sera utile dans la suite.

Remarque 2. Si L est une extension algébrique d'un corps K, la seule valuation de L dont la restriction à K est triviale est elle-même triviale. Soit en effet x un élément de L, zéro d'un polynome $X^n + \sum_{i=1}^{n} a_i X^{n-i}$ à coefficients dans K. On a $\psi(a_i) \geq 0$ $(1 \leq i \leq n)$; si on avait $\psi(x) > 0$, les éléments $\psi(x^n)$, $\psi(a_i x^{n-i})$ seraient tous distincts, ce qui est impossible puisque $x^n + \sum_{i=1}^{n} a_i x^{n-i} = 0$. Donc ψ ne prend que des valeurs ≤ 0, et ψ est triviale.

PSMS 603 46

linéairement indépendants par rapport à K, donc que $\sum_{i=1}^{h} e_i s_i \leq [L:K]$. Les nombres e_i, s_i étant ≥ 1, on a $h \leq [L:K]$, $s_i \leq [L:K]$ $(1 \leq i \leq h)$. Il ne peut donc y avoir plus de $[L:K]$ valuations mutuellement inéquivalentes de L dont les restrictions à K soient équivalentes à φ, et chacune en de degré fini d_i. On peut alors prendre $s_i = d_i$ et supposer que $\psi_1, \ldots, \psi_h$ forment un système maximal de valuations inéquivalentes de L prolongeant φ. Le théorème en est donc démontré.

Théorème

Soient σ un anneau normal, K le corps des quotients de σ et L une extension algébrique de degré fini de K. L'anneau J des éléments de L qui sont entiers par rapport à K est alors un anneau normal. Si σ est un anneau de Dedekind, il en est de même de J.

Soit Φ la famille des valuations normées essentielles de σ, et soit Φ' la famille des valuations de L dont les restrictions à K sont des $\varphi \in \Phi$ équivalentes à des valuations $\varphi \in \Phi$. Il est clair que l'anneau de toute valuation $\varphi' \in \Phi'$ contient J. Soit inversement x un élément de L non contenu dans J, et soit $f(X)$ le polynome minimal de x par rapport à K $= X^n + \sum_{i=1}^{n} a_i X^{n-i}$ le polynome minimal de x par rapport à K. L'un au moins des a_i n'est pas dans σ ; il existe donc une valuation $\varphi \in \Phi$ telle que $\varphi(a_i) < 0$, et x n'est pas entier par rapport à l'anneau de valuation σ' de φ (Prop ,). Il existe donc une valuation φ' non triviale de L telle que $\varphi'(x) \geq 0$ dont l'anneau contient σ mais ne contient pas x. Soit φ_1 la restriction de φ' à σ ; on $\varphi'(x^n) < \varphi'(x^{n-i})$ pour $1 \leq i \leq n$; puisque $x^n + \sum_{i=1}^{n} a_i x^i = 0$, il est impossible que les $\varphi'(x^i)$ soient tous ≥ 0, ce qui montre que φ_1 n'est donc pas triviale. Or σ' est un anneau de Dedekind (Prop ,) ; φ_1 est donc équivalente à φ, et il résulte du théorème que φ' est équivalente à une valuation de l'ensemble Φ'. On voit donc que J est l'intersection des anneaux des valuations de Φ'. Soit y un élément $\neq 0$ de J ; il existe donc une relation de la forme $y^m + \sum_{j=0}^{m} b_j y^{m-j} = 0$ telle que $b_m \neq 0$; si $\varphi' \in \Phi'$, $\varphi'(y) > 0$, on a $\varphi'(b_m) > 0$; or φ' est équivalente à une valuation $\varphi \in \Phi$, et il n'y a qu'un nombre fini de valuations $\varphi \in \Phi$ telles que $\varphi(b_m) > 0$. Pour chacune d'elles il n'y a qu'un nombre fini de $\varphi' \in \Phi'$ dont les restrictions à K lui sont équivalentes. On en conclut qu'il n'y a qu'un nombre fini de

valuations $\varphi' \in \Phi'$ telles que $\varphi'(y) > 0$. L'anneau J est donc normal. Montrons que les valuations de la famille Φ' sont essentielles. Soit φ' l'une d'elles, et soient $\varphi'_1 = \varphi', \dots, \varphi'_g$ les éléments distincts de Φ' dont les restrictions à K sont équivalentes à celle φ de Φ. Il existe, en vertu de la Prop. 13, un élément $u \in L$ tel que $\varphi'_1(u) = -1$, $\varphi'_i(u) = 0$ pour $2 \leqslant i \leqslant g$. Il n'y a qu'un nombre fini de valuations $\psi \in \Phi$ qui possèdent des extensions $\psi' \in \Phi'$ telles que $\psi'(u) \neq 0$; soient $\psi_1, \dots, \psi_k$ ces valuations, et en excluant φ. Soit m un entier $\geqslant 0$ au moins égal à tous les nombres $-\psi'(u)$, $\psi' \in \Phi'$. Il existe alors un $x \in K$ tel que $\varphi(x) = 0$, $\psi_i(x) \geqslant m$ $(1 \leqslant i \leqslant k)$ et $\psi(x) \geqslant 0$ pour toute valuation $\psi \in \Phi$ distincte de $\varphi, \psi_1, \dots, \psi_k$. Si nous posons $v = ux$, on a $\varphi'(v) = -1$, $\psi'(v) \geqslant 0$ pour tout $\psi' \in \Phi'$ distinct de φ'. Si on désigne par $\mathfrak{p}$ l'ensemble des $y \in J$ tels que $\varphi'(y) > 0$, on a $v\mathfrak{p} \subset J$, $v \notin J$, ce qui montre que φ' est essentielle. Supposons maintenant que o soit un anneau de Dedekind. Si θ' est une valuation non triviale de J, la restriction de θ à K est une valuation non triviale de o, donc équivalente à une valuation de la famille Φ, d'où il résulte que θ est équivalente à une valuation de la famille Φ' ; J est donc un anneau de Dedekind.

Soit K une extension de degré fini du corps $\mathbb{Q}$ des nombres rationnels. On appelle <u>entiers</u> les éléments de K qui sont entiers par rapport à l'anneau des entiers rationnels. On a donc le résultat suivant :

<u>Proposition</u>.

<u>Si K est une extension de degré fini du corps $\mathbb{Q}$ des nombres rationnels, les entiers de K forment un anneau de Dedekind.</u>

Soit J cet anneau. A tout idéal premier $\mathfrak{p}$ de J correspond une valuation normée $\varphi_{\mathfrak{p}}$ de K, qu'on appelle la <u>valuation $\mathfrak{p}$-adique</u> de K. Si φ est une valuation quelconque de K, l'anneau de valuation de φ, qui contient nécessairement $\mathbb{Z}$, contient aussi J. On a donc le résultat suivant.

<u>Proposition</u>.

<u>Soient K une extension de degré fini du corps $\mathbb{Q}$ des nombres rationnels, et J l'anneau des entiers de K. Toute valuation non triviale de K est alors équivalente à une valuation $\mathfrak{p}$-adique, $\mathfrak{p}$ étant un idéal premier de J.</u>

Définition.

~~On appelle valuation d'un anneau~~ d'un domaine d'intégrité σ, toute valuation φ du corps des quotients K de σ telle que l'on ait $\varphi(x) \geq 0$ pour tout $x \in \sigma$.

Proposition. Soit φ une application de l'ensemble des éléments $\neq 0$ d'un domaine d'intégrité σ dans un groupe totalement ordonné Γ. ~~Il existe alors une valuation de σ qui prolonge~~ telle que l'on ait $\varphi(xy) = \varphi(x) + \varphi(y)$ (si x, y sont des éléments $\neq 0$ de σ) et $\varphi(x+y) \geq \min\{\varphi(x), \varphi(y)\}$ (si $x, y, x+y$ sont des éléments $\neq 0$ de σ). On peut alors prolonger φ par une valuation de σ.

Soit K le corps des quotients de σ. Il résulte de ..... que l'on peut prolonger φ par un homomorphisme φ_1 du groupe multiplicatif K^* des éléments $\neq 0$ de K dans Γ. Soient x, y des éléments de K^* tels que $x+y \in K^*$. Il existe un $z \in \sigma$, $z \neq 0$ tel que zx, zy soient dans σ. On a $\varphi_1(x+y) = \varphi(xz+yz) - \varphi(z) \geq \min\{\varphi(xz), \varphi(yz)\} - \varphi(z) = \min\{\varphi_1(x) + \varphi(z), \varphi_1(y) + \varphi(z)\} - \varphi(z) = \min\{\varphi_1(x), \varphi_1(y)\}$, ce qui montre que φ_1 est une valuation de K

PSMS 003 49

Proposition

Soient o un ~~anneau~~ domaine d'intégrité, K le corps des quotients de o, et L une extension de K. Supposons que tout élément de K entier par rapport à o y soit contenu. Pour qu'un élément $x \in L$ soit entier par rapport à o, il faut et suffit que x soit algébrique par rapport à K et que le polynome minimal de x par rapport à K soit à coefficients dans o.

La condition énoncée en est évidemment suffisante. Supposant x entier par rapport à o; ~~soit $f(X)$~~ x est donc évidemment algébrique par rapport à K. Désignons par $f(X)$ son polynome minimal par rapport à K. Il existe une extension normale N de degré fini de K contenant x, et on peut écrire $f(X) = \prod_{i=1}^{n} (X - x_i)$, $x_i \in N$. On sait qu'il existe pour chaque i un automorphisme σ_i de N, laissant fixes les éléments de K, tel que $\sigma_i \cdot x = x_i$. Il en résulte que chacun des x_i est entier par rapport à o. Les éléments de N entiers par rapport à o formant un anneau, on voit que les coefficients de f sont entiers par rapport à o. Ces coefficients, étant dans K, appartiennent à o.