Une valuation discrète est unique

Tsung-Hsuan TSAI Sarah TIMHADJELT

École Normale Supérieure de Rennes

28 Avril 2017

Abstrait

Une valuation est **une mesure de la multiplicité**. Cette notion est une généralisation du degré de divisibilité d'un entier par un nombre premier.

Dans cette présentation, on démontrera que pour un **corps complet de valuation discrète**, une valuation discrète est unique.

On aura notamment besoin du **lemme d'approximation** et du **lemme de Hensel**. Pour éviter de parler d'extension du corps, on supposera que le corps résiduel est algébriquement clos.

Table des matières

Section 1

Généralité sur la valuation

Définition d'une valuation

Définition

Soit $(K, +, \times)$ un corps commutatif et $(G, +, <)$ un groupe abélien totalement ordonné. On appelle **valuation** une application $v : K \to G \cup \{\infty\}$ vérifiant

- $v(x) = \infty \Leftrightarrow x = 0$
- $v(xy) = v(x) + v(y)$
- $v(x + y) \geqslant \min\{v(x), v(y)\}$

On étend les lois de $(G, +, <)$ sur $G \cup \{\infty\}$ par :

- $x + \infty = \infty$ et $x < \infty \quad \forall x \in G$
- $\infty + \infty = \infty$ et $\infty \leqslant \infty$

On appelle K **corps de valuation**.

Exemples

Exemple

L'application $v : K \to G \cup \{\infty\}$ vérifiant

$$v(a) = \begin{cases} 0 & \text{si} \quad a \neq 0 \\ \infty & \text{si} \quad a = 0 \end{cases}$$

est une valuation, dite **valuation triviale**.

Exemples

Exemple

L'application $v : K \to G \cup \{\infty\}$ vérifiant

$$v(a) = \begin{cases} 0 & \text{si} \quad a \neq 0 \\ \infty & \text{si} \quad a = 0 \end{cases}$$

est une valuation, dite **valuation triviale**.

Exemple

Soit A un anneau intègre commutatif, $v : A \to G \cup \{\infty\}$ vérifiant

- $v(0) = \infty \Leftrightarrow x = 0$
- $v(xy) = v(x) + v(y)$
- $v(x + y) \geqslant \min\{v(x), v(y)\}$

se prolonge naturellement en une valuation sur $\mathrm{Frac}(A)$ par $v(a/b) = v(a) - v(b)$.

Propriétés et Définitions

Lemme

Si $v(a) \neq v(b)$, alors $v(a+b) = \min\{v(a), v(b)\}$.

Propriétés et Définitions

Lemme

Si $v(a) \neq v(b)$, alors $v(a+b) = \min\{v(a), v(b)\}$.

Définition

$A_v := \{a \in K | v(a) \geqslant 0\}$ munit des opérations induites est un sous anneau de K. On l'appelle **anneau de valuation** associé à v.

Propriétés et Définitions

Lemme

Si $v(a) \neq v(b)$, alors $v(a+b) = \min\{v(a), v(b)\}$.

Définition

$A_v := \{a \in K | v(a) \geqslant 0\}$ munit des opérations induites est un sous anneau de K. On l'appelle **anneau de valuation** associé à v.

Proposition

$\mathfrak{m}_v := \{a \in K | v(a) > 0\}$ est l'unique idéal maximal de A_v. (i.e. A_v est un anneau local.)

Définition d'une valuation discrète

Une valuation v est dite **discrète** si $v(K^\times)$ (qui est un sous groupe de G) est isomorphe au groupe cyclique $\mathbb{Z}$.
Une valuation discrète sur K se ramène à une application **surjective** $v : K \to \mathbb{Z} \cup \{\infty\}$.

Définition d'une valuation discrète

Une valuation v est dite **discrète** si $v(K^\times)$ (qui est un sous groupe de G) est isomorphe au groupe cyclique $\mathbb{Z}$.
Une valuation discrète sur K se ramène à une application **surjective** $v : K \to \mathbb{Z} \cup \{\infty\}$.

- K est appelé corps de valuation discrète
- A_v est appelé anneau de valuation discrète

Propriétés

- $v(A_v) = \mathbb{N} \cup \{\infty\}$

Propriétés

- $v(A_v) = \mathbb{N} \cup \{\infty\}$
- $\pi \in A_v$ est appelé une **uniformisante** si $v(\pi) = 1$

Propriétés

- $v(A_v) = \mathbb{N} \cup \{\infty\}$
- $\pi \in A_v$ est appelé une **uniformisante** si $v(\pi) = 1$
- $\mathfrak{m}_v = \{a \in A_v | v(a) > 0\} = \{a \in A_v | v(a) \geqslant 1\} = (\pi)$

Propriétés

- $v(A_v) = \mathbb{N} \cup \{\infty\}$
- $\pi \in A_v$ est appelé une **uniformisante** si $v(\pi) = 1$
- $\mathfrak{m}_v = \{a \in A_v | v(a) > 0\} = \{a \in A_v | v(a) \geqslant 1\} = (\pi)$
- $\{a \in K | v(a) \geqslant n\}$ avec $n \in \mathbb{N}$ sont **les idéaux** de A_v

Propriétés

- $v(A_v) = \mathbb{N} \cup \{\infty\}$
- $\pi \in A_v$ est appelé une **uniformisante** si $v(\pi) = 1$
- $\mathfrak{m}_v = \{a \in A_v | v(a) > 0\} = \{a \in A_v | v(a) \geqslant 1\} = (\pi)$
- $\{a \in K | v(a) \geqslant n\}$ avec $n \in \mathbb{N}$ sont **les idéaux** de A_v
- $\{a \in K | v(a) \geqslant n\} = \mathfrak{m}_v^n = (\pi^n)$

Exemples

Exemple

Soit p premier, $a \in \mathbb{Z}$. On définit :

$$v_p(a) = \sup\{n \in \mathbb{N} \mid p^n \text{ divise } a\}$$

v_p se prolonge en une valuation discrète sur $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$, vérifiant

$$v_p\left(\frac{a}{b}\right) = \begin{cases} n \in \mathbb{Z} & \text{si} \quad \frac{a}{b} = p^n \frac{a'}{b'} \quad \text{avec} \quad p \nmid a', p \nmid b' \\ \infty & \text{si} \quad a = 0 \end{cases}$$

On l'appelle **valuation *p*-adique** de $\mathbb{Q}$.
$A_{v_p} = \{\frac{a}{b} \mid a, b \in \mathbb{Z}, p \nmid b\}$; $\mathfrak{m}_{v_p} = pA_{v_p}$; $k_{v_p} \cong \mathbb{Z}/p\mathbb{Z}$.

Section 2

Valeur absolue associée et Lemme d'approximation

Définition d'une valeur absolue

Le lemme d'approximation est un résultat pour les valeurs absolues. Pour une valuation à valeurs réelles, on peut lui associer une valeur absolue. Ce résultat admet donc une version pour les valuations.

Définition d'une valeur absolue

Le lemme d'approximation est un résultat pour les valeurs absolues. Pour une valuation à valeurs réelles, on peut lui associer une valeur absolue. Ce résultat admet donc une version pour les valuations.

Définition

Soit K un corps. Une **valeur absolue** sur K est une application $|\cdot|$ de K dans $\mathbb{R}^+$ telle que $\forall x, y \in K$:

- $|x| = 0 \Leftrightarrow x = 0$
- $|xy| = |x| \cdot |y|$
- $|x + y| \leqslant |x| + |y|$

Si en plus $|x + y| \leqslant max(|x|, |y|)$, alors $|\cdot|$ est dite **ultramétrique**.

Exemples

Exemple

L'application $|\cdot| : K \to \mathbb{R}^+$ définie par :

$$|x| = \begin{cases} 1 & \text{si} \quad x \neq 0 \\ 0 & \text{si} \quad x = 0 \end{cases}$$

est une valeur absolue sur K, appelé **valeur absolue triviale**.

Exemples

Exemple

L'application $|\cdot| : K \to \mathbb{R}^+$ définie par :

$$|x| = \begin{cases} 1 & \text{si} \quad x \neq 0 \\ 0 & \text{si} \quad x = 0 \end{cases}$$

est une valeur absolue sur K, appelé **valeur absolue triviale**.

Exemple

La valeur absolue usuelle sur $\mathbb{R}$ définie par :

$$|x| = \begin{cases} x & \text{si} \quad x \geqslant 0 \\ -x & \text{sinon} \end{cases}$$

Distance et Topologie associées

On définit la distance associée par $d(x, y) = |x - y|$.
(K, d) est un espace métrique.

Distance et Topologie associées

On définit la distance associée par $d(x, y) = |x - y|$.
(K, d) est un espace métrique.

Définition

Deux valeurs absolues $|\cdot|_1, |\cdot|_2$ sur un corps K sont dites équivalentes si elles définissent la même topologie.

Distance et Topologie associées

On définit la distance associée par $d(x, y) = |x - y|$.
(K, d) est un espace métrique.

Définition

Deux valeurs absolues $|\cdot|_1, |\cdot|_2$ sur un corps K sont dites équivalentes si elles définissent la même topologie.

Lemme

Les assertions suivantes sont équivalentes pour deux valeurs absolues non triviales sur un corps K :

1. $|\cdot|_1$ et $|\cdot|_2$ sont équivalentes
2. $\forall x \in K \ (|x|_1 < 1 \Leftrightarrow |x|_2 < 1)$
3. $\exists \alpha \geqslant 0 \ \forall x \in K \ (|x|_1 = |x|_2^{\alpha})$

Afin de démontrer le lemme d'approximation, il nous faut un lemme intermédiaire :

Lemme

Soit $|\cdot|_1, ..., |\cdot|_J$ des valeurs absolues non triviales non équivalentes sur un corps K. Alors il existe $x \in K$ tel que $|x|_1 > 1$ et $\forall j \in [\![2, J]\!]\ |x|_j < 1$.

Afin de démontrer le lemme d'approximation, il nous faut un lemme intermédiaire :

Lemme

Soit $|\cdot|_1, ..., |\cdot|_J$ des valeurs absolues non triviales non équivalentes sur un corps K. Alors il existe $x \in K$ tel que $|x|_1 > 1$ et $\forall j \in [\![2, J]\!]\ |x|_j < 1$.

Démonstration : (cas $J = 2$)
Sachant que $|\cdot|_1, |\cdot|_2$ non équivalentes et non triviales, il existe $y \in K^\times$ tel que $|y|_1 < 1, |y|_2 \geqslant 1$ et
$z \in K$ tel que $|z|_1 \geqslant 1, |z|_2 < 1$.
On pose $x = zy^{-1}$. Alors $|x|_1 > 1$ et $|x|_2 < 1$.

Le lemme d'approximation dit que pour les valeurs absolues non équivalentes, on peut approcher simultanément les éléments de K.

Théorème (lemme d'approximation)

Soient $\epsilon > 0$, $J \in \mathbb{N}$ et $|\cdot|_1, ..., |\cdot|_J$ des valeurs absolues sur un corps K non triviales non équivalentes. Soit $(b_1, ..., b_J) \in K^J$, alors il existe $x \in K$ tel que $\forall j \in [\![1, J]\!]$ on ait $|x - b_j|_j < \epsilon$.

Le lemme d'approximation dit que pour les valeurs absolues non équivalentes, on peut approcher simultanément les éléments de K.

Théorème (lemme d'approximation)

Soient $\epsilon > 0$, $J \in \mathbb{N}$ et $|\cdot|_1, ..., |\cdot|_J$ des valeurs absolues sur un corps K non triviales non équivalentes. Soit $(b_1, ..., b_J) \in K^J$, alors il existe $x \in K$ tel que $\forall j \in [\![1, J]\!]$ on ait $|x - b_j|_j < \epsilon$.

Démonstration :(cas $J = 2$)
Soit $x_1 \in K$ tel que $|x_1|_1 > 1$ et $|x_1|_2 < 1$. On a alors

$$\lim_{n\to\infty} \left|\frac{x_1^n}{1+x_1^n}\right|_1 = 1 \text{ et } \lim_{n\to\infty} \left|\frac{x_1^n}{1+x_1^n}\right|_2 = 0$$

Le lemme d'approximation dit que pour les valeurs absolues non équivalentes, on peut approcher simultanément les éléments de K.

Théorème (lemme d'approximation)

Soient $\epsilon > 0$, $J \in \mathbb{N}$ et $|\cdot|_1, ..., |\cdot|_J$ des valeurs absolues sur un corps K non triviales non équivalentes. Soit $(b_1, ..., b_J) \in K^J$, alors il existe $x \in K$ tel que $\forall j \in [\![1, J]\!]$ on ait $|x - b_j|_j < \epsilon$.

Démonstration :(cas $J = 2$)
Soit $x_1 \in K$ tel que $|x_1|_1 > 1$ et $|x_1|_2 < 1$. On a alors

$$\lim_{n\to\infty} \left|\frac{x_1^n}{1+x_1^n}\right|_1 = 1 \text{ et } \lim_{n\to\infty} \left|\frac{x_1^n}{1+x_1^n}\right|_2 = 0$$

On construit de même x_2, on pose alors

$$x = \frac{x_1^n}{1+x_1^n} b_1 + \frac{x_2^n}{1+x_2^n} b_2 \quad \text{pour } n \text{ assez grand.}$$

Valeur absolue associée à une valuation

Définition

Pour un corps K muni d'une valuation v à valeurs réelles, on peut définir la valeur absolue associée à cette valuation par :

$$\begin{array}{rccc} |\cdot|_v : & K & \to & \mathbb{R}^+ \\ & x & \mapsto & e^{-v(x)} \end{array}$$

avec la convention $e^{-\infty} = 0$.

La constante e peut être remplacée par un réel $p > 1$.

Valeur absolue associée à une valuation

Définition

Pour un corps K muni d'une valuation v à valeurs réelles, on peut définir la valeur absolue associée à cette valuation par :

$$\begin{array}{rccc} |\cdot|_v : & K & \to & \mathbb{R}^+ \\ & x & \mapsto & e^{-v(x)} \end{array}$$

avec la convention $e^{-\infty} = 0$.

La constante e peut être remplacée par un réel $p > 1$.

Exemple

La **Valeur absolue p-adique** est la valeur absolue associé à la valuation p-adique.

$$\begin{array}{rccc} |\cdot|_p : & \mathbb{Q} & \to & \mathbb{R}^+ \\ & x & \mapsto & p^{-v_p(x)} \end{array}$$

Équivalences des valuations

Corollaire

Les assertions suivantes sont équivalentes pour deux valuations non triviales sur un corps K.

1. v et w sont équivalentes
2. $A_v = A_w$
3. v et w sont positivement proportionnelles.

Équivalences des valuations

Corollaire

Les assertions suivantes sont équivalentes pour deux valuations non triviales sur un corps K.

1. v et w sont équivalentes
2. $A_v = A_w$
3. v et w sont positivement proportionnelles.

Par conséquence, si on se donne deux valuations discrètes surjectives (sur $\mathbb{Z} \cup \{\infty\}$) équivalentes, alors qu'elles sont identiques.

Lemme d'approximation pour les valuations

Corollaire

Soient $c \in \mathbb{R}$, $J \in \mathbb{N}$ et $v_1, ..., v_J$ des valuations non triviales sur un corps K non équivalentes. Soit $(b_1, ..., b_J) \in K^J$, alors il existe $x \in K$ tel que $\forall j \in [\![1, J]\!]$ on ait $v_j(x - b_j) > c$.

Section 3

Corps complet et Lemme de Hensel

Définition d'un corps complet de valuation

Un corps de valuation K est dit **complet** si $(K, |\cdot|_v)$ est un espace complet.

Définition d'un corps complet de valuation

Un corps de valuation K est dit **complet** si $(K, |\cdot|_v)$ est un espace complet.

- K est appelé corps complet par rapport à la valuation v, ou **corps complet de valuation**.

Définition d'un corps complet de valuation

Un corps de valuation K est dit **complet** si $(K, |\cdot|_v)$ est un espace complet.

- K est appelé corps complet par rapport à la valuation v, ou **corps complet de valuation**.
- Une suite (a_n) de K est convergente si et seulement si $v(a_{n+1} - a_n) \longrightarrow \infty$.

Exemples

Exemple

La complétion de $(\mathbb{Q}, |\cdot|_p)$, notée $\mathbb{Q}_p$, est un corps complet de valuation discrète par rapport à v_p.

- On prolonge v_p par continuité.
- On note souvent $\mathbb{Z}_p$ son anneau de valuation.

Exemples

Exemple

La complétion de $(\mathbb{Q}, |\cdot|_p)$, notée $\mathbb{Q}_p$, est un corps complet de valuation discrète par rapport à v_p.

- On prolonge v_p par continuité.
- On note souvent $\mathbb{Z}_p$ son anneau de valuation.

Exemple

L'anneau des séries formelles $K[[X]]$ munit de l'ordre de $f = \sum_{n\in\mathbb{N}} a_n X^n \in K[[X]]$ définie par

$$o(f) = \inf\{n \in \mathbb{N} \mid a_n \neq 0\}$$

se prolonge au corps des séries formelles de Laurent $K((X))$ en un corps complet de valuation discrète.

Corps résiduel

- Le corps résiduel associé est défini par $k_v := A_v/\mathfrak{m}_v$.

Corps résiduel

- Le corps résiduel associé est défini par $k_v := A_v/\mathfrak{m}_v$.
- On note $\overline{a}$ la classe de $a \in A_v$ dans k_v.
- Si $f = \sum_{i=0}^{n} a_i X^i \in A_v[X]$, on note $\overline{f} = \sum_{i=0}^{n} \overline{a_i} X^i \in k_v[X]$.

Corps résiduel

- Le corps résiduel associé est défini par $k_v := A_v/\mathfrak{m}_v$.
- On note $\overline{a}$ la classe de $a \in A_v$ dans k_v.
- Si $f = \sum_{i=0}^{n} a_i X^i \in A_v[X]$, on note $\overline{f} = \sum_{i=0}^{n} \overline{a_i} X^i \in k_v[X]$.
- $f \in A_v[X]$ est un représentant de $F \in k_v[X]$ si $\overline{f} = F$.

Lemme de Hensel

Le **lemme de Hensel** relève la décomposition premier d'un polynôme de $k_v[X]$ à $A_v[X]$. Il s'applique sur tout **corps complet de valuation discrète**.

Théorème (lemme de Hensel)

Soit $f \in A_v[X]$ unitaire tel que $\overline{f} = GH$ avec G, H unitaires premiers entre eux dans $k_v[X]$.
Alors il existe $g, h \in K[X]$ unitaires tels que

- $\overline{g} = G,\ \overline{h} = H$
- $d^\circ G = d^\circ g,\ d^\circ H = d^\circ h$
- $f = gh$.

Lemme de Hensel

Démonstration :

- On construit récursivement des représentants g_n, h_n de G, H, tels que $f - g_n h_n \in \mathfrak{m}_v^n[X]$.

Lemme de Hensel

Démonstration :

- On construit récursivement des représentants g_n, h_n de G, H, tels que $f - g_n h_n \in \mathfrak{m}_v^n[X]$.
- Par la complétude de K, on obtient g, h les limites simple des suites $(g_n), (h_n)$. Par construction $\overline{g} = G$, $\overline{h} = H$ et $f = gh$.

Lemme de Hensel

Démonstration :

- On construit récursivement des représentants g_n, h_n de G, H, tels que $f - g_n h_n \in \mathfrak{m}_v^n[X]$.
- Par la complétude de K, on obtient g, h les limites simple des suites $(g_n), (h_n)$. Par construction $\overline{g} = G$, $\overline{h} = H$ et $f = gh$.
- Le coefficient dominant de g vaut $1 + a$ avec $a \in \mathfrak{m}_v$. Remplaçons g par $(1 + a)^{-1} g$ et h par $(1 + a)h$, on obtient $f = gh$ avec g, h unitaires car f est unitaire.

Lemme de Hensel version faible

Corollaire (Lemme de Hensel version faible)

Soit f un polynôme unitaire dans $A_v[X]$ tel que le polynôme correspondant $\overline{f}$ admet une racine simple $a \in k_v$. Alors f admet une racine simple $b \in K$ telle que $\overline{b} = a$.

Lemme de Hensel version faible

Corollaire (Lemme de Hensel version faible)

Soit f un polynôme unitaire dans $A_v[X]$ tel que le polynôme correspondant $\overline{f}$ admet une racine simple $a \in k_v$. Alors f admet une racine simple $b \in K$ telle que $\overline{b} = a$.

Démonstration :

- $\overline{f}$ se décompose en $\overline{f} = (X - a)H$ avec $H(a) \neq 0$, donc $\exists g, h \in A_v[X]$ unitaires tels que $f = gh$, $d^\circ g = 1$.

Lemme de Hensel version faible

Corollaire (Lemme de Hensel version faible)

Soit f un polynôme unitaire dans $A_v[X]$ tel que le polynôme correspondant $\overline{f}$ admet une racine simple $a \in k_v$. Alors f admet une racine simple $b \in K$ telle que $\overline{b} = a$.

Démonstration :

- $\overline{f}$ se décompose en $\overline{f} = (X - a)H$ avec $H(a) \neq 0$, donc $\exists g, h \in A_v[X]$ unitaires tels que $f = gh$, $d^\circ g = 1$.
- On pose $g = X - b$, ainsi b est une racine de f et $\overline{b} = a$.

Lemme de Hensel version faible

Corollaire (Lemme de Hensel version faible)

Soit f un polynôme unitaire dans $A_v[X]$ tel que le polynôme correspondant $\overline{f}$ admet une racine simple $a \in k_v$. Alors f admet une racine simple $b \in K$ telle que $\overline{b} = a$.

Démonstration :

- $\overline{f}$ se décompose en $\overline{f} = (X - a)H$ avec $H(a) \neq 0$, donc $\exists g, h \in A_v[X]$ unitaires tels que $f = gh$, $d^\circ g = 1$.
- On pose $g = X - b$, ainsi b est une racine de f et $\overline{b} = a$.
- Si b était une racine de h, alors a serait une racine de H, absurde. Donc b est une racine simple de f.

Section 4

Unicité de valuation discrète sur un corps complet

Une valuation discrète est unique !

Théorème

Soit K un corps complet par rapport à une valuation discrète v, alors v est la seule valuation discrète surjective sur K.

Une valuation discrète est unique !

Théorème

Soit K un corps complet par rapport à une valuation discrète v, alors v est la seule valuation discrète surjective sur K.

Démonstration : (cas k_v algébriquement clos)

- Soit w une autre valuation discrète surjective, π une uniformisante de w.
  Par le lemme d'approximation, il existe $a \in K$ tel que $v(a-1) > 1$ et $w(a-\pi) > 1$. On a alors $v(a) = v(1) = 0$ et $w(a) = w(\pi) = 1$.

Une valuation discrète est unique !

- Si $\mathrm{char}(k_v) = p > 0$, on choisit $m > 1$ premier avec p, sinon un entier $m > 1$ suffit.
  On pose $f = X^m - a \in K[X]$, r une racine de $\overline{f}$.
  Si elle est multiple, alors $r = 0$ et $\overline{a} = 0$. Ce qui est absurde car on a déjà $v(a) = 0$ qui implique $a \notin \mathfrak{m}_v$.

Une valuation discrète est unique !

- Si $\mathrm{char}(k_v) = p > 0$, on choisit $m > 1$ premier avec p, sinon un entier $m > 1$ suffit.
  On pose $f = X^m - a \in K[X]$, r une racine de $\overline{f}$.
  Si elle est multiple, alors $r = 0$ et $\overline{a} = 0$. Ce qui est absurde car on a déjà $v(a) = 0$ qui implique $a \notin \mathfrak{m}_v$.
- r étant une racine simple, par le lemme de Hensel (version faible) on obtient $b \in A_v$ tel que $b^m = a$.
  Mais $m \cdot w(b) = w(b^m) = w(a) = 1$, contradiction.

Contre exemple

Nous illustrons un exemple de corps non complet de valuation qui admet des valuations discrètes non équivalentes.

Exemple

Soient $p \neq q \in \mathbb{N}$ premiers. On pose $a = \frac{p}{q} \in \mathbb{Q}$, alors $v_p(a) = 1$ et $v_q(a) = -1$.
Donc v_p et v_q ne sont pas équivalentes sur $\mathbb{Q}$.

L'hypothèse de la complétude est donc nécessaire.