Rapport de stage
Initiation à la recherche

Maître de stage : Vincent Cossart
Université de Versailles Saint-Quentin
UFR de mathématiques

Anneaux de Valuations

Lauriane Huguet
Université de Rennes 1

Versailles, le 22 Juin 2012

Table des matières

I. Préliminaires 5
I.A. Rappels 5
I.B. Anneaux de fractions 6
I.C. Extension de corps et Théorie de GALOIS 8
I.D. Extension d'anneau, éléments entiers 11
II. Anneaux de valuation 15
II.A. Généralités 15
II.B. Valuation discrète 33
III. Applications et utilisations de la théorie 36
III.A. Théorème d'Ostrowski - Analyse p-adique 36
III.B. Géométrie algébrique 38

Stage de magistère 1re année (L3), effectué au laboratoire de mathématiques de l'UVSQ, dans l'équipe d'Algèbre et Géométrie,

sous la direction de Vincent Cossart.

Je remercie toute l'équipe pour leur accueil chaleureux.

Je remercie tout particulierement les doctorants Jérémy Berthomieu, Tamara El Bouti, Aurélien Greuet, Cécile Mailler et Daniele Turchetti pour leur soutien et leur bonne humeur.

Merci à Vincent Cossart de m'avoir accordé son temps et m'avoir fait découvrir le monde merveilleux des valuations.

Merci à Jérémy Berthomieu et Théo Pierron pour leur conseils avisés en LaTeX.

Introduction

Le but de ce stage était d'introduire la notion d'anneaux de valuation.

Ce rapport a été rédigé en suivant la logique globale de la section "valuation rings" du chapitre 5, du livre *Introduction to Commutative Algebra* de M.F Atiyah et I.G Macdonald [AM], et en y incorporant la rédaction des exercices se rapportant au chapitre ainsi que des compléments nécessaires à la compréhension.

L'introduction des anneaux de valuation est assez récente puisque qu'elle date du début du XX^{e}s.

Tous les anneaux considérés seront commutatifs et unitaires.

I. Préliminaires

I.A. Rappels

Définition I.1 Un *idéal maximal* $\mathfrak{m}$ d'un anneau commutatif $A \neq (0)$ est un idéal tel qu'il existe exactement deux idéaux qui le contiennent, à savoir lui-même et l'anneau entier.

En d'autres termes, $\mathfrak{m} \neq A$ et $\forall I \subset A$, I idéal de A, si $\mathfrak{m} \subseteq I$ alors $I = A$ ou $I = \mathfrak{m}$.

Définition I.2 Soit A un anneau, A est un *anneau local* s'il admet un unique idéal maximal.

Rappel I.1 *:* Théorème de Krull.

Soit A un anneau non nul, I un idéal de A, $I \neq A$, alors il existe $\mathfrak{m}$ un idéal maximal de A tel que $I \subseteq \mathfrak{m}$.

Définition I.3 Soit A un anneau intègre. On appelle $K = \left\{ \frac{a}{b} \ \middle| a, b \in A \right\}$ le *corps des fractions de* A, parfois noté $\mathrm{Frac}(A)$.

Proposition I.A.1
Soient A un anneau, $A \neq (0)$ et $\mathfrak{m} = \{x \in A \ | x^{-1} \notin A\}$. A est local si, et seulement si, $\mathfrak{m}$ est un idéal de A. Dans ce cas, $\mathfrak{m}$ est l'idéal maximal de A.

Preuve

- Supposons que $\mathfrak{m}$ est un idéal de A.
  Soit I un idéal de A.
  Si I contient un élément inversible de A alors $I = A$.
  Sinon, il ne contient aucun inversible de A donc $I \subset \mathfrak{m}$.
  On en déduit que $\mathfrak{m}$ est l'unique idéal maximal de A et que A est local.

- Supposons maintenant que A est local, d'idéal maximal $\max(A)$.
  $\max(A) \subset \mathfrak{m}$ sinon $\max(A) = A$.
  Si $x \in \mathfrak{m}$, $\langle x \rangle \subset \max(A)$ car $\max(A)$ est l'idéal maximal de A. Donc $x \in \max(A)$ et $\mathfrak{m} \subset \max(A)$.
  On a donc montré que $\max(A) = \mathfrak{m}$ donc $\mathfrak{m}$ est un idéal de A.

□

Rappel I.2 *: Lemme de* Zorn

Si un ensemble ordonné est tel que toute chaîne (sous-ensemble totalement ordonné) possède un majorant, alors il possède un élément maximal.

Rappel I.3 *: Premier théorème d'isomorphisme de Emmy* Noether

Soit $f : A \to A'$ un homomorphisme de groupes, d'anneaux ou de modules, alors $A/\ker f$ est isomorphe à $\operatorname{Im} f$.

I.B. Anneaux de fractions

Définition I.4 Soit $S \subset A$, non vide. On dit que S est une *partie multiplicative de* A si $1 \in S$, $0 \notin S$ et S est stable par multiplication.

Définition I.5 Soient A un anneau et S une partie multiplicative de A. *La localisation de* A *par rapport à la partie multiplicative* S est $S^{-1}A = (A \times S)/\mathcal{R}$ où $(a, s)\mathcal{R}(a', s')$ si, et seulement si, $\exists u \in S$, $u(as' - a's) = 0$.

Proposition I.B.1
$S^{-1}A$ est un anneau.

Preuve
(*cf* : cours de L3)

Définition I.6 Si A est un anneau intègre alors $S = A \setminus \{0\}$ est une partie multiplicative de A et $S^{-1}A$ est le corps de fractions de A.

PROPOSITION I.B.2
Si $\mathfrak{p}$ est un idéal premier de A alors $S = A \setminus \mathfrak{p}$ est multiplicative et on note $A_\mathfrak{p} := S^{-1}A$.

Définition I.7 $A_\mathfrak{p}$ est dit *localisé de A en $\mathfrak{p}$*.

THÉORÈME I.1
Soient A un anneau et $\mathfrak{p}$ un idéal premier de A. $A_\mathfrak{p}$ est un anneau local, d'idéal maximal $\mathfrak{p}A_\mathfrak{p} := \{\frac{a}{s} \mid a \in \mathfrak{p}, s \notin A \setminus \mathfrak{p}\}$.

Preuve
$A_\mathfrak{p} = \{\frac{a}{s},\ \ a \in A,\ \ s \notin A \setminus \mathfrak{p}\}$

Montrons que $\mathfrak{p}A_\mathfrak{p}$ est un idéal de $A_\mathfrak{p}$.

Soient $\frac{a}{s_1}, \frac{b}{s_2} \in \mathfrak{p}A_\mathfrak{p}$ et $\frac{c}{s_3} \in A_\mathfrak{p}$.

$$\frac{a}{s_1} \cdot \frac{c}{s_3} = \frac{ac}{s_1 s_3}$$

Comme $\mathfrak{p}$ est un idéal, $ac \in \mathfrak{p}$ car $a \in \mathfrak{p}$ et $\frac{ac}{s_1 s_3} \in \mathfrak{p}A_\mathfrak{p}$.

$$\frac{a}{s_1} + \frac{b}{s_2} = \frac{as_2 + bs_1}{s_1 s_2}$$

Comme $\mathfrak{p}$ est un idéal et $a, b \in \mathfrak{p}$, $as_2 + bs_1 \in \mathfrak{p}$ donc $\frac{as_2+bs_1}{s_1 s_2} \in \mathfrak{p}A_\mathfrak{p}$.

Donc $\mathfrak{p}A_\mathfrak{p}$ est un idéal de $A_\mathfrak{p}$.

Remarquons que $1 = \frac{1}{1} \notin \mathfrak{p}A_\mathfrak{p}$ donc $\mathfrak{p}A_\mathfrak{p} \neq A_\mathfrak{p}$.

Soit $x = \frac{u}{v} \notin \left\{a \in A_\mathfrak{p} \mid \frac{1}{a} \notin \mathfrak{p}A_\mathfrak{p}\right\}$.
$u \notin \mathfrak{p}$ donc $u \in S$ et $\frac{v}{u} = x^{-1} \in A_\mathfrak{p}$.

Donc $\mathfrak{p}A_\mathfrak{p} = \left\{x \in A_\mathfrak{p} \mid \frac{1}{x} \notin A_\mathfrak{p}\right\}$.

D'après la proposition I.A.1, $A_\mathfrak{p}$ est local, d'idéal maximal $\mathfrak{p}A_\mathfrak{p}$. □

Remarque : Si A est un anneau intègre, $\mathfrak{p} \in \operatorname{Spec} A$, $A \subset K = \operatorname{Frac}(A)$ et $A_\mathfrak{p}$ s'injecte dans K par $\frac{a}{s} \mapsto \frac{a}{s}$.

$$A \subset A_\mathfrak{p} \subset K.$$

THÉORÈME I.2
Les idéaux propres de $\mathfrak{p}A_\mathfrak{p}$ sont de la forme $IA_\mathfrak{p}$ avec I un idéal de A, $I \subseteq \mathfrak{p}$.

Preuve
$IA_\mathfrak{p}$, $I \subset \mathfrak{p}$, est un idéal de $A_\mathfrak{p}$ par les même arguments que précédemment.

Réciproquement, soit J un idéal de $A_\mathfrak{p}$ alors $J \subset \mathfrak{p}A_\mathfrak{p}$. Soit $\varphi : A \mapsto S^{-1}A$ telle que $\varphi(a) = \frac{a}{1}$ pour tout élément a de A.

φ est un morphisme d'anneau (*cf* : cours de L3).

$\varphi^{-1}(J)$ est un idéal de A et $\varphi^{-1}(A) \subset \varphi^{-1}(\mathfrak{p}A_\mathfrak{p}) = \mathfrak{p}$ donc $IA_\mathfrak{p} \subset J$ avec $I = \varphi^{-1}(J)$.

$\forall \frac{a}{s} \in J$, $\frac{1}{s} \in A_\mathfrak{p}$ donc $\frac{a}{1} = \frac{a}{s}\frac{s}{1} \in J$ car J est un idéal de $A_\mathfrak{p}$.

On en déduit que $a \in I$ donc que $\frac{a}{s} \in IA_\mathfrak{p}$.

D'où $J \subset IA_\mathfrak{p}$ et $J = IA_\mathfrak{p}$. □

I.C. Extension de corps et Théorie de GALOIS

Définition I.8 Soient A et B deux anneaux tels que A est un sous-anneau de B. On dit que B est *une extension* de A.

On dit que $x \in B$ est *algébrique sur* A s'il existe $P \in A[X]$ non nul, tel que $P(x) = 0$.

Sinon, on dit que x est *transcendant sur* A.

Définition I.9 Soient A et B deux anneaux tels que A est un sous-anneau de B. On dit que $x \in B$ est *entier sur* A s'il existe $a_0, a_1, \ldots, a_{n-1} \in A$ non nuls, tels que $a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n = 0$.

Remarque : entier ⇒ algébrique. La réciproque est fausse en général, elle est vraie si A est un corps.

Définition I.10 Soient k un corps, k' une extension de k et x un élément de k' algébrique sur k.

On appelle *polynôme minimal de* x un polynôme non nul de $k[X]$ de degré minimal tel que $P(x) = 0$.

Rappel I.4 *:* Un idéal principal est un idéal engendré par un seul élément.

Rappel I.5 *:* Un anneau principal est un anneau dont tous les idéaux sont principaux.

THÉORÈME I.3

Soient k un corps, k' une extension de k et x un élément de k'.

Si x est algébrique sur k de polynôme minimal Π, alors $[k[x] : k] = \deg \Pi$, $k[x]$ est un k-espace vectoriel de dimension $n = \deg P$ et de base $(1, x, \ldots, x^{n-1})$.

De plus, si Ω est un corps algébriquement clos et g un homomorphisme de k dans Ω, alors g peut être étendu à $k[x]$.

Preuve

Soit f_x défini de la manière suivante :

$$\begin{aligned} f_x : k[X] &\to k' \\ e \in k &\mapsto e \\ X &\mapsto x \in k'. \end{aligned}$$

Par définition de f_x, $\operatorname{Im} f_x = k[x]$. D'après le rappel I.3, $k[X]/\ker f_x \simeq \operatorname{Im} f_x$.

$\operatorname{Im} f_x$ est intègre donc $\ker f_x$ est un idéal premier de $k[X]$ qui est principal.

On a alors $\ker f_x = (0)$ ou $\ker f_x = \langle \Pi(X) \rangle$ avec Π un élément irréductible de $k[X]$.

Si $\ker f_x = (0)$ alors f_x est injective, donc $k[X] \simeq k[x]$ et $\forall P \in k[X], P \neq 0$, $P(x) \neq 0$, donc x est transcendant sur k.

Sinon, $\ker f_x = \langle \Pi(X) \rangle$, $\Pi(x) = 0$ donc x est algébrique sur k.

Remarque : Π est le polynôme minimal de x, il est défini à un inversible près.

De plus, $\langle \Pi(X) \rangle$ est un idéal maximal de $k[X]$ donc $k[X]/\ker f_x = k[x]$ est un corps.

$\forall P \in k[X]$, $\exists Q_P, R_P \in k[X]$ tels que :

$$P(X) = Q_P(X) \cdot \Pi(X) + R_P(X) \text{ avec } \deg R_P < \deg \Pi.$$

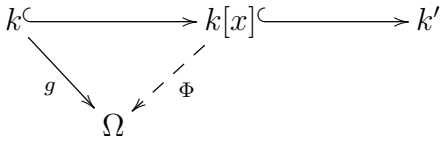
Comme $P(x) = Q_P(x) \cdot \underbrace{\Pi(x)}_{=0} + R_P(x)$, $\forall P \in k[X]$, $f_x(P) = R_P$ et $f_x : k[X] \to k[x]$ est surjective, donc $k[x] = k[x]_{n-1}$ où $n = \deg \Pi$.

On en déduit que $k[x] = \{\alpha_0 + \alpha_1 x + \cdots + \alpha_{x-1} x^{n-1} \mid \alpha_i \in k\}$ donc $k[x]$ est un espace vectoriel et $\{1, x, \ldots, x^{n-1}\}$ est une famille génératrice de $k[x]$.

Si $\{1, x, \ldots, x^{n-1}\}$ est lié, on obtient une relation $D(x) = 0$ de degré strictement plus petit que n avec D un multiple de Π. Donc $D = 0$.

D'où : $k[x]$ est un espace vectoriel de dimension $n = \deg \Pi$ sur k et $\{1, x, \ldots, x^{n-1}\}$ forment une base de $k[x]$.

Soit Ω un corps algébriquement clos. On montre qu'il existe Φ qui prolonge $g : k \to \Omega$ telle que $\Phi : k[x] \to \Omega$.



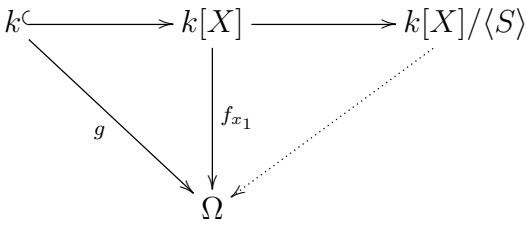
Comme Ω est algébriquement clos, Π a au moins une racine dans Ω.

On choisit n'importe quelle racine de Π dans Ω, on la note x_1.

On définit $f_{x_1} : k[X] \to \Omega$ de la manière suivante :

$$\begin{aligned} f_{x_1} : k[X] &\to \Omega \\ e \in k &\mapsto e \\ X &\mapsto x_1 \in \Omega. \end{aligned}$$

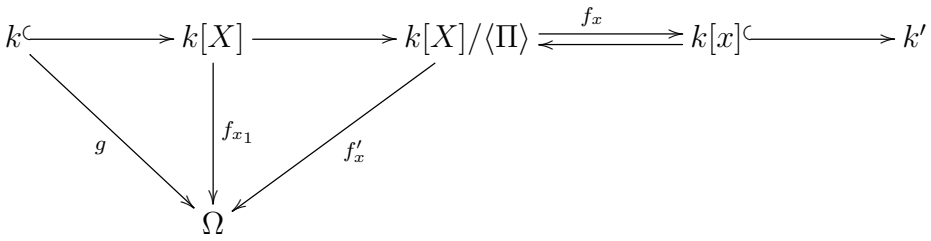
On obtient alors :



Soit $\langle S \rangle = \ker f_{x_1}$, avec S un polynôme irréductible de $k[X]$. On sait que $\ker f_{x_1} \neq (0)$ car il contient Π.

$\langle S \rangle$ est un idéal premier de $k[x]$ contenant $\langle \Pi \rangle$ qui est maximal. Donc $\langle S \rangle = \langle \Pi \rangle$.

Il suffit donc d'envoyer $\overline{X} \in k[X]/\langle \Pi \rangle$ sur $x_1 \in \Omega$ pour définir $f'_x : k[X]/\langle \Pi \rangle \to \Omega$.



Comme f_x est bijective, $f'_x \circ f_x : k[x] \to \Omega$ prolonge g.

□

I.D. Extension d'anneau, éléments entiers

Définition I.11 Soit A un anneau. Un *A-module* $\mathcal{M}$ est un groupe abélien tel que :

$$A \times \mathcal{M} \mapsto \mathcal{M}$$
$$(a, m) \mapsto a \cdot m,$$

avec $\cdot$ distributif par rapport aux additions $+_{\mathcal{M}}$ et $+_A$, associatif et $1_A \cdot m = m$.

Définition I.12 Un A-module de *type fini* est un A-module qui admet un système fini de générateurs.

Définition I.13 Un A-module *fidèle* $\mathcal{M}$ est un A-module tel que :

$$\forall a \in A,\ a\mathcal{M} = \langle 0\rangle \Rightarrow a = 0.$$

Lemme I.D.1 Lemme de Nakayama 1.
Soient A un anneau local d'idéal maximal $\mathfrak{m}$ et M un A-module de type fini.

Si $\mathfrak{m}M = M$, alors $M = (0)$.

Preuve
M est de type fini donc $M = \langle u_1, \ldots, u_n\rangle$ avec n minimal. Supposons $M \neq (0)$, comme $\mathfrak{m}M = M$, il existe $a_1, \ldots, a_n \in \mathfrak{m}$ tels que :

$$u_n = a_1u_1 + \cdots + a_nu_n$$
$$u_n(\underbrace{1 - a_n}_{\notin \mathfrak{m}\ sinon\ 1 \in \mathfrak{m}}) = a_1u_1 + \cdots + a_{n-1}u_{n-1}.$$

Donc $1 - a_n$ est inversible, et :

$$u_n = (1 - a_n)^{-1}(a_1 u_1 + \cdots + a_{n-1} u_{n-1}).$$

Ce qui contredit la minimalité de n donc $M = (0)$.

□

Lemme I.D.2 Lemme de Nakayama 2.
Soient A un anneau local d'idéal maximal $\mathfrak{m}$, M un A-module de type fini, N un sous-module de M.

Si $M = \mathfrak{m}M + N$ alors $M = N$.

Preuve
On a $M/N = \mathfrak{m}M + N/N = \mathfrak{m}(M/N)$. D'après le lemme I.D.1, $M/N = (0)$ donc $M = N$.

□

Lemme I.D.3 Lemme de Nakayama 3.
Soient A un anneau local d'idéal maximal $\mathfrak{m}$ et M un A-module de type fini. Soient $\overline{x_1}, \ldots, \overline{x_n} \in M/\mathfrak{m}M$ des éléments qui engendrent $M/\mathfrak{m}M$ et $N = \langle x_1, \ldots, x_n \rangle$. Alors $N = M$.

Preuve
N est un sous module de M par définition.

Soit $\overline{m} \in M/\mathfrak{m}M$, $\overline{m} = \overline{a_1 x_1} + \cdots + \overline{a_n x_n}$. Donc $m = \underbrace{a_1 x_1 + \cdots + a_n x_n}_{\in N} + \alpha$ où α est un élément de $\mathfrak{m}M$. Donc $M = N + \mathfrak{m}M$ et d'après le lemme I.D.2, $M = N$.

□

Définition I.14 L'ensemble $\overline{A}$ des éléments $x \in B$ entiers sur A est appelé *clôture intégrale* de A dans B.

Si $\bar{A} = A$, on dit que A est intégralement clos.

Si $\bar{A} = B$, on dit que B est entier sur A ou que l'extension $A \subset B$ est entière.

PROPOSITION I.D.1

Les assertions suivantes sont équivalentes :

(i) $x \in B$ est entier sur A ;
(ii) $A[x]$ est un A-module de type fini ;
(iii) $A[x]$ est contenu dans un sous-anneau C de B qui est un A-module de type fini ;
(iv) il existe un $A[x]$-module fidèle M qui est un A-module de type fini.

Preuve

(i) $\Rightarrow$ (ii). Par définition, il existe $a_1, \ldots, a_n \in A$ tels que

$$\Pi(x) = x^n + a_1 x^{n-1} + \cdots + a_n = 0.$$

Soit $P \in A[X]$, comme le coefficient dominant de Π est 1, on peut effectuer la division euclidienne : $P = \Pi Q + R$ avec $\deg R < n$ donc $P(x) = R(x)$ et $A[x] = A1 + Ax + Ax^2 + \cdots + Ax^{n-1}$.

(ii) $\Rightarrow$ (iii). Il suffit de choisir $C = A[x]$.

(iii) $\Rightarrow$ (iv). On prend $C = M$. Soit $y \in A[x]$, $yC = \langle 0 \rangle$ implique $y \cdot 1 = 0$ et donc $y = 0$. C est bien fidèle.

(iv) $\Rightarrow$ (i). Soit $(z_1, \ldots, z_n)$ un système de générateurs du A-module M.

On considère la matrice $\mathcal{M}$ de coefficients a_{ij} donnés par : $xz_i = \sum_{1 \leq j \leq n} a_{ji} z_j$, *i.e.*, $x \cdot m = \mathcal{M}m$, $\mathcal{M}$ est une matrice de l'endomorphisme "multiplication par x" dans le système de générateurs $(z_1, \ldots, z_n)$.

Soit $\chi(X) = \det(\mathcal{M} - XId)$ le polynôme caractéristique de $\mathcal{M}$.

Remarque : Soit $B = \begin{pmatrix} X_{11} & \cdots & X_{1n} \\ \vdots & \ddots & \vdots \\ X_{n1} & \cdots & X_{nn} \end{pmatrix}$. $\Pi(X) = \det(B - XI_n) \in \mathbb{Z}[X_{11}, \ldots, X_{nn}][X]$.
Or $\mathbb{Z}[X_{11}, \ldots, X_{nn}] \subset \mathbb{Q}[X_{11}, \ldots, X_{nn}] \subset \Omega$ où Ω est algébriquement clos, on peut appliquer le théorème de CAYLEY - HAMILTON : $\Pi(B) = 0$.

Par l'application : $\begin{aligned} \mathbb{Z}[X_{11}, \ldots, X_{nn}] &\to A \\ X_{ij} &\mapsto a_{ij} \\ 1 &\mapsto 1_A, \end{aligned}$, on obtient que $\chi(\mathcal{M}) = 0$.

On s'intéresse maintenant à l'endomorphisme « multiplication par $\chi(x)$ ».

Comme $\chi(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1} + (-1)^n x^n$, une matrice de l'endomorphisme est : $c_0 I_n + c_1 \mathcal{M} + \cdots + c_{n-1} \mathcal{M}^{n-1} + (-1)^n \mathcal{M}^n = \chi(\mathcal{M})$.

Or $\chi(\mathcal{M}) = 0$ donc l'endomorphisme de multiplication par $\chi(x)$ est nul, $\chi(x)\mathcal{M} = 0$ mais $\mathcal{M}$ est fidèle donc $\chi(x) = 0$, x est entier sur A.

□

Corollaire I.D.1
Soient $x_i,\ 1 \leq i \leq n$ des éléments de B entiers sur A, alors l'anneau $A[x_1, \ldots, x_n]$ est un A-module de type fini.

Preuve
On fait une récurrence sur n.

- *Initialisation :* Soit $x_1 \in B$, entier sur A, alors il existe un polynôme $P \in A[X]$ de coefficient dominant 1 tel que $P(x_1) = 0$. On a donc $A[x_1] = A[x_1]_{\deg(P)-1}$ et $(1, x_1, \ldots, x_{\deg(P)-1})$ est un système de générateurs de $A[x_1]$ en tant que A-module.
- *Hérédité :* On suppose que $A[x_1, \ldots, x_m]$ est un A-module de type fini.
  Soit $\{e_1, \ldots, e_n\}$ un système de générateurs de $A[x_1, \ldots, x_m]$.
  $A[x_1, \ldots, x_m][x_{m+1}] = \left\{ \sum_{j=0}^{r} \left(\sum_{i=1}^{n} a_{i,j} e_i\right) x_{m+1}^j \;\middle|\; a_{i,j} \in A,\ \ r \in \mathbb{N} \right\}$. Or x_{m+1} est entier sur A, $\beta_0 + \beta_1 x_{m+1} + \cdots + \beta_{p-1} x_{m+1}^{p-1} + x_{m+1}^p = 0$.
  Ainsi toutes les puissances supérieures à p de x_{m+1} s'expriment en fonction des puissances inférieures ou égales à $p-1$ de x_{m+1}.
  Donc $A[x_1, \ldots, x_m][x_{m+1}] = \left\{ \sum_{j=0}^{p-1} \left(\sum_{i=1}^{n} a_{i,j} e_i\right) x_{m+1}^j \;\middle|\; a_{i,j} \in A \right\}$
  et $\left\{ x_{m+1}^i e_j \;\middle|\; 0 \leq i \leq p-1, 1 \leq j \leq n \right\}$ est un système de générateurs de $A[x_1, \ldots, x_m, x_{m+1}]$ qui est donc un A-module de type fini sur A.

□

Corollaire I.D.2
La clôture intégrale de A dans B est un sous-anneau de B.

Preuve
Soit C la clôture intégrale de A dans B. Il suffit de montrer que C est stable pour l'addition et la multiplication. Soient $x, y \in C$, alors le module $A[x, y]$ contient xy et $x + y$. Par la proposition I.D.1(iv) et le corollaire I.D.1, xy et $x + y$ sont entiers sur A. □

Corollaire I.D.3
Soient $A \subset B \subset C$ trois anneaux tels que les extensions $A \subset B$ et $B \subset C$ soient entières, alors l'extension $A \subset C$ est entière.

Preuve
Soit $x \in C$ et soient $a_0, \dots a_{n-1} \in B$ tels que

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0.$$

Alors, par le corollaire I.D.1, l'anneau $B' = A[a_0, \dots, a_{n-1}]$ est un A-module de type fini et $B'[x]$ est aussi un B'-module de type fini. Donc $B'[x]$ est un A-module de type fini. Par la proposition I.D.1(iii), on conclut que x est entier sur A. □

Corollaire I.D.4
Soit $A \subset B$ une extension d'anneaux et soit C la clôture intégrale de A dans B, alors C est intégralement clos dans B.

Preuve
Soit $x \in B$, entier sur C :

$$A \subset C \subset C[x]$$

Or $A \subset C$ est une extension entière et $C \subset C[x]$ est aussi une extension entière, d'après le corollaire I.D.1. D'après le corollaire I.D.3, $A \subset C[x]$ est une extension entière, donc $x \in C$.

Ainsi, si $x \in B$ est entier sur C, alors il est entier sur A, ce qui nous donne par définition de C, $x \in C$ et $C = \overline{C}$.

□

II. Anneaux de valuation

II.A. Généralités

Définition II.1 Soient K un corps et A un sous-anneau de K. A est un *anneau de valuation* de K si $\forall x \in K$, $x \neq 0$, $x \in A$ ou $x^{-1} \in A$.

EXEMPLE

- Soit K un corps, K est un anneau de valuation de K.
- $\mathbb{Z}_p = \left\{ \frac{a}{s} \in \mathbb{Q} \;\middle|\; s \notin p\mathbb{Z} \right\}$, p premier, est un anneau de valuation de $\mathbb{Q}$.

Preuve
Soit $x \in \mathbb{Q}$, $x = \frac{u}{v}$, on choisit u et v premiers entre eux. Si p ne divise pas u, alors $x^{-1} \in \mathbb{Z}_p$. Sinon p ne divise pas v, car u et v sont premiers entre eux, donc $x \in \mathbb{Z}_p$. □

PROPOSITION II.A.1
Un anneau de valuation A est un anneau local.

Preuve
On considère le sous-ensemble $\mathfrak{m}$ de A défini de la manière suivante :

$$\mathfrak{m} = \left\{x \in A, x^{-1} \notin A\right\}.$$

On a *a fortiori* $1 \notin \mathfrak{m}$ donc $\mathfrak{m} \neq A$.

Montrons que $\mathfrak{m}$ est un idéal.

Soient $x \in \mathfrak{m}, y \in A$, $xy \in A$. On suppose que $xy \notin \mathfrak{m}$:

$$\exists u \in A, \quad xyu = 1.$$

Il en découle que $yu = x^{-1} \in A$, ce qui contredit $x \in \mathfrak{m}$.

Soient $x, y \in \mathfrak{m}$. Si x ou y est nul, alors on a évidemment $x + y \in \mathfrak{m}$.

Si x et y sont non nuls alors

$$x + y = y\left(xy^{-1} + 1\right) = x\left(yx^{-1} + 1\right).$$

On vient de montrer que $\mathfrak{m}$ est stable par produit par un élément de A.

De plus, xy^{-1} ou yx^{-1} est dans A, d'où $xy^{-1}+1$ *ou* $yx^{-1}+1 \in A$, donc $x+y \in \mathfrak{m}$.

On a donc montré que si A est un anneau de valuation, alors $\mathfrak{m}$ est un idéal de A. Par la proposition I.A.1, A est local, d'idéal maximal $\mathfrak{m}$.

□

PROPOSITION II.A.2
Soient K un corps et A un anneau de valuation de K. Soit A' un sous-anneau de K tel que :

$$A \subseteq A' \subseteq K,$$

alors A' est un anneau de valuation.

Preuve
$\forall x \in K$, $x \in A$ donc $x \in A'$ ou $x^{-1} \in A$, donc $x^{-1} \in A'$.

□

PROPOSITION II.A.3
Soit A un anneau de valuation, alors A est intégralement clos.

Preuve
Soit $x \in K$ entier sur A.

Si $x \in A$, $x - x = 0$, $n = 1$ et $a_1 = -x$.

Sinon $x^{-1} \in A$ et

$$\begin{aligned} 1 + a_1 x^{-1} + \cdots + a_n x^{-n} &= 0 \\ 1 + x^{-1}\left(a_1 + \cdots + a_n x^{-n+1}\right) &= 0 \\ x^{-1} \cdot \left(-\left(a_1 + \cdots + a_n x^{-n+1}\right)\right) &= 1. \end{aligned}$$

On a donc : $x = -\left(a_1 + \cdots + a_n x^{-n+1}\right) \in A$.

□

Notations : Soient K un corps, Ω un corps algébriquement clos et $\Sigma_{\preceq} = \{(A, f), A \subset K$ un anneau, $f : A \to \Omega$ un homomorphisme $\}$.

On définit une relation d'ordre partielle sur Σ :

$$(A, f) \preceq (A', f') \quad si \quad A \subseteq A' \quad et \quad f'|_A = f.$$

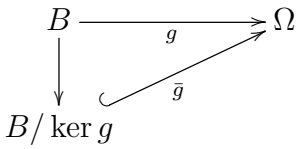
On veut appliquer le lemme de ZORN (le rappel I.2) à $\Sigma_{\preceq}$.

On considère une chaîne de $\Sigma_{\preceq}$. On pose (E, Φ) tel que $E = \bigcup A$ et $\Phi(x) = f_A(x)$ pour A tel que $x \in A$. Alors (E, Φ) est un élément majorant de la chaîne.

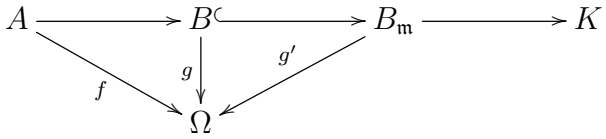
On se retrouve alors dans les conditions d'application du lemme de ZORN (le rappel I.2) donc $\Sigma_{\preceq}$ possède un élément maximal, *que l'on note* (B, g).

LEMME II.A.1
B est un anneau local et $\mathfrak{m} = \ker g$ est son idéal maximal.

Preuve
D'après le rappel I.3 appliqué à $g : B \mapsto \Omega$, on a :



$g(B) = \bar{g}(B/\ker g)$ et $\bar{g}(B/\ker g) \simeq B/\ker g$. $\bar{g}(B/\ker g)$ est un sous-anneau de Ω, donc c'est un anneau intègre. On en déduit que $B/\ker g$ est intègre et donc que $\ker g$ est premier.



où $B_{\mathfrak{m}} = \left\{ \frac{b}{s} \;\middle|\; b, s \in B, s \notin \mathfrak{m} = \ker g \right\}$ et $g'\left(\frac{b}{s}\right) = \frac{g(b)}{g(s)}$. g' est bien définie, *i.e.*, ne dépend pas du représentant choisi.

Donc $(B_{\mathfrak{m}}, g') \in \Sigma$ et (B, g) est un élément maximal de $\Sigma_{\preceq}$, d'où $(B, g) = (B_{\mathfrak{m}}, g')$.

De plus, $B_{\mathfrak{m}} = S^{-1}B$ avec $S = B \setminus \mathfrak{m}$ donc son idéal maximal est

$$\mathfrak{m}B_{\mathfrak{m}} = \mathfrak{m}B = \mathfrak{m}.$$

C'est-à-dire : B est local, d'idéal maximal $\mathfrak{m}$. □

LEMME II.A.2
Soit $x \in K$ un élément non nul. Alors $\mathfrak{m}[x] \neq B[x]$ ou $\mathfrak{m}[x^{-1}] \neq B[x^{-1}]$.

Preuve
On suppose que $\mathfrak{m}[x] = B[x]$ et $\mathfrak{m}[x^{-1}] = B[x^{-1}]$, $\exists \alpha_0, \alpha_1, ..., \alpha_n, \beta_0, \beta_1, ..., \beta_d \in \mathfrak{m}$ tels que :

$$1 = \alpha_0 + \alpha_1 x + \cdots + \alpha_n x^n \tag{0.1}$$

$$1 = \beta_0 + \beta_1 x^{-1} + \cdots + \beta_d x^{-d} \tag{0.2}$$

On choisit n et d minimaux. Comme ils jouent des rôles symétriques, on suppose $n \geq d > 1$. En multipliant (0.2) par x^n, on obtient :

$$x^n = \beta_0 x^n + \beta_1 x^{n-1} + \cdots + \beta_d x^{n-d}$$
$$x^n(1 - \beta_0) = \beta_1 x^{n-1} + \cdots + \beta_d x^{n-d}.$$

Comme $\beta_0 \in \mathfrak{m}$, $1-\beta_0$ est inversible.

$$x^n = (1-\beta_0)^{-1} \cdot \left(\beta_1 x^{n-1} + \cdots + \beta_d x^{n-d}\right)$$

On injecte dans (0.1) :

$$\begin{aligned} 1 =& \alpha_0 + \alpha_1 x + \cdots + \alpha_n (1-\beta_0)^{-1} \left(\beta_1 x^{n-1} + \cdots + \beta_d x^{n-d}\right) \\ 1 =& \alpha_0 + \alpha_1 x + \cdots + \alpha_n (1-\beta_0)^{-1} \beta_d x^{n-d} \\ & + \alpha_n (1-\beta_0)^{-1} \beta_{d-1} x^{n-p+1} + \cdots + \alpha_n (1-\beta_0)^{-1} \beta_1 x^{n-1}. \end{aligned}$$

On obtient donc une nouvelle relation de degré strictement inférieur à n, ce qui contredit la minimalité de n.

On conclut alors que $\mathfrak{m}[x] \neq B[x]$ ou $\mathfrak{m}[x^{-1}] \neq B[x^{-1}]$.

□

THÉORÈME II.1
Soit (B, g) un élément maximal de $\Sigma_{\preceq}$, alors B est un anneau de valuation du corps K.

Preuve
Soit $x \in K$ tel que $x \neq 0$. On veut montrer que $x \in B$ ou $x^{-1} \in B$.

D'après le lemme II.A.2, $\mathfrak{m}[x] \neq B[x]$ ou $\mathfrak{m}[x^{-1}] \neq B[x^{-1}]$ et il est clair que $\mathfrak{m}[x]$ est un idéal de $B[x]$. Comme x et x^{-1} jouent des rôles symétriques, on suppose que $\mathfrak{m}[x] \neq B[x]$.

D'après le rappel I.1, il existe alors $\mathfrak{m}' \subset B[x]$ tel que $\mathfrak{m}'$ est un idéal maximal de $B[x]$ qui contient $\mathfrak{m}[x]$. On a donc :

$$\mathfrak{m}[x] \subset \mathfrak{m}' \subset B[x]$$

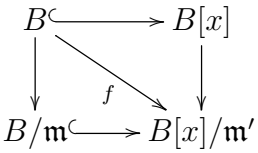
De plus, $\mathfrak{m}' \cap B$ est un idéal de B car c'est l'image réciproque de $\mathfrak{m}'$ par l'injection de B dans $B[x]$. De plus, $\mathfrak{m} \subset \mathfrak{m}[x] \subset \mathfrak{m}'$ et $\mathfrak{m} \subset B$, donc $\mathfrak{m} \subset \mathfrak{m}' \cap B$.

Comme $\mathfrak{m}' \cap B \neq B$ sinon $\mathfrak{m}' = B[x]$, on en déduit que $\mathfrak{m}' \cap B$ est un idéal de B qui contient l'idéal maximal $\mathfrak{m}$ de B, donc $\mathfrak{m}' \cap B = \mathfrak{m}$.

Comme $\mathfrak{m}$ est l'idéal maximal de B et $\mathfrak{m}'$ est un idéal maximal de $B[x]$, il découle que $k := B/\mathfrak{m}$ et $k' := B[x]/\mathfrak{m}'$ sont des corps.

On a $f : B \to B[x]/\mathfrak{m}'$ où f est la composée de l'injection de B dans $B[x]$ et du passage au quotient de $B[x]$ dans $B[x]/\mathfrak{m}'$. Le noyau de f est alors l'ensemble des éléments de B qui sont dans $\mathfrak{m}'$, c'est à dire $B \cap \mathfrak{m}' = \mathfrak{m}$.

D'après le rappel I.3, on a donc une injection de $B/\mathfrak{m}$ dans $B[x]/\mathfrak{m}'$:

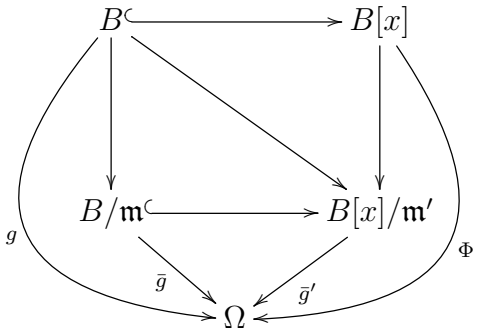


$$\begin{aligned} B[x] &= \{b_0 + b_1 x + \cdots + b_n x^n \mid n \in \mathbb{N}, b_i \in B\} \\ k' = B[x]/\mathfrak{m}' &= \{\overline{b_0} + \overline{b_1}\overline{x} + \cdots + \overline{b_n}\overline{x^n} \mid n \in \mathbb{N}, \ \overline{b_i} \in B/\mathfrak{m}\} \\ &= k[\overline{x}]. \end{aligned}$$

On en déduit que $\bar{x}$ est algébrique sur k : $\exists \beta_1, \beta_2, \ldots, \beta_d \in k$ tels que $P(\bar{x}) = \beta_d + \beta_{d-1}\bar{x} + \cdots + \beta_1 \bar{x}^{d-1} + \bar{x}^d = 0$, donc $k' = k[\bar{x}]$ est une extension de degré $n \leq d-1$ de k, d'après le théorème I.3.

Comme (B, g) est un élément maximal de $\Sigma_{\preceq}$, on a $g : B \mapsto \Omega$ et $\ker g = \mathfrak{m}$ et, par le rappel I.3, on a $\bar{g} : B/\mathfrak{m} \mapsto \Omega$.

De plus, comme Ω est algébriquement clos, P a au moins une racine dans Ω, on étend $\bar{g}$ à $\bar{g}' : B'/\mathfrak{m}' \mapsto \Omega$, tel que $\bar{g}'$ associe $\bar{x}$ à l'une des racines de P dans Ω.



On a donc trouvé $(B[x], \Phi)$ tel que $(B[x], \Phi) \succeq (B, g)$, or (B, g) est un élément maximal de $\Sigma_{\preceq}$ donc $B = B[x]$, d'où $x \in B$ car $x \in B[x]$.

□

Notations : Soit K un corps. Soient A, B deux anneaux locaux de K.

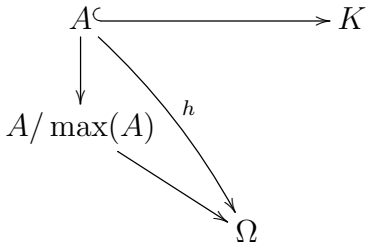
On dit que B domine A, $A \leq_{\text{dom}} B$, si A est un sous-anneau de B et que $\max(A) = \max(B) \cap A$, où $\max(A)$ (resp. $\max(B)$) est l'idéal maximal de A (resp. B).

La relation de domination, $\leq_{\text{dom}}$, est une relation d'ordre sur
$\Sigma_{\leq_{\text{dom}}} = \{A,\ A \text{ sous-anneau local de } K\}$.

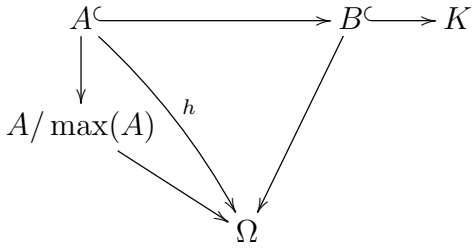
Corollaire II.A.1
Soit K un corps et A un sous-anneau local de K, alors il existe V, un anneau de valuation de K, qui domine A.

$$A \hookrightarrow V \hookrightarrow K$$

Preuve
Soit Ω la clôture algébrique de $A/\max(A)$. Comme A est un sous-anneau de K, on a :



Soit $h : A \to \Omega$. On a donc un couple $(A, h) \in \Sigma_{\preceq}$. Il existe alors un élément maximal $(B, g) \in \Sigma_{\preceq}$ avec $(A, f) \preceq (B, g)$. Par le théorème II.1, B est un anneau de valuation et A est un sous-anneau de B.



$\max(A) = \ker h \subset \max(B) \cap A$ donc $\max(A) = \max(B) \cap A$. B domine A. □

Corollaire II.A.2
★ Exercice 27, chapitre 5, [AM].

A est un élément maximal de $\Sigma_{\leq_{\text{dom}}}$ pour $\leq_{\text{dom}}$ si, et seulement si, A est un anneau de valuation de K.

Preuve
1^{re} *étape* : On veut appliquer le lemme de Zorn (*cf* : le rappel I.2).

Soit Φ une chaîne de $\Sigma_{\leq_{\text{dom}}}$. Soit $B = \bigcup_{A\in\Phi} A$, on montre que B est un majorant de Φ.

Soient $x, y \in B$, $\exists A_1, A_2 \in \Phi$ tels que $x \in A_1$, $y \in A_2$. Comme Φ est une chaîne, $A_1 \leq_{\text{dom}} A_2$ ou $A_2 \leq_{\text{dom}} A_1$, donc $x \in A_2$ et $xy \in A_2$, *i.e.*, $x + y \in A_2$ ou $y \in A_1$, donc $xy \in A_1$ et $x + y \in A_1$.

On a donc $xy, x+y \in B$, B est un sous-anneau de K qui contient tous les éléments de Φ.

On pose $\mathfrak{m}_B = \bigcup_{A\in\Phi} \mathfrak{m}_A$ où $\mathfrak{m}_A$ est l'idéal maximal de A.

Soient $x \in B$, $y \in \mathfrak{m}_B$, $\exists A_1 \in \Phi$ tel que $y \in \mathfrak{m}_{A_1}$, $\exists A_2$ tel que $x \in A_2$.

Si $A_1 \leq_{\text{dom}} A_2$, alors $y \in \mathfrak{m}_{A_2}$, donc $xy \in \mathfrak{m}_{A_2}$, $xy \in \mathfrak{m}_B$.

Si $A_2 \leq_{\text{dom}} A_1$, $x \in A_1$ $xy \in \mathfrak{m}_{A_1}$, $xy \in \mathfrak{m}_B$.

Soient $x, y \in \mathfrak{m}_B$, $\exists A_1, A_2 \in \Phi$ tel que $y \in \mathfrak{m}_{A_1}$, $x \in \mathfrak{m}_{A_2}$.

Si $A_1 \leq_{\text{dom}} A_2$, alors $y \in \mathfrak{m}_{A_2}$, donc $x + y \in \mathfrak{m}_{A_2}$, $x + y \in \mathfrak{m}_B$.

Si $A_2 \leq_{\text{dom}} A_1$, $x \in m_{A_1}$, $x + y \in \mathfrak{m}_{A_1}$, $x + y \in \mathfrak{m}_B$.

$\mathfrak{m}_B$ est un idéal de B.

Soit $x \in B \setminus \mathfrak{m}_B$, $\exists A \in \Phi$ tel que $x \in A$.

Si x n'est pas inversible dans B, alors x n'est pas inversible dans A, donc $x \in \mathfrak{m}_A$ et on en déduit que $x \in \mathfrak{m}_B$, ce qui contredit $x \in B \setminus \mathfrak{m}_B$. On en déduit que x est inversible dans B. Donc $\mathfrak{m} = \{x \in B \mid x^{-1} \notin B\}$.

Réciproquement, si $x \in \mathfrak{m}_B$ et x inversible dans B, alors il existe $A_1, A_2 \in \Phi$ tels que $x \in \mathfrak{m}_{A_1}$, $x^{-1} \in \mathfrak{m}_{A_2}$. Comme Φ est une chaîne, $A_1 \preceq A_2$ ou $A_2 \preceq A_1$.

Par la proposition I.A.1, B est un anneau local, d'idéal maximal $\mathfrak{m}_B$ et B est un majorant de Φ. On peut alors appliquer le Lemme de Zorn (le rappel I.2), $\Sigma_{\leq_{\text{dom}}}$ admet un élément maximal.

2^{e} *étape :* On montre l'équivalence A anneau de valuation de K si, et seulement si, A est un élément maximal de $\Sigma_{\leq_{\text{dom}}}$.

$\Leftarrow$) Soit A un élément maximal de $\Sigma_{\leq_{\text{dom}}}$. A est un sous-anneau local de K, par le corollaire II.A.1, il existe V un anneau de valuation de K qui le domine. Or A est maximal, donc $V = A$. A est un anneau de valuation.

$\Rightarrow$) Soit V un anneau de valuation de K.

Si V n'est pas un élément maximal de $\Sigma_{\leq \text{dom}}$, alors il existe $B \in \Sigma_{\leq \text{dom}}$ maximal tel que $V \subseteq B \subseteq K$.

$\forall x \in K$:
Soit $x \in V$, alors $x \in B$.

Soit $x \notin V$, alors $x^{-1} \in V$, car V est un anneau de valuation et x^{-1} est non inversible dans V, donc $x^{-1} \in \mathfrak{m}_V$. Comme $\mathfrak{m}_V = V \cap \mathfrak{m}_B$, $x^{-1} \in \mathfrak{m}_B$, c'est à dire, x^{-1} est non inversible dans B, donc $x \notin B$.

On vient de montrer que $V = B$, donc V est un élément maximal de $\Sigma_{\leq \text{dom}}$.

□

Corollaire II.A.3
Soient V un anneau de valuation de K et K' une extension de K. Il existe V' anneau de valuation de K' qui domine V.

De plus $V' \cap K = V$, $\mathfrak{m}_{V'} \cap K = \mathfrak{m}_V$.

Preuve
V est un anneau local, sous-anneau de K', donc il existe un élément V', sous-anneau de K', maximal pour $\leq_{\text{dom}}$ qui le domine. Par le corollaire II.A.2, V' est un anneau de valuation de K'.

$$\begin{array}{ccc} V & \longrightarrow & K \\ \downarrow & & \downarrow \\ V' & \longrightarrow & K' \end{array}$$

Comme V' domine V, $\mathfrak{m}_V = \mathfrak{m}_{V'} \cap V$. Soit $a \in K \cap V'$, $w(a) \geq 0$.

- 1^{er} *cas :* $a \in \mathfrak{m}_{V'} \cap K$.
  Si $a \notin V$, comme V est un anneau de valuation de K, $a^{-1} \in \mathfrak{m}_V$, donc $a^{-1} \in \mathfrak{m}_{V'} \subset V'$. On en déduit que a est inversible dans V', ce qui contredit $a \in \mathfrak{m}_{V'}$, et donc que $a \in V$ et $a \in V \cap \mathfrak{m}_{V'}$, donc $a \in \mathfrak{m}_V$.
- 2^{e} *cas :* $a \in K$, a inversible dans V'.
  Si $a \notin V$, $a^{-1} \in \mathfrak{m}_V$, donc $a^{-1} \in \mathfrak{m}_{V'}$, ce qui contredit $a \in V'$. Donc $a \in V$.
  On a donc montré que si $a \in K \cap V'$, alors $a \in V$. Réciproquement, si $a \in V$, alors $a \in V'$, donc $a \in K \cap V'$.

□

Corollaire II.A.4

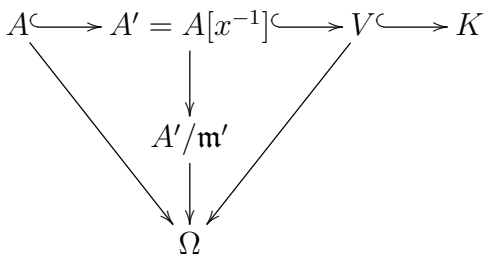
Soient A un sous-anneau d'un corps K. La clôture intégrale $\overline{A}$ de A dans K est l'intersection de tous les anneaux de valuations de K contenant A.

Preuve

Soit V un anneau de valuation qui contient A. Comme V est intégralement clos, $\bar{A} \subset V$. On a donc $\bar{A} \subset \bigcap_{A \subset V} V$, où tous les V sont des anneaux de valuations.

Pour montrer l'inclusion réciproque, on montre par contraposée que si $x \notin \overline{A}$, alors il existe un anneau de valuation V tel que $x \notin V$.

Soit $x \notin \bar{A}$, alors $x \notin A' := A[x^{-1}]$, sinon $x = \alpha_0 + \alpha_1 x^{-1} + \cdots + \alpha_d x^{-d}$, donc $x^{d+1} = \alpha_0 x^d + \alpha_1 x^{d-1} + \cdots + \alpha_d$ ce qui contredirait $x \notin \bar{A}$. On a donc x^{-1} non inversible dans A', donc $x^{-1} \in \mathfrak{m}'$, l'idéal maximal de A'. De plus, par le corollaire II.A.1, il existe V un anneau de valuation de K qui contient A', d'où :



On a donc $x^{-1} \mapsto 0$ dans Ω car $x^{-1} \in \mathfrak{m}'$. Si $x \in V$, alors
$1 = g(x \cdot x^{-1}) = g(x) \cdot g(x^{-1}) = 0$: contradiction.

On a donc $x \notin V$.

□

Proposition II.A.4

★ Exercice 28, chapitre 5, [AM].

Soient A un anneau intègre et K son corps de fractions. Les assertions suivantes sont équivalentes :

(i) A est un anneau de valuation de K ;

(ii) Si I et J sont deux idéaux de A, alors $I \subseteq J$ ou $J \subseteq I$.

Preuve

(i) $\Rightarrow$ (ii) A est un anneau de valuation de K.

$\forall x \in K$, $x \in A$ ou $x^{-1} \in A$.
Supposons $I \nsubseteq J$. $\exists y \in I$, $y \notin J$. Soit $x \in J$. Comme A est un anneau de valuation, $\frac{x}{y} \in A$ ou $\frac{y}{x} \in A$.
Or, $\frac{y}{x} \notin A$, sinon $y = \frac{y}{x} \cdot x \in I$. Donc $\frac{x}{y} \in A$ et $x = \frac{x}{y} \cdot y \in I$.
On en déduit donc que $J \subseteq I$.

(ii) $\Rightarrow$ (i) Les idéaux de A sont totalement ordonnés pour l'inclusion.
Soit $x \in K$, $\exists u, v \in A$ tel que $x = \frac{u}{v}$.
Si $\langle u \rangle \subseteq \langle v \rangle$, alors $\exists y \in A$ tel que $u = vy$. On a alors $x = y \in A$.
Sinon, $\langle v \rangle \subseteq \langle u \rangle$, alors $\exists y \in A$ tel que $v = uy$. On a alors $x^{-1} = y \in A$.
A est un anneau de valuation.

□

EXEMPLE
Soient A un anneau de valuation et $\mathfrak{p}$ un idéal premier de A.

♮ D'après le théorème I.2, la propriété (ii) est vérifiée dans $A_{\mathfrak{p}}$, donc $A_{\mathfrak{p}}$ est un anneau de valuation.

Rappel II.1 *:* Il existe une bijection entre les idéaux de A qui contiennent $\mathfrak{p}$ et les idéaux de $A/\mathfrak{p}$:

$$\begin{array}{c} \text{Idéaux de } A \text{ qui contiennent } \mathfrak{p} \leftrightarrow \text{idéaux de } A/\mathfrak{p} \\ \mathfrak{p} \subset I \rightleftarrows I/\mathfrak{p}. \end{array}$$

♮ Les idéaux de $A/\mathfrak{p}$ sont donc totalement ordonnés pour l'inclusion et $A/\mathfrak{p}$ est un anneau de valuation de son corps de fractions.

PROPOSITION II.A.5
★ Exercice 29, chapitre 5, [AM].

Soit A un anneau de valuation d'un corps K. Alors tout sous-anneau de K qui contient A est de la forme $A_{\mathfrak{p}}$, où $\mathfrak{p}$ est un idéal premier de A.

Preuve
Tout sous-anneau de K de la forme $A_{\mathfrak{p}}$ est un sous-anneau de K qui contient A, c'est un anneau de valuation.

Soit B un sous-anneau de K qui contient A, $A \subseteq B \subseteq K$, donc B est un anneau de valuation, d'après la proposition II.A.2.

On pose $\mathfrak{p} = \mathfrak{m}_B \cap A$. $\mathfrak{p}$ est premier car c'est l'image réciproque de $\mathfrak{m}_B$ qui est un idéal maximal. On a alors $\mathfrak{p} \subseteq A_{\mathfrak{p}} \cap \mathfrak{m}_B$.

Soit $s \in A \setminus \mathfrak{p}$, alors $s \notin \mathfrak{m}_B$ et s est inversible dans B, *i.e.*, $\frac{1}{s} \in B$.

On en déduit, $\forall a \in A$, $\frac{a}{s} \in B$, donc $A_\mathfrak{p} \subset B$.

D'où $A \subseteq A_\mathfrak{p} \subseteq B$ et $\mathfrak{p}A_\mathfrak{p} \subseteq A_\mathfrak{p} \cap \mathfrak{m}_B$.

Or, d'après le théorème I.1, $\mathfrak{p}A_\mathfrak{p}$ est l'idéal maximal de $A_\mathfrak{p}$.

Comme $1 \notin \mathfrak{m}_B$, $1 \notin A_\mathfrak{p} \cap \mathfrak{m}_B$, donc $A_\mathfrak{p} \cap \mathfrak{m}_B$ est un idéal propre de $A_\mathfrak{p}$.

De plus $A_\mathfrak{p} \cap \mathfrak{m}_B$, contient l'idéal maximal, donc $\mathfrak{p}A_\mathfrak{p} = A_\mathfrak{p} \cap \mathfrak{m}_B$.

On en déduit que $A_\mathfrak{p} \leq_{\text{dom}} B$. Comme $A_\mathfrak{p}$ est un anneau de valuation, d'après le corollaire II.A.2, il est maximal pour $\leq_{\text{dom}}$ dans l'ensemble des sous-anneaux locaux de K, donc $B = A_\mathfrak{p}$.

□

PROPOSITION II.A.6
★ Exercice 30, chapitre 5, [AM].

Soit A un anneau de valuation d'un corps K. Soit U l'ensemble des inversibles de A qui est un sous-groupe du groupe multiplicatif K^* de K. Soit $\Gamma = K^*/U$.

Si $\xi, \eta \in \Gamma$ sont représentés par $x, y \in K$, on dit que $\xi \geq \eta$ si $xy^{-1} \in A$. Comme A est un anneau de valuation, cette relation est une relation d'ordre totale sur Γ et est compatible avec la structure de groupe ($\forall \omega \in \Gamma$, $\xi \geq \eta \Rightarrow \xi\ \omega \geq \eta\ \omega$).

Soit $v : K^* \mapsto \Gamma$ l'homomorphisme canonique.

Alors $\forall x, y \in K^*$, $v(x+y) \geq \min(v(x), v(y))$.

Preuve
Montrons que $\geq$ est un ordre total sur Γ compatible avec la structure de groupe.

- Montrons que $\geq$ ne dépend pas du représentant choisi. Soient $\xi, \eta \in \Gamma$, $x, x' \in \xi$, et $y, y' \in \eta$, on suppose $xy^{-1} \in A$.
  Comme $x, x' \in \xi$, et $y, y' \in \eta$, on a, $x'x^{-1} \in U$ et $yy'^{-1} \in U$. On en déduit que $x'y'^{-1} = x'(x^{-1}x)(y^{-1}y)y'^{-1} = \underbrace{(x'x^{-1})}_{\in A}\underbrace{xy^{-1}}_{\in A}\underbrace{(yy'^{-1})}_{\in A}$. Donc $x'y'^{-1} \in A$, et l'ordre $\geq$ ne dépend pas du représentant choisi.

- Il est évident que l'ordre $\geq$ est réflexif, transitif et antisymétrique.

- Montrons que $\geq$ est total. Soient $\xi = \bar{x}$ et $\eta = \bar{y}$. Comme A est un anneau de valuation, xy^{-1} ou $x^{-1}y \in A$, *i.e.*, $\xi \geq \eta$ ou $\eta \geq \xi$.

- Montrons que $\geq$ est compatible avec la structure de groupe. Soient $\xi = \bar{x}$, $\eta = \bar{y}$ et $\omega = \bar{z}$. Si $\eta \geq \xi$, alors $yx^{-1} \in A$.
  On a alors $xz(yz)^{-1} = x(zz^{-1})y^{-1} = yx^{-1} \in A$, donc $\eta\omega \geq \xi\omega$.

Comme x et y jouent des rôles symétriques, on suppose $v(x) \geq v(y)$, donc $xy^{-1} \in A$ et $\min(v(x), v(y)) = v(y)$.

On a alors

$$(x+y)\,y^{-1} = \underbrace{xy^{-1}}_{\in A} + \underbrace{1}_{\in A} \in A, \text{ donc } v(x+y) \geq v(y)$$

i.e., $v(x+y) \geq \min(v(x), v(y))$.

□

Définition II.2 Le groupe Γ ainsi défini est appelé le *groupe des valeurs* de A.

En général, la loi est notée $+$.

Corollaire II.A.5
★ Exercice 31, chapitre 5, [AM].

Soient Γ un groupe abélien totalement ordonné et K un corps. Une valuation de K à valeurs dans Γ est une application $v : K^* \mapsto \Gamma$ telle que, $\forall x, y \in K^*$:

1. $v(xy) = v(x) + v(y)$.
2. $v(x+y) \geq \min(v(x), v(y))$.

Alors $V = \{x \in K^* \mid v(x) \geq 0\}$ est un anneau de valuation de K.

Preuve
Soit $x \in K$. Si $x \in V$, alors il n'y a rien à montrer. Sinon, $v(x) < 0$,
$v(xx^{-1}) = v(x) + v(x^{-1}) = v(1)$, donc $v(x^{-1}) = 1 - v(x)$.

De plus, $v(x) = v(1 \cdot x) = v(x) + v(1)$, donc $v(1) = 0$. On a donc $v(x^{-1}) > 0$, donc $x^{-1} \in V$. Donc V est un anneau de valuation, d'idéal maximal
$\mathfrak{m} = \{x \in K^* \mid v(x) > 0\}$.

□

Définition II.3 L'anneau V ainsi défini est appelé *anneau de valuation* de v.

Par le corollaire II.A.5 et la proposition II.A.6, il y a équivalence entre les définitions II.1 et II.3 d'un anneau de valuation.

Remarque : Ainsi, le corollaire II.A.3 s'interprète de la manière suivante :

Soient V un anneau de valuation définie par une valuation $v : K \to \Gamma \cup \infty$ où $K = \mathrm{Frac}(V)$, K' une extension de K, alors il existe w, une valuation de K', $w : K' \to \Gamma' \cup \infty$ telle que $w|_K = v$.

On verra plus tard l'exemple de M. Spivakovsky (III.B).

Définition II.4 Soient A un anneau intègre et Γ un groupe totalement ordonné.

On appelle valuation de A à valeurs dans Γ, une application $v : \mathrm{Frac}(A) \mapsto \Gamma \cup \{\infty\}$ telle que v vérifie les conditions 1 et 2 dans le corollaire II.A.5 et $v(0) = +\infty$.

Par convention, $\forall a \in \Gamma$, $a + (+\infty) = (+\infty) + (+\infty) = +\infty$.

Définition II.5 Le corps $\mathcal{K}_V = V/\max(V)$ est le corps résiduel de la valuation v où $V = v^{-1}(\Gamma^+)$.

EXEMPLE

♮ $v_p : \mathbb{Q} \mapsto \mathbb{Z}$ telle que $v_p(\frac{a}{b}) = v_p(a) - v_p(b)$ et, si $a \in \mathbb{Z}$, $v_p(a)$ est l'exposant associé à p dans la décomposition de a en facteurs premiers.
v_p est la valuation p-adique de $\mathbb{Q}$.
$\mathbb{Z}_p$ est l'anneau de valuation de v_p.
$\mathbb{Z}$ est le groupe de valeurs de $\mathbb{Z}_p$.
$\mathbb{Z}/p\mathbb{Z}$ est le corps résiduel de v_p.

Proposition II.A.7
Soit v une valuation d'un anneau A, pour tout $(a_1, \ldots, a_d) \in A$,
$v\left(\sum_{i=1}^d a_i\right) \geq \inf\{v(a_i) \mid 1 \leq i \leq d\}$. De plus, s'il existe $k \in \{1, \ldots, d\}$ tel que $\forall i \neq k$, $v(x_i) > v(x_k)$, alors il y a égalité dans l'inégalité précédente.

Preuve
Comme v est une valuation, $v(x+y) \geq \inf(v(x), v(y))$. On suppose par récurrence que pour toute famille de cardinal $m \geq n$, on a $v\left(\sum_{i=1}^m a_i\right) \geq \inf_{1 \leq i \leq m}(v(a_i))$.

Au rang $n+1$:

$$\begin{aligned} v\left(\sum_{i=1}^{n+1} a_i\right) = v\left(a_{n+1} + \sum_{i=1}^{n} a_i\right) &\geq \inf\left(v(a_{n+1}), v\left(\sum_{i=1}^{n} a_i\right)\right) \\ &\geq \inf\left(v(a_{n+1}), \inf_{1 \leq i \leq n}(v(a_i))\right) \\ &\geq \inf\{v(a_i) \mid 1 \leq i \leq n+1\}. \end{aligned}$$

On se ramène au cas $n = 2$: $v(x) < v(y)$, $v(x+y) \geq v(x)$.

De plus

$$v(x) = v((x+y)+(-y)) \geq \inf(v(x+y), v(-y))$$

et

$$v(y) = v(-y)$$

car $v((-1)(-1)) = v(-1) + v(-1) = v(1) = 0$

donc $v(-1) = 0$ et $v(-y) = v(-1) + v(y) = v(y)$.

$$v(x+y) \geq v(x) \geq \inf(v(x+y), v(y))$$

or, si $\inf(v(x+y), v(y)) = v(y)$, on obtient une contradiction avec $v(x) > v(y)$.

Donc $\inf(v(x+y), v(y)) = v(x+y)$ et $v(x) = v(x+y)$.

Par récurrence, on obtient l'égalité voulue.

□

Définition II.6 Soient Γ un groupe abélien totalement ordonné et Δ un sous-groupe de Γ. Δ est *isolé* si, quels que soient $0 \leq \beta \leq \alpha$ avec $\alpha \in \Delta$, on a $\beta \in \Delta$.

Corollaire II.A.6
★ Exercice 32, chapitre 5, [AM].

Soit Γ un groupe abélien totalement ordonné. Soit A un anneau de valuation d'un corps K dont Γ est le groupe des valeurs.

Si $\mathfrak{p}$ est un idéal premier de A, alors $v(A \setminus \mathfrak{p})$ est l'ensemble des éléments positifs dans un sous-groupe isolé Δ de Γ. L'application de $\mathrm{Spec}(A)$ dans l'ensemble des sous-groupes isolés de Γ est une bijection.

Preuve
On montre que $\langle v(A \setminus \mathfrak{p})\rangle = v(A \setminus \mathfrak{p}) \cup -v(A \setminus \mathfrak{p})$.

Si $x \in v(A \setminus \mathfrak{p})$, $-x = -v(a) \in -v(A \setminus \mathfrak{p})$ donc $-v(A \setminus \mathfrak{p}) \subset \langle v(A \setminus \mathfrak{p})\rangle$.

Soient $x, y \in v(A \setminus \mathfrak{p}) \cup -v(A \setminus \mathfrak{p})$, $x = v(a)$, $y = v(b)$, a ou a^{-1}, b ou $b^{-1} \in A \setminus \mathfrak{p}$.
$x + y = v(a) + v(b) = v(ab)$. Trois cas possibles :
1$^{\text{e}}$cas : $a, b \in A \setminus \mathfrak{p}$ $ab \in A$ et $ab \notin \mathfrak{p}$ car $\mathfrak{p}$ est premier.
2$^{\text{e}}$cas : $a^{-1}, b^{-1} \in A \setminus \mathfrak{p}$ et $a^{-1}b^{-1} \in A \setminus \mathfrak{p}$ car $\mathfrak{p}$ est premier.
3$^{\text{e}}$cas : $a^{-1}, b \in A \setminus \mathfrak{p}$ ou $b^{-1}, a \in A \setminus \mathfrak{p}$. Les deux possibilités étant symétriques, prenons $a^{-1}, b \in A \setminus \mathfrak{p}$ et $a^{-1}b \in A \setminus \mathfrak{p}$ car $\mathfrak{p}$ est premier.

$x + y = v(a) + v(b) = v(ab)$.
Comme A est un anneau de valuation : ab ou $a^{-1}b^{-1} \in A$.
Si $ab \in A$ et $ab \in \mathfrak{p}$ alors $aba^{-1} = b \in \mathfrak{p}$ car $a^{-1} \in A$ et $\mathfrak{p}$ est un idéal de A, ce qui est impossible par hypothèse.
Si $a^{-1}b^{-1} \in A$ et $a^{-1}b^{-1} \in \mathfrak{p}$ alors $a^{-1} = a^{-1}b^{-1}b \in \mathfrak{p}$ car $b \in A$ et $\mathfrak{p}$ est un idéal de A.

On a donc montré que $\Delta' := v(A \setminus \mathfrak{p}) \cup -v(A \setminus \mathfrak{p})$ est un sous-groupe tel que :

$$v(A \setminus \mathfrak{p}) \subset \Delta' \subset \langle v(A \setminus \mathfrak{p}) \rangle,$$

d'où l'égalité annoncée.

On suppose que Δ' n'est pas isolé.

Il existe $y \in A \setminus \mathfrak{p}$ et $x \in \mathfrak{p}$ tels que $0 \leq v(x) \leq v(y)$, *i.e*, $yx^{-1} \in A$.

Comme $\mathfrak{p}$ est un idéal de A, $\underbrace{x}_{\in \mathfrak{p}} \underbrace{(yx^{-1})}_{\in A} = y \in \mathfrak{p}$, ce qui contredit l'hypothèse $y \in A \setminus \mathfrak{p}$.

$\langle v(A \setminus \mathfrak{p}) \rangle$ est donc isolé.

Soient Δ un sous-groupe isolé de Γ et $\mathfrak{p} = \{a \in A | v(a) \notin \Delta\}$.

Soient $x \in \mathfrak{p}$, $y \in A$. Comme Δ est isolé, $\forall e \in \Delta$, $v(x) > e$, sinon $0 \leq v(x) \leq e$ et $v(x) \in \Delta$, ce qui contredirait $x \in \mathfrak{p}$.

On a $v(y) \geq 0$.

$$v(xy) = v(x) + v(y) \geq v(x)$$

$$\forall e \in \Delta,\ v(xy) \geq v(x) > e,\ v(xy) \notin \Delta,\ xy \in \mathfrak{p}.$$

Soient $x, y \in \mathfrak{p}$

$$v(x + y) \geq \min(v(x), v(y))$$

$$\forall e \in \Delta,\ v(x) > e,\ v(y) > e, \text{ donc } v(x + y) > e \text{ et } v(x + y) \notin \Delta,\ x + y \in \mathfrak{p}.$$

Donc $\mathfrak{p}$ est un idéal.

En outre, $\Delta = \langle v(A \setminus \mathfrak{p}) \rangle$ est un sous-groupe de Γ, donc Δ est stable par addition. Il en découle que $A \setminus \mathfrak{p}$ est stable par multiplication et donc que $\mathfrak{p}$ est premier.

Spec(A)	{ sous-groupes isolés de Γ}
$\mathfrak{p}$	$\langle v(A \setminus \mathfrak{p}) \rangle$
$\{a \in A \mid v(a) \notin \Delta\}$	Δ

La bijection est décroissante. □

EXEMPLE
Soient A un anneau de valuation du corps K et $\mathfrak{p}$ un idéal premier de A.

- Le groupe des valeurs de $A/\mathfrak{p}$ est $\Delta = v(A \setminus \mathfrak{p})$.
  Les éléments de $\mathfrak{p}$ dans A constituent la classe de 0 dans $A/\mathfrak{p}$, donc $v(A/\mathfrak{p}) = \Delta$.
- Le groupe des valeurs de $A_{\mathfrak{p}}$ est Γ/Δ.

Remarque : Soient A un anneau intègre et $K = \mathrm{Frac}(A)$. La valuation $v : A \to \Gamma$ se prolonge de manière unique en une valuation de K par $v(\frac{a}{b}) = v(a) - v(b)$.

Preuve
Soit $x \in K$, $x = \frac{a}{b}, a \in A,\ b \in A \setminus \{0\}$. On pose $v'(x) = v(a) - v(b)$.

Cette définition ne dépend pas du représentant choisi pour x.

$$x = \frac{a}{b} = \frac{c}{d}$$

$$ab^{-1}dc^{-1} = 1$$

donc

$$\begin{aligned} v(ab^{-1}dc^{-1}) &= v(a) + v(d) + v(b^{-1}) + v(c^{-1}) \\ &= v(a) - v(b) + v(d) - v(c) \\ &= 0 \\ v(a) - v(b) &= v(c) - v(d), \end{aligned}$$

$$\begin{aligned} v\left(\frac{a}{b} \cdot \frac{c}{d}\right) &= v(ac) - v(bd) \\ &= v(a) + v(c) - v(b) - v(d) \\ &= v(a) - v(b) + v(b) - v(d) \\ &= v\left(\frac{a}{b}\right) + v\left(\frac{c}{d}\right), \end{aligned}$$

$$\begin{aligned} v\left(\frac{a}{b} + \frac{c}{d}\right) &= v\left(\frac{ad + bc}{bd}\right) \\ &= v(ad + bc) - v(bd) \\ &= v(ad + bc) - v(b) - v(d), \end{aligned}$$

$$\begin{aligned} v\left(\frac{a}{b} + \frac{c}{d}\right) &\geq \min\left(v(ad), v(bc)\right) - v(b) - v(d) \\ &= \min\left(v(a) - v(b), v(c) - v(d)\right) \\ v\left(\frac{a}{b} + \frac{c}{d}\right) &\geq \min\left(v\left(\frac{a}{b}\right), v\left(\frac{c}{d}\right)\right). \end{aligned}$$

Soit v'' un autre prolongement de v à K. Soit $x \in K$.

Si $x \in A$, alors $v'(x) = v''(x) = v(x)$.

Sinon, $x^{-1} \in A$, $v''(xx^{-1}) = v''(1) = v(1) = 0$ car $1 \in A$. Et v'' est une valuation, donc $v''(xx^{-1}) = v''(x) + v''(x^{-1}) = 0$,
i.e., $v''(x) = -v''(x^{-1}) = -v'(x^{-1}) = v'(1) - v'(x^{-1}) = v'(x)$. D'où $v' = v''$.

□

Corollaire II.A.7
★ Exercice 33, chapitre 5, [AM].

Soient k un corps quelconque, Γ un groupe ordonné et $A = k[\Gamma]$.
$A =$Vect$(x_\alpha, \alpha \in \Gamma)$. A est un anneau intègre. Soit $u = \lambda_1 x_{\alpha_1} + \cdots + \lambda_n x_{\alpha_n}$ avec $\forall 1 \leq i \leq n, \lambda_i \neq 0$ et $\alpha_1 < \alpha_2 < \cdots < \alpha_n$.

Si u n'est pas inversible dans A, on définit $v(u) = \alpha_1$.

Preuve
Soient $u, w \in A$,

$$u = \lambda_1 x_{\alpha_1} + \cdots + \lambda_n x_{\alpha_n},$$
$$w = \mu_1 x_{\beta_1} + \cdots + \mu_n x_{\beta_d},$$

avec $\alpha_1 < \cdots < \alpha_n$ et $\beta_1 < \cdots < \beta_d$ donc $\alpha_1\beta_1 \leq \alpha_i\beta_j$ $\forall 1 \leq i, j \leq n$.

$$uw = \lambda_1\mu_1 x_{\alpha_1} x_{\beta_1} + \cdots + \lambda_n\mu_d x_{\alpha_n} x_{\beta_d},$$
$$uw = \lambda_1\mu_1 x_{\alpha_1+\beta_1} + \cdots + \lambda_n\mu_d x_{\alpha_n+\beta_d},$$

$$v(uw) = \alpha_1 + \beta_1 = v(u) + v(w).$$
$$v(u + w) \geq \min(v(u), v(w)).$$

Il y a égalité si $\lambda_1 x_{\alpha_1} \neq -\mu_1 x_{\beta_1}$.

□

N'importe quel groupe ordonné est donc le groupe des valeurs d'une valuation.

EXEMPLE

♮ $A = K((X))[[Y]] = \left\{ \sum_{j\in\mathbb{N}} \left(\sum_{i\in\mathbb{Z}, i\geq i_0(j)} a_{(j,i)} X^i \right) Y^j \;\middle|\; a_{(j,i)} \in K \right\}$.
On rappel que $K((X))$ est constitué des séries de Laurent en X à coefficients dans K et que $K[[Y]]$ est constitué des séries formelles en Y à coefficients dans K.

On définit la valuation v : $v(P \in A) = \inf\{(j,i) \mid a_{(j,i)} \neq 0\}$ pour l'ordre lexicographique.
L'anneau de valuation de A par rapport à v est $\{P \in A \mid v(P) \geq 0\}$.
$v(P) \geq 0$ si $\inf(j,i) \geq 0$, *i.e.*, $\inf(j,i) = (a,b)$ avec $a > 0$ ou $a = 0$ et $b \geq 0$.
Si $a > 0$, alors $P \in YK((X))[[Y]]$.
Si $a = 0$ et $b \geq 0$, alors $P \in K[[X]]$.
On a donc $\{P \in A \mid v(P) \geq 0\} = K[[X]] + YK((X))[[Y]]$.

♮ Sous groupes isolés : $\langle 0\rangle \subset (0 \times \mathbb{Z}) \subset \mathbb{Z}^2$:
$\langle 0\rangle = v(A \setminus \langle X, Y\rangle)$.
$(0 \times \mathbb{Z}) = v(A \setminus YA)$.
$\mathbb{Z}^2 = v(A \setminus \langle 0\rangle)$.
La bijection $\mathfrak{p} \leftrightarrow v(A \setminus \mathfrak{p})$ est donc bien décroissante.

II.B. Valuation discrète

Définition II.7 v est une valuation discrète si son groupe des valeurs est $\mathbb{Z} \cup \{\infty\}$.

Remarque : Attention, il existe d'autres définitions. Par exemple, pour

O. Zariski, les valuations discrètes sont les valuations de groupe des valeurs

$\Gamma = \mathbb{Z}^n_{\text{lex}}$.

Définition II.8 Soit V un anneau intègre de corps des fractions K. V est un anneau de valuation discrète, ou DVR (*Discrete Valuation Ring*), s'il existe une valuation discrète v de K telle que V soit l'anneau de valuation de v.

Rappel II.2 *:* Soit I un idéal de A, $I^n = \langle a_1 a_2 \cdots a_n | a_i \in I\rangle$.

Rappel II.3 *:* Soit A un anneau, A est noethérien si tous les idéaux de A sont de type finis, *i.e.*, engendré par un nombre fini d'éléments de A.

Définition II.9 La dimension de Krull d'un anneau A est la borne supérieure de la longueur des chaînes d'idéaux premiers de A.

Proposition II.B.1
Soit A un anneau intègre local noethérien, de dimension de Krull 1, d'idéal maximal $\mathfrak{m}$ et de corps résiduel $k = A/\mathfrak{m}$. Les assertions suivantes sont équivalentes :
(i) A est un DVR ;
(ii) A est intégralement clos dans $\text{Frac}(A)$;
(iii) $\mathfrak{m}$ est principal ;
(iv) $\dim_k \mathfrak{m}/\mathfrak{m}^2 = 1$;

(v) Tout idéal non nul de A est une puissance de $\mathfrak{m}$;
(vi) Il existe $t \in A$ tel que tout idéal non nul de A est de la forme $\langle t^m \rangle$ avec $m \in \mathbb{N}$.

Définition II.10 t est appelé « uniformisante » de A et est défini à un inversible près.

Preuve

(i) $\Rightarrow$ (ii) déjà vu, voir la proposition II.A.3.

(ii) $\Rightarrow$ (iii)

- Soit $a \in \mathfrak{m}$, non nul.
  Rappel II.4 *:* Le radical de $\langle a \rangle$ est : $\sqrt{aA} = \bigcap_{\mathfrak{p} \subset aA} \mathfrak{p}$, $\mathfrak{p}$ idéal premier de A.
  Comme A est de dimension de Krull 1, $\mathrm{Spec}(A)=\{(0), \mathfrak{m}\}$ et $\sqrt{aA} = \mathfrak{m}$.
  De plus, A est noethérien donc $\mathfrak{m} = \langle a_1, \ldots, a_m \rangle$ et il existe $N \in \mathbb{N}$ tel que $a_1^N, a_2^N, \ldots, a_m^N \in aA$.
  $\mathfrak{m}^{N'} = \langle a_1^{u(1)} \cdots a_m^{u(m)} \rangle$ avec $u(1) + \cdots + u(m) = N'$.
  Si $N' \geq mN$, alors $\mathfrak{m}^{N'} \subset aA$.
- Soit n_0 le plus petit entier tel que $\mathfrak{m}^{n_0} \subset aA$.
  Si $n_0 = 1$, alors $\langle a \rangle = \mathfrak{m}$, donc $\mathfrak{m}$ est principal.
  Sinon, $\mathfrak{m}^{n_0-1} \nsubseteq aA$. Donc, $\exists b \in \mathfrak{m}^{n_0-1}$, $b \notin aA$. Posons $x = \frac{a}{b} \in \mathrm{Frac}(A)$, alors $x^{-1} \notin A$, sinon $b = \frac{b}{a} \cdot a \in aA$, ce qui est faux par hypothèse. Donc x^{-1} n'est pas entier sur A, car A est intégralement clos.
  Par la proposition I.D.1 (iv), $x^{-1}\mathfrak{m} \nsubseteq \mathfrak{m}$, sinon $\mathfrak{m}$ serait un $A[x^{-1}]$-module fidèle de type fini sur A. Cependant, $x^{-1}\mathfrak{m} \subset A$ car $\forall m \in \mathfrak{m}, bm \in \mathfrak{m}^{n_0}$ puisque $b \in \mathfrak{m}^{n_0-1}$ et $\mathfrak{m}^{n_0} \subset aA$.
  Donc $x^{-1}\mathfrak{m}$ est un sous-A-module de A, donc c'est un idéal de A et $x^{-1}\mathfrak{m}$ n'est pas inclus dans l'idéal maximal de A. $x^{-1}\mathfrak{m} = A$.
  De là, on conclut que $\mathfrak{m} = xA = \langle x \rangle$ car $\forall a \in A, \exists m \in \mathfrak{m}, a = x^{-1}m$, d'où $xa = m$.

(iii) $\Rightarrow$ (iv) $\mathfrak{m}/\mathfrak{m}^2$ est un groupe additif. On définit :

$$\begin{aligned}(A/\mathfrak{m} \times \mathfrak{m}/\mathfrak{m}^2) &\to \mathfrak{m}/\mathfrak{m}^2 \\ (\tilde{a}, \overline{m}) &\mapsto \tilde{a}\overline{m} = \overline{am}.\end{aligned}$$

Cette application est bien définie : $\tilde{a} = \tilde{b}$, $\overline{\mu} = \overline{m}$ alors $b = a + \nu$, $\mu = m + \rho$ avec $\nu \in \mathfrak{m}$ et $\rho \in \mathfrak{m}^2$. On a donc :

$$b\mu = am + \underbrace{\underbrace{a\rho}_{\in \mathfrak{m}^2 \ car \ \rho \in \mathfrak{m}^2} + \underbrace{\nu m}_{\in \mathfrak{m}^2 \ car \ \nu, m \in \mathfrak{m}} + \underbrace{\nu\rho}_{\in \mathfrak{m}^3 \ donc \ \in m^2}}_{\in \mathfrak{m}^2}$$

et

$$\overline{b\mu} = \overline{am}$$

ce qui définit une structure de k-espace vectoriel sur $\mathfrak{m}/\mathfrak{m}^2$.
Comme $\mathfrak{m}$ est principal, $\forall m \in \mathfrak{m}, m = ax$, $\overline{m} = \overline{ax} = \tilde{a}\overline{x}$.
Donc $\mathfrak{m}/\mathfrak{m}^2$ est engendré pas $\overline{x}$.
Par le lemme I.D.3, si $\mathfrak{m}/\mathfrak{m}^2 = (0)$, alors $\mathfrak{m} = (0)$, ce qui contredit $\dim A = 1$.
Donc $\mathfrak{m}/\mathfrak{m}^2 \neq (0)$.
On en déduit que $\mathfrak{m}/\mathfrak{m}^2$ est de dimension 1.

(iv) $\Rightarrow$ (v) et (vi) **Par le lemme I.D.3, si $\dim_k \mathfrak{m}/\mathfrak{m}^2 = 1$, alors $\mathfrak{m}$ est principal.**
Soit I un idéal de A, $I \neq (0)$, $I \neq A$. Il existe $n \in \mathbb{N}$ tel que $\mathfrak{m}^n \subset I$ et $\mathfrak{m}^{n-1} \nsubseteq I$.
Remarque : $I \subset \mathfrak{m}$ et $\forall n' \geq n$, $\mathfrak{m}^{n'} \subseteq I$.
Soit n_0 le plus grand entier tel que $I \subset \mathfrak{m}^{n_0}$, par la remarque précédente n_0 existe.
Donc $I \subset \mathfrak{m}^{n_0}$ et $I \nsubseteq \mathfrak{m}^{n_0+1}$. Soit $y \in I \setminus \mathfrak{m}^{n_0+1}$, $y = ax^{n_0}$ et $a \notin \mathfrak{m}$, sinon $y \in \mathfrak{m}^{n_0+1}$. Comme A est local, $\mathfrak{m}$ est l'ensemble des éléments non inversibles de A, donc a est inversible.
Comme a est inversible, $x^{n_0} \in I$ donc $\langle x^{n_0} \rangle = \mathfrak{m}^{n_0} \subset I$.
On obtient alors $I = \mathfrak{m}^{n_0} = \langle x^{n_0} \rangle$.

(v) $\Rightarrow$ (vi) $\mathfrak{m}/\mathfrak{m}^2 \neq (0)$, sinon, par le lemme I.D.3, si $\mathfrak{m}/\mathfrak{m}^2 = (0)$, alors $\mathfrak{m} = (0)$, ce qui contredit $\dim A = 1$.
Soit $x \in \mathfrak{m}/\mathfrak{m}^2$, $\langle x \rangle \subset \mathfrak{m}$ et $\langle x \rangle \nsubseteq \mathfrak{m}^r$, $\forall r \geq 2$. Donc $\langle x \rangle = \mathfrak{m}$ et $\langle x^r \rangle = \mathfrak{m}^r$, $r \geq 1$.

(vi) $\Rightarrow$ (i) Les idéaux de A sont donc totalement ordonnés pour l'inclusion. Par la proposition II.A.4, A est un anneau de valuation de son corps de fractions.
De plus, $\forall a \in A, \langle a \rangle = (t^r)$ avec un r unique.
En effet, si $a = ut^r = vt^s$ avec $r \leq s$, alors $t^r(u - vt^{s-r}) = 0$. Donc $u = vt^{s-r}$ et t^{s-r} est inversible. On en déduit donc que tout idéal de A est A, ce qui contredit A de dimension 1.
D'où : $\forall a \in K = \mathrm{Frac}(A)$, $a = ut^r$, $r \in \mathbb{Z}$, u inversible dans A. On pose $v(a) = r$; v est une valuation de groupe des valeurs $\mathbb{Z}$, d'anneau de valuation A.
Donc A est un DVR.

□

Cette proposition contient les critères usuels pour reconnaitre un DVR.

III. Applications et utilisations de la théorie

III.A. Théorème d'Ostrowski - Analyse p-adique

Définition III.1 Soit K un corps. Une *norme* sur K est une application $x \mapsto |x|$, de K dans $\mathbb{R}^+$ telle que :

1. $\forall x \in K, |x| = 0 \Leftrightarrow x = 0$;
2. $\forall x, y \in K, |xy| = |x||y|$;
3. $\forall x, y \in K, |x + y| \leq |x| + |y|$.

Définition III.2 Deux normes sur un corps K sont dites équivalentes si elles définissent la même topologie.

Proposition III.A.1
Deux normes $|\cdot|_1$ et $|\cdot|_2$ sont équivalentes si, et seulement si, il existe $s \in R^{*+}$ tel que l'on ait $|x|_1 = |x|_2^s$ quel que soit $x \in K^*$.

Preuve
Si $|\cdot|$ est une norme sur un corps K, alors $|x| < 1$ si, et seulement si, la suite de terme général x^n tend vers 0 quand n tend vers $+\infty$.
On en déduit le fait que si $|\cdot|_1$ et $|\cdot|_2$ sont équivalentes, alors

$$\{x \in K|\ |x|_1 < 1\} = \{x \in K|\ |x|_2 < 1\}.$$

Si ce dernier ensemble est réduit à $\{0\}$, on a $|x|_1 = |x|_2 = 1$ quel que soit $x \in K^*$. Sinon, soit $x \in K^*$ vérifiant $|x|_1 < 1$. Si $y \in K^*$, $a \in \mathbb{Z}$ et $b \in \mathbb{N}$, alors

$$|y^b x^{-a}|_1 < 1 \Leftrightarrow |y^b x^{-a}|_2 < 1.$$

On en déduit le fait que :

$$\left\{ r \in \mathbb{Q} \middle|\ r < \frac{\log |y|_1}{\log |x|_1} \right\} = \left\{ r \in \mathbb{Q} \middle| r < \frac{\log |y|_2}{\log |x|_2} \right\}$$

et donc que les deux quotients $\frac{\log |y|_1}{\log |x|_1}$ et $\frac{\log |y|_2}{\log |x|_2}$ sont les bornes supérieures d'un ensemble borné non vide de $\mathbb{Q}$. Les deux quotients sont donc égaux, ce qui montre que la fonction $y \mapsto \log |y|_1$ est constante sur K^* et permet de conclure.

□

Définition III.3 On définit la norme p-adique sur $\mathbb{Q}$ par $\forall x \in \mathbb{Q}$, $x = p^r \frac{a}{b}$, tel que p ne divise ni a ni b, $|x|_p = p^{-r}$.

THÉORÈME III.1

Théorème d'Ostrowski. Toute norme non triviale sur $\mathbb{Q}$ est équivalente à la valeur absolue usuelle $|\cdot|_\infty$ ou à une certaine valeur absolue p-adique $|.|_p$.

Preuve

Soit $|\cdot|$ une norme non triviale sur $\mathbb{Q}$.

S'il existe $k \in \mathbb{N}$ tel que $|k| > 1$, alors $|k| = |\underbrace{1 + \cdots + 1}_{k fois}| \leq k|1| = k$

Donc il existe $\alpha \in]0; 1]$ tel que $|k| = k^\alpha$.

Soit $m \in \mathbb{N}$, alors la décomposition de m en base k est :

$$m = \sum_{i=0}^{n} a_i k^i, \quad a_i \in \{0, 1, \ldots, k-1\}, \;\; a_n \neq 0.$$

$m \geq k^n$, $|a_i| \leq a_i \leq k - 1$.

$$|m| \leq \sum_{i=0}^{n} |a_i||k^i| = (k-1) \sum_{i=0}^{n} |k^i|$$

$$\leq (k-1) \sum_{i=0}^{n} (k^\alpha)^i = (k-1) \frac{k^{(n+1)\alpha} - 1}{k^\alpha - 1} = \frac{k^\alpha (k-1)}{k^\alpha - 1} - \underbrace{\frac{\overbrace{k-1}^{\geq 0}}{\underbrace{k^\alpha}_{=|k|>1} - 1}}_{\geq 0}$$

$$\leq (k^n)^\alpha \underbrace{\frac{k^\alpha (k-1)}{k^\alpha - 1}}_{C}$$

$$|m| \leq C m^\alpha.$$

Comme C est indépendant de m, on peut remplacer m par m^n, d'où $|m^n| = |m|^n \leq C m^{n\alpha}$. En passant à la racine n-ième on obtient : $|m| \leq \exp(\frac{1}{n} \ln C) m^\alpha$. En passant ensuite à la limite quand n tend vers l'infini, on obtient : $|m| \leq m^\alpha$.

$$|k| = k^\alpha \;\; donc \;\; \ln|k| = \alpha \ln k,$$

$$|m| \leq m^\alpha \;\; donc \;\; \ln|m| = \alpha \ln m = \frac{\ln|k|}{\ln k} \ln m,$$

$$\frac{\ln|m|}{\ln m} \leq \frac{\ln|k|}{\ln k}.$$

Si $|m| \geq 1$ alors, de même, il existe β tel que : $|m| = m^\beta$, $|k| \leq k^\beta$.

Donc $\frac{\ln|k|}{\ln k} \leq \frac{\ln|m|}{\ln m}$ d'où l'égalité.

De plus, $\forall m \in \mathbb{N}$, $\exists n \in \mathbb{N}$ tel que $|k^n m| > 1$ et $\frac{\ln|k|}{\ln k} = \frac{\ln|k^n m|}{\ln k^n m} = \frac{n\ln|k|+\ln|m|}{n\ln k+\ln m}$ d'où $\frac{\ln|k|}{\ln k} = \frac{\ln|m|}{\ln m}$.

Soit $x \in \mathbb{Q}$, $x = \pm\frac{a}{b}$ $a, b \in \mathbb{N}$ donc $|x| = |\frac{a}{b}| = \frac{|a|}{|b|}$ et $|x|_\infty = \frac{a}{b}$.

$\ln|x| = \ln\frac{|a|}{|b|} = \ln|a| - \ln|b| = (\ln a - \ln b)\frac{\ln|k|}{\ln k} = \frac{\ln|k|}{\ln k}\ln|x|_\infty$.

$\frac{\ln|x|}{\ln|x|_\infty} = \frac{\ln|k|}{\ln k} = \alpha$ donc $|x| = |x|_\infty^\alpha$ et $|\cdot|$ est équivalente à $|\cdot|_\infty$.

Sinon, $\forall k \in \mathbb{N}$, $|k| \leq 1$. *A fortiori*, $\forall p \in \mathbb{N}$, p premier, $|p| \leq 1$. Comme $|.|$ est non triviale, par la décomposition en facteurs premiers, $\exists p$ premier, tel que $|p| < 1$. S'il existe p et q de normes strictement plus petites que 1 alors, par le théorème de Bézout :

$$\exists u_n, v_n \in \mathbb{Z}, 1 = u_n p^n + v_n q^n$$

d'où :

$$1 = |u_n p^n + v_n q^n| \leq |u_n||p^n| + |v_n||q^n| \leq |p|^n + |q|^n.$$

Or, quand n est suffisamment grand, $1 > |p|^n + |q|^n$, ce qui amène une contradiction. Donc $|.|$ est équivalente à la norme p-adique $|.|_p$.

□

III.B. Géométrie algébrique

Définition III.4 Soit k un corps. On dit que $F \subset k^n$ est un *fermé (de Zariski)* si $\exists I \subset k[X_1, \ldots, X_n]$, $F = \{(a_1, \ldots, a_n) \in k^n \mid \forall P \in I \;\; P(a_1, \ldots, a_n) = 0\}$.
$I(F) = \{P \in k[X_1, \ldots, X_n] \mid P \text{ est nul sur } F\}$.
Remarque : $I \subset I(F)$.

Définition III.5 On dit que F est *irréductible* si $I(F)$ est premier.

Définition III.6 Soit F irréductible.

On appelle *anneau de* F, l'anneau $k[F] := k[X_1, \ldots, X_n]/I(F)$.

On appelle *corps de* F, $k(X_1, \ldots, X_n)/I(F)$ le corps des fractions de $k[F]$.

Définition III.7 La *dimension* de F est $\dim(F) := \dim k[F]$.

Théorème III.2
Théorème de Dedekind, Noether, Riemann.

Soit F une courbe « normale » projective (pas de définition donnée ici). Il y a une bijection entre les points de F et les anneaux de valuations de $k[F]$ contenant k, ces anneaux sont des DVR.

Théorème III.3
Théorème de Zariski.

Soit F un fermé projectif irréductible. Il y a une application surjective continue pour la topologie de Zariski qui envoie l'ensemble des anneaux de valuations de $k[F]$ (*i.e.*, la variété de Riemann – Zariski) sur les points de F.

Ces théorèmes donnent un aperçu de ce qui pourrait être étudié ensuite. Leurs démonstrations font appel aux théorèmes vus pendant ce stage mais aucune preuve ne sera fournie ici.

Exemple de M. Spivakovsky ([Spi]) : une extension non triviale

On s'intéresse à $\mathbb{C}[u,v]_{\langle u,v\rangle} = \left\{ \frac{P(u,v)}{Q(u,v)} \middle| Q(0,0) \neq 0 \right\}$.

$$\mathbb{C}[u,v]_{\langle u,v\rangle} \subset \mathbb{C}\{u,v\}$$

où $\mathbb{C}\ \{u,v\}$ est l'ensemble des séries en u et v de rayons de convergence non nul.

On pose $t = u + \sum_{n=1}^{\infty} \frac{1}{n!} v^n = u + \mathrm{e}^v - 1$.

Comme $\mathbb{C}\{u,v\}$ est factoriel,

$$\forall f \in \mathbb{C}\{u,v\},\ f = t^n \varphi \text{ où } \varphi \text{ n'est pas divisible par } t.$$

On considère alors l'application :

$$\forall f \in \mathbb{C}\{u,v\},\ \nu(f) = (n, \mathrm{ord}_{\langle u,v\rangle}\, \varphi) \in \mathbb{Z}^2_{\mathrm{lex}}.$$

$f = t^n\varphi$, $g = t^m\phi$. $fg = t^{n+m}\varphi\phi$, t ne divise ni φ, ni ϕ donc t ne divise pas $\varphi\phi$.

Comme $ord_{u,v}$ est une valuation, on a :

$$\begin{aligned}\nu(fg) &= (n+m, \operatorname{ord}_{\langle u,v\rangle} \varphi\phi) \\ &= (n, \operatorname{ord}_{u,v} \varphi) + (m, \operatorname{ord}_{\langle u,v\rangle} \phi) \\ &= \nu(f) + \nu(g).\end{aligned}$$

Quitte à intervertir f et g, supposons $n \geq m$:

$$\begin{aligned}\nu\left(f+g\right) &= \nu\left(t^n\varphi + t^m\phi\right) \\ &= \nu\left(t^m\left(t^{n-m}\varphi + \phi\right)\right) \\ &\geq \min\left(\nu\left(f\right), \nu\left(g\right)\right).\end{aligned}$$

v est donc une valuation et son groupe des valeurs est $\mathbb{Z}^2_{\text{lex}}$.

$$u = t - \textstyle\sum_{n=1}^{\infty} \frac{1}{n\,!} v^n.$$

De plus, t ne divise pas $\sum_{n=1}^{\infty} \frac{1}{n!} v^n$, sinon $\sum_{n=1}^{\infty} \frac{1}{n!} v^n = t\rho$ et $\frac{1}{1!} v^1 = v = (u+v)\rho_0$, ce qui est impossible. Donc, $\nu(u) = (0,1)$. De même :

$$\nu(u+v) = \nu(t - \sum_{n=2}^{\infty} \frac{1}{n\,!} v^n) = (0,2)$$

$$\nu(u+v+\frac{1}{2}v^2) = \nu(t - \sum_{n=3}^{\infty} \frac{1}{n\,!} v^n) = (0,3)$$

$$\vdots$$

$$\nu(u + \sum_{j=1}^{n} \frac{1}{j\,!} v^j) = \nu(t - \sum_{j=n+1}^{\infty} \frac{1}{j\,!} v^j) = (0, n+1).$$

On montre alors que la restriction de v à $\mathbb{C}[u,v]$ admet $\mathbb{Z}$ comme groupe des valeurs :

$$\forall s \in \mathbb{C}[u,v],\ s(u,v) = \textstyle\sum \lambda_{a,b} u^a v^b = t\phi = (u + \mathrm{e}^v - 1)\phi$$

$$s(1 - \mathrm{e}^v, v) = \textstyle\sum \lambda_{a,b} (1 - e^v)^a v^b = 0$$

$$\forall n \in \mathbb{N},\ s(1 - \mathrm{e}^n, n) = \textstyle\sum \lambda_{a,b} (1 - \mathrm{e}^n)^a n^b = 0$$

ce qui est impossible car e est transcendant, donc t ne divise pas s et $\nu(s) = (0,m)$.

Il est commode de regarder le développement en série de $\frac{P(u,v)}{Q(u,v)}$, car ce développement contient des informations cruciales, notamment grâce au polygone de Newton.

Une valuation sur $\mathbb{C}[u,v]_{\langle u,v\rangle}$ s'étend à $\mathbb{C}\{u,v\}$ ou $\mathbb{C}[u,v]$ par le corollaire II.A.3. Mais, ATTENTION, le groupe des valeurs peut changer, et même changer de dimension !

Bibliographie

[Abh] S.S. Abhyankar, *Resolution of singularities and modular galois theory* , Bull. Amer. Math. Soc. 38 (2001), 131–169

[AM] M.F. Atiyah, I.G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley Publishing Co., Reading, Menlo Park, London, Don Mills, 1969

[C] P. Colmez, *Les nombres p-adiques*, notes de cours de M2.

[Spi] M. Spivakovsky, *Valuations in function fields of surfaces*, American Journal of Mathematics, Vol. 112, No.1 (Feb., 1990).

[Vaq] M. Vaquié, *Valuations*, Resolution of singularities (Obergurgl, 1997), 539 – 590, Progr.Math., 181, Birkhauser, Basel, 2000

[Z] O. Zariski, P. Samuel, *Commutative Algebra*, Vol. II, Springer-Verlag, New York, 1960.