Une valuation discrète est unique

Tsung-Hsuan TSAI Sarah TIMHADJELT

Résumé

Une valuation, ou valuation de Krull, est **une mesure de la multiplicité**. Cette notion est une généralisation de l'ordre d'annulation d'un polynôme en algèbre, du degré de divisibilité en théorie des nombres, ou de l'ordre d'un pôle en analyse complexe.

Le but de cet article est de démontrer que pour un **corps complet de valuation discrète**, une **valuation discrète est unique**.

On introduira d'abord la notion de valuation. Ensuite on aura besoin du **lemme d'approximation** et du **lemme de Hensel**, pour déduire le résultat final.

Table des matières

1 Généralité sur les valuations

1.1 Valuation

Pour un groupe abélien totalement ordonné $(G, +, <)$, on étend ses lois sur $G \cup \{\infty\}$ par :

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

Définition 1.1. *Soit $(K,+,\times)$ un corps commutatif et $(G,+,<)$ un groupe abélien totalement ordonné. On appelle* ***valuation*** *un morphisme de groupes $v : K^\times \to G$, avec $v(0) := \infty$, vérifiant $v(a+b) \geqslant \min\{v(a), v(b)\}\ \forall a, b \in K$. Si un corps K admet une valuation, on l'appelle* ***corps de valuation****.*

Exemple 1.1. 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 1.2. Soit $(A,+,\times)$ un anneau intègre commutatif et $(G,+,<)$ un groupe abélien totalement ordonné. Soit $v : A\backslash\{0\} \to G$ un morphisme de monoïde avec $v(0) := \infty$, vérifiant $v(a+b) \geqslant \min\{v(a), v(b)\}\ \forall a, b \in A$.

On note $F(A)$ le corps de fractions de A, alors v se prolonge naturellement en une valuation à $F(A)$ par $v(a/b) = v(a) - v(b)$. Il suffit de vérifier que $v(a_1/b_1 + a_2/b_2) = v(a_1b_2 + a_2b_1) - v(b_1b_2) = \min\{v(a_1b_2), v(a_2b_1)\} - v(b_1b_2) = \min\{v(a_1/b_1), v(a_2/b_2)\}$.

Soit $a, b \in K$, d'après la définition, on a directement :

- $v(1) = v(-1) = 0$
- $v(a) = v(-a)$
- $v(a-b) \geqslant \min\{v(a), v(b)\}$
- $v(a^m) = m \cdot v(a) \quad \forall m \in \mathbb{Z}$

Lemme 1.2. *Si $v(a) \neq v(b)$, alors $v(a+b) = \min\{v(a), v(b)\}$.*

Démonstration. Sans perte de généralité supposons que $v(a) < v(b)$. On a $v(a+b) \geqslant min\{v(a), v(b)\} = v(a)$. En plus $v(a) = v(a+b-b) \geqslant min\{v(a+b), v(b)\} = v(a+b)$, si $v(a+b) \geqslant v(b)$ alors $v(a) \geqslant v(b)$ absurde, donc $v(a+b) < v(b)$ et $v(a) \geqslant v(a+b)$. D'où l'égalité. □

On s'intérésse ensuite aux éléments de valuation supérieur à l'élément neutre 0 de G.

Définition 1.3. *$A_v := \{a \in K | v(a) \geqslant 0\}$ muni des opérations induites est un sous anneau de K. On l'appelle* ***anneau de valuation*** *associé à v.*

Si $a, b \in A_v$, alors $v(a-b) \geqslant \min\{v(a), v(b)\} \geqslant 0$, et $v(ab) = v(a) + v(b) \geqslant 0$. En plus $1 \in A_v$, ce qui justifie que A_v est un anneau.

Pour $a \in A_v$, on note (a) l'idéal de A_v engendré par a. On définit le produit des idéaux I et J comme l'idéal engendré par $\{ij | i \in I, j \in J\}$.

Lemme 1.4. *Soit $a \in A_v$. L'idéal engendré par a dans A_v s'écrit $(a) = \{b \in K | v(b) \geqslant v(a)\}$.*

Démonstration. Soit $b \in A_v$ tel que $v(b) \geqslant v(a)$. Le cas $a = 0$ est trivial. Si $a \neq 0$ on pose $c = ba^{-1}$. On a $v(c) \geqslant 0$, donc $b = ca$ avec $c \in A_v$, on a $b \in (a)$. Réciproquement si $b \in (a)$ alors $v(ba^{-1}) \geqslant 0$, donc $v(b) \geqslant v(a)$. Par conséquence, $\forall a \in A_v \quad v(b) \geqslant v(a) \iff b \in (a)$. □

Lemme 1.5. *$v(a) = 0$ si et seulement si a est inversible dans A_v.*

Démonstration. On remarque que $v(a^{-1}) = -v(a)$. Si $v(a) = 0$, alors $v(a^{-1}) = 0$, donc $a^{-1} \in A_v$, a est inversible dans A_v. Réciproquement si $v(a) \neq 0$, alors soit $a \notin A_v$, soit $a^{-1} \notin A_v$. Ainsi $v(a) = 0 \Leftrightarrow a \in A_v^\times$. □

De ce fait, $v(a) = v(b) \Leftrightarrow (a) = (b)$. On peut ainsi classifier les idéaux principaux de A_v :

Proposition 1.6. *Soit $\mathcal{I}$ l'ensemble des idéaux principaux de A_v, alors l'application*

$$\begin{array}{rccc} \Psi : & \mathcal{I} & \to & v(A_v) \\ & (a) & \mapsto & v(a) \end{array}$$

est une bijection.

Démonstration. Par l'équivalence $v(a) = v(b) \Leftrightarrow (a) = (b)$, Ψ est bien définie et injective. Elle est clairement surjective. □

Plus généralement, les éléments de K de valuation plus grand qu'un élément de G forme un idéal de A_v.

Lemme 1.7. *Soit $x \in G$ tel que $x \geqslant 0$. $I = \{a \in K | v(a) \geqslant (>)\, x\}$ est un idéal de A_v.*

Démonstration. Sachant que $x \geqslant 0$, on a $I \subset A_v$. Si $a, b \in I$, alors $v(a-b) \geqslant \min\{v(a), v(b)\} \geqslant (>)$ x ; si $a \in I, b \in A_v$, alors $v(ab) = v(a) + v(b) \geqslant (>)\, x$. I est un idéal de A_v. □

En plus, pour les idéaux $I = \{a \in K | v(a) \geqslant x\}$ et $J = \{a \in K | v(a) \geqslant y\}$, leur produit est $IJ = \{a \in K | v(a) \geqslant x + y\}$. Si l'un des inégalités de départ est stricte, alors l'inégalité finale est stricte. On voit bien que les idéaux de cette forme sont totalement ordonnée par l'inclusion, avec A_v le plus grand, et $\{a \in K | v(a) > 0\}$ le second.

Proposition 1.8. *A_v est un anneau local (i.e. anneau qui n'admet qu'un idéal maximal), avec l'idéal maximal $\mathfrak{m}_v := \{a \in K | v(a) > 0\}$.*

Démonstration. Par le lemme 1.7 $\mathfrak{m}_v$ est un idéal de A_v , en plus par le lemme 1.5 $A_v \backslash \mathfrak{m}_v = \{a \in K | v(a) = 0\} = A_v^\times$. $\mathfrak{m}_v$ est l'ensemble des non inversibles dans A_v. Un idéal propre I de A_v ne contient aucun élément inversible, donc $I \in \mathfrak{m}_v$. D'où $\mathfrak{m}_v$ est l'unique idéal maximal de A_v. □

On définit ainsi $k_v := A_v/\mathfrak{m}_v$ le corps résiduel associé. Pour un élément $a \in A_v$, on note $\overline{a} = a + \mathfrak{m}_v$ sa classe dans k_v. Pour un polynôme $f \in A_v[X]$, on note $\overline{f}$ le polynôme correspondant dans $k_v[X]$, i.e.

$$\text{pour} \quad f = \sum_{i=0}^{n} a_i X^i \quad \text{on note} \quad \overline{f} = \sum_{i=0}^{n} \overline{a_i} X^i$$

Pour un polynôme $F \in k_v$, on dit que $f \in A_v$ est un représentant de F si $\overline{f} = F$. On remarque que pour $F \in k_v$, on peut en choisir un représentant de même degré. Cette notion sera utile dans le chapitre 3.

1.2 Valuation discrète

Une valuation est dite **discrète** si son image de $K^\times$ est un groupe cyclique. Quitte à composer par l'isomorphisme de $v(K^\times)$ dans $\mathbb{Z}$, une valuation discrète se ramène à une application **surjective** $v : K \to \mathbb{Z} \cup \{\infty\}$. Si un corps K admet une valuation discrète, on l'appelle **corps de valuation discrète**. Dans ce cas A_v est appelé **anneau de valuation discrète** associé.

Un élément $\pi \in A_v$ est appelé une **uniformisante** si $v(\pi)$ engendre $v(K^\times)$ (qui n'existe que dans le cas discret). Pour une valuation discrète surjective, on a $v(\pi) = 1$. D'après le lemme 1.4 on a $(\pi) = \{a \in A_v | v(a) \geqslant 1\}$, qui coïncide avec $\mathfrak{m}_v = \{a \in A_v | v(a) > 0\}$.

Lemme 1.9. *Soit A un anneau principal et π un élément non nul non inversible. Alors qu'il n'existe pas d'élément non nul a qui puisse s'écrire $a = a_n\pi^n$ avec $a_n \in A$ pour tout $n \in \mathbb{N}$.*

Démonstration. L'ensemble $\bigcap_{n\in\mathbb{N}} (\pi^n)$ est un idéal comme intersection des idéaux. Désignons par c son générateur, on veut montrer que $c = 0$.

Pour tout $n \in \mathbb{N}$, on peut écrire $c = c_n\pi^n$ avec $c_n \in A$. Puisque $\pi \neq 0$, pour tout $n\mathbb{N}$, $c_1 = c_{n+1}\pi^n$, donc $c_1 \in (c)$. On peut alors écrire $c_1 = ac$ avec $a \in A$ si bien que $c_1 = c_1 a\pi$, donc $c_1(1 - a\pi) = 0$. Puisque π est non inversible, cela montre que $c = 0$. □

Proposition 1.10. *Une valuation v est discrète si et seulement si son anneau de valuation associé A_v est principal.*

Démonstration. Soit v une valuation discrète (surjective sur $\mathbb{Z}$). Soit I un idéal de A_v, on pose $a \in I$ tel que $v(a)$ soit minimal. On a déjà $(a) \subset I$. Pour $b \in I$, or $v(b) \geqslant v(a)$ donc $b \in (a)$. Ainsi $I = (a)$, A_v est principal.

Réciproquement si A_v est principal, on pose $\mathfrak{m}_v = (\pi)$. Soit $a \in A_v$, on pose $n = \sup\{n \in \mathbb{N} \mid \pi^n \text{ divise } a\}$. Puisque π est non inversible, par le lemme 1.9 si $n = \infty$ alors $a = 0$. Sinon on a $a = \pi^n a'$ avec $\pi \nmid a'$, i.e. $a' \notin (\pi) = \mathfrak{m}_v$, a' est inversible. Ainsi par lemme 1.5 $v(a) = n \cdot v(\pi)$. Pour $a \in K\backslash A_v$, or $a^{-1} \in A_v$ donc $\exists n \in \mathbb{N}$ $v(a) = -n \cdot v(\pi)$. Par conséquence, $\forall a \in K^\times \exists n \in \mathbb{Z}$ $v(a) = n \cdot v(\pi)$. Donc $v(K) = v(\pi)\mathbb{Z} \cup \{\infty\}$, v est discrète. □

Pour une valuation discrète, son anneau de valuation A_v n'admet que des idéaux principaux et $v(A_v) = \mathbb{N}$, donc par lemme 1.4, les ensembles $\{a \in K | v(a) \geqslant n\}$ avec $n \in \mathbb{N}$ sont **les idéaux** de A_v. Ils s'écrivent aussi $\mathfrak{m}_v^n$ ou $\pi^n A_v$.

Exemple 1.3. Soit p un nombre premier, $a \in \mathbb{Z}$ anneau des entiers. Or $\mathbb{Z}$ est factoriel, il existe $n \in \mathbb{N}$ tel que $a = p^n b$ où b est premier avec p. On définit l'ordre de divisibilité par p comme

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

On remarque que si $a = 0$ alors $v(a) = \infty$. Pour $a, b \in \mathbb{Z}$ on écrit $a = p^{v(a)}a'$ et $b = p^{v(b)}b'$ avec a', b' premier avec p. On vérifie que $v(ab) = v\left(p^{v(a)+v(b)}a'b'\right) = v(a) + v(b)$, et que si $v(a) \leqslant v(b)$ alors $v(a + b) = v\left(p^{v(a)}(a'p^{v(b)-v(a)} + b')\right) \geqslant v(a)$. Par l'exemple 1.2, v_p se prolonge en une valuation discrète à $\mathbb{Q}$, qui vérifie

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

La valuation v_p est appelée **valuation *p*-adique** de $\mathbb{Q}$. Dans ce cas $A_{v_p} = \{\frac{a}{b} \mid a, b \in \mathbb{Z}, p \nmid b\}$, $\mathfrak{m}_{v_p} = pA_{v_p}$, et $k_{v_p} \cong \mathbb{Z}/p\mathbb{Z}$.

Cette construction s'applique pour tout anneau factoriel avec un élément premier.

Exemple 1.4. Soit K un corps commutatif. X étant un élément premier de $K[X]$, l'ordre d'un polynôme $f = \sum_{n=0}^{N} a_n X^n \in K[X]$ défini par

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

se prolonge en une valuation au corps des fractions rationnelles $K(X)$. Dans ce cas $A_o = \{\frac{f}{g} \mid f, g \in K[X], g(0) \neq 0\}$, $\mathfrak{m}_o = XA_o$, et $k_o \cong K$.

2 Valeur absolue associée et Lemme d'approximation

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.

2.1 Lemme d'approximation pour les valeurs absolues

Définition 2.1. *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 on a $|x+y| \leqslant max(|x|, |y|)$ qui est une condition plus forte que $|x+y| \leqslant |x|+|y|$, cette valeur absolue $|\cdot|$ est dite **ultramétrique**.*

Exemple 2.1. 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 2.2. La valeur absolue sur $\mathbb{R}$ définie par :

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

est dite la valeur absolue usuelle.

La donnée d'une valeur absolue $|\cdot|$ sur un corps K nous permet de définir une distance $d : K \times K \to \mathbb{R}^+$ par $d(x, y) = |x - y|$ pour $x, y \in K$. On définit alors un espace métrique (K, d), il admet ainsi une topologie induite.

L'inégalité triangulaire implique que $||x| - |y||_{\mathbb{R}} \leqslant |x - y|$, c'est-à-dire $d_{\mathbb{R}}(|x|, |y|) \leqslant d(x, y)$ la valeur absolue est lipschitzienne donc continue.

On munit $K \times K$ de la topologie produit. On vérifie aisément que l'addition et le produit du corps sont des applications continues de $K \times K$ dans K. Ainsi le corps K muni de la topologie induite par une valeur absolue est un corps topologique.

Définition 2.2. *Deux valeurs absolues $|\cdot|_1, |\cdot|_2$ sur un corps K sont dites équivalentes si elles définissent la même topologie.*

On s'intéresse aux conditions nécessaires et suffisantes pour que deux valeurs absolues soient équivalentes.

Lemme 2.3. *Soient $|\cdot|_1, |\cdot|_2$ deux valeurs absolues non triviales sur un corps K,alors les assertions suivantes sont équivalentes :*

1. $|\cdot|_1, |\cdot|_2$ *sont équivalentes*
2. $\forall x \in K\ |x|_1 < 1 \Leftrightarrow |x|_2 < 1$
3. $\exists \alpha \geqslant 0\ \forall x \in K\ |x|_1 = |x|_2^\alpha$

Démonstration.

$1 \Rightarrow 2$: Si les deux valeurs absolues sont équivalentes et $|x|_1 < 1$, on a $x^n \xrightarrow{|\cdot|_1} 0$ donc $x^n \xrightarrow{|\cdot|_2} 0$ aussi. Ainsi $|x|_2^n \to 0$ et $|x|_2 < 1$, d'où $|x|_1 < 1 \Rightarrow |x|_2 < 1$. La réciproque est symétrique.

$2 \Rightarrow 3$: Remarquons que $|x|_1 > 1 \Leftrightarrow |x^{-1}|_1 < 1 \Leftrightarrow |x^{-1}|_2 < 1 \Leftrightarrow |x|_2 > 1$, en plus $|x|_1 = 1 \Leftrightarrow |x|_2 = 1$. La valeur absolue $|\cdot|_1$ étant non triviale, il existe $a \in K^\times$ telle que $|a|_1 < 1$, donc $|a|_2 < 1$. On pose $\alpha = \dfrac{\log|a|_1}{\log|a|_2} > 0$.

Soit $b \in K^\times$, on veut montrer que $|b|_1 = |b|_2^\alpha$. On distingue trois cas :

i. $|b|_1 = 1$, alors $|b|_2 = 1$, d'où $|b|_1 = |b|_2^\alpha$

ii. $|b|_1 < 1$, alors $|b|_2 < 1$. On pose $\beta_i = \dfrac{\log|a|_i}{\log|b|_i}$ pour $i = 1, 2$.

Si $\beta_1 < \beta_2$, il existe $r = \frac{m}{n} \in \mathbb{Q} \cap]\beta_1, \beta_2[$ par densité. On pose alors $x = a^n b^{-m} \in K^\times$, ainsi

$$\log|x|_i = n\log|a|_i - m\log|b|_i = n\log|b|_i(\beta_i - r) \quad \text{pour } i = 1, 2$$

Or $\log|b|_1 < 0$, $\log|b|_2 < 0$, $\beta_1 > r$ et $\beta_2 < r$, donc $\log|x|_1 < 0$ et $\log|x|_2 > 0$, ainsi $|x|_1 < 1$ et $|x|_2 > 1$, Contradiction.

Le même raisonnement s'applique en supposant $\beta_1 < \beta_2$. On en conclut que $\beta_1 = \beta_2$, soit $\dfrac{\log|b|_1}{\log|b|_2} = \dfrac{\log|a|_1}{\log|a|_2} = \alpha$, d'où $|b|_1 = |b|_2^\alpha$.

iii. Si $|b|_1 > 1$, alors $|b|_2 > 1$. On applique le raisonnement précédent à b^{-1}. Ainsi $|b^{-1}|_1 = |b^{-1}|_2^\alpha$, donc $|b|_1 = |b|_2^\alpha$.

$3 \Rightarrow 1$: Une boule ouverte pour la topologie induite par $|\cdot|_1$ (respectivement $|\cdot|_2$) est une boule ouverte pour la topologie induite par $|\cdot|_2$ (resp. $|\cdot|_1$). On a donc bien la double inclusions des deux topologies. □

Lemme 2.4. *Soient K un corps et $|\cdot|$ une valeur absolue sur K. Si $x \in K$ tel que $|x| \neq 1$, alors*

$$\frac{x^n}{1+x^n} \xrightarrow[n\to\infty]{|\cdot|} \begin{cases} 0 & \text{si} \quad |x| < 1 \\ 1 & \text{si} \quad |x| > 1 \end{cases}$$

Démonstration. $|x| \neq 1$, donc $1 + x^n$ ne s'annule pas, la fraction est bien définie. Si $|x| < 1$, $|x^n| = |x|^n \xrightarrow[n\to\infty]{} 0$. Par la continuité de la valeur absolue $x^n \xrightarrow[n\to\infty]{|\cdot|} 0$. Sachant que le corps est topologique, on a $\dfrac{x^n}{1+x^n} \xrightarrow[n\to\infty]{|\cdot|} 0$.

Si $|x| > 1$, alors $|x^{-1}| < 1$ donc $x^{-n} \xrightarrow[n\to\infty]{|\cdot|} 0$. Ainsi $\dfrac{x^n}{1+x^n} = \dfrac{1}{1+x^{-n}} \xrightarrow[n\to\infty]{|\cdot|} 1$. □

Soit K un corps. Le **lemme d'approximation** nous dit que pour les valeurs absolues $|\cdot|_1, ..., |\cdot|_J$ non équivalentes et les éléments $b_1, ..., b_J$ de K, on peut trouver un élément x de K qui approche b_j simultanément dans la topologie de $|\cdot|_j$, aussi proche que l'on veut. Afin de démontrer ce résultat, il nous faut un lemme intermédiaire :

Lemme 2.5. *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. Par récurrence sur J,

- $J = 2$: D'après le point 2 du lemme 2.3, sachant que $|\cdot|_1, |\cdot|_2$ non équivalentes et non triviales, on trouve $y \in K^\times$ 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 satisfait les conditions.
- $J > 2$: Par l'hypothèse de récurrence au rang $J-1$, on trouve $y \in K$ tel que $|y|_1 > 1$ et $|y|_j < 1$ pour $2 \leqslant j \leqslant J-1$. On trouve également $z \in K$ tel que $|z|_1 > 1$ et $|z|_J < 1$ par l'hypothèse au rang 2. On a alors 3 possibilités :
  i. Si $|y|_J < 1$, alors $x = y$ convient.
  ii. Si $|y|_J = 1$, alors la suite $|y^n z|_j \xrightarrow[n\to\infty]{} 0$ pour $2 \leqslant j \leqslant J-1$, on choisit $x = y^n z$ avec $n \in \mathbb{N}$ assez grand.
  iii. Si $|y|_J > 1$, alors par le lemme 2.4

$$\left|\frac{y^n}{1+y^n}\right|_j \xrightarrow[n\to\infty]{} \begin{cases} 0 & \text{si} \quad 2 \leqslant j \leqslant J-1 \\ 1 & \text{si} \quad j = 1, J \end{cases}$$

  Ainsi on pose $x = \dfrac{y^n}{1+y^n} z$ pour n assez grand, on obtient bien le résultat voulu. □

Théorème 2.6 (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. D'après le lemme 2.5, pour tout $j \in [\![1, J]\!]$ il existe $x_j \in K$ tel que $|x_j|_j > 1$ et $|x_j|_i < 1$ $\forall i \neq j$. On a alors $\lim\limits_{n\to\infty} \left|\dfrac{x_j^n}{1+x_j^n}\right|_j = 1$ et $\forall i \neq j$ $\lim\limits_{n\to\infty} \left|\dfrac{x_j^n}{1+x_j^n}\right|_i = 0$.

On pose alors $w_n = \sum\limits_{j=1}^{J} \dfrac{x_j^n}{1+x_j^n} b_j$, ainsi $\lim\limits_{n\to\infty} |w_n - b_j|_j = 0$. On choisit alors $x = w_n$ pour n assez grand. □

2.2 Valeur absolue associé à une valuation

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 d'Euler e peut être remplacée par un nombre réel strictement supérieur à 1. On définit ainsi des valeurs absolues équivalentes.

Exemple 2.3. La valeur absolue associé à la valuation p-adique sur $\mathbb{Q}$ est appelé **Valeur absolue p-adique**. Elle est conventionnellement définie comme :

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

On remarque alors que, pour la valuation triviale, on retrouve la valeur absolue triviale. On a en effet l'équivalence suivant :

Proposition 2.7. *Soit K un corps. Une application de K dans $\mathbb{R}$ est une valeur absolue associée à une valuation à valeurs réelles si et seulement si elle est une valeur absolue ultramétrique.*

Démonstration. Soit v une valuation de K à valeurs réelles. On vérifie que pour $x, y \in K$:

- $|x|_v = 0 \Leftrightarrow v(x) = \infty \Leftrightarrow x = 0$
- $|x+y|_v = e^{-v(x+y)} \leqslant e^{-\min\{v(x),v(y)\}} = \max\{e^{-v(x)}, e^{-v(y)}\} = \max\{|x|_v, |y|_v\}$
- $|xy|_v = e^{-v(xy)} = e^{-v(x)-v(y)} = |x|_v \cdot |y|_v$

Réciproquement soit $|\cdot|$ une valeur absolue ultramétrique sur K. On définit $v : K \to \mathbb{R} \cup \{\infty\}$ telle que $\forall a \in K$

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

On vérifie que pour $a, b \in K$

- $v(a) = \infty \Leftrightarrow |a| = 0 \Leftrightarrow a = 0$
- $v(a+b) = -\ln|a+b| \geqslant -\ln(\max\{|a|, |b|\}) = \min\{v(x), v(y)\}$
- $v(ab) = -\ln|ab| = -\ln|a| - \ln|b| = v(a) + v(b)$

On définit bien une valuation à valeurs dans le groupe totalement ordonné $(\mathbb{R}, +, <)$. □

Grâce à cette proposition, les résultats de valeurs absolues ultramétrique s'applique sur les valuations. Pour une valuation v, notons d_v la distance associée à sa valeur absolue associée. Cette distance vérifie donc $d_v(a,b) = e^{-v(a-b)}$. (K, d_v) est un espace ultramétrique. On dit que deux valuations sont équivalentes si elles définissent la même topologie.

Les deux corollaires suivants proviennent du lemme 2.3 et du théorème 2.6.

Corollaire 2.8. *Soient v, w deux valuations non triviales sur un corps K, alors les assertions suivantes sont équivalentes :*

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

Démonstration. On les identifie les points avec ceux du lemme 2.3.

1. Par la définition.
2. Soit $a \in K$. Si $a \neq 0$ alors $|a^{-1}|_v < 1 \Leftrightarrow |a^{-1}|_w < 1$, donc $|a|_v > 1 \Leftrightarrow |a|_w > 1$. Par les contrapositions $|a|_v \leqslant 1 \Leftrightarrow |a|_w \leqslant 1$, donc $v(a) \geqslant 0 \Leftrightarrow w(a) \geqslant 0$. D'où $A_v = A_w$.
3. Soit $\alpha \geqslant 0$ tel que $\forall a \in K\ |a|_v = |a|_w^\alpha$. Ainsi $\ln|a|_v = \alpha \ln|a|_w$, donc $v(a) = \alpha \cdot w(a)$. □

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

Corollaire 2.9. *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 $v_j(x - b_j) > c$.*

Démonstration. On pose $\epsilon = e^{-c} > 0$. Les valeurs absolues associées $|\cdot|_1, ..., |\cdot|_J$ sont non triviales non équivalentes, donc par le lemme d'approximation il existe $x \in K$ tel que $\forall j \in [\![1, J]\!]$ $|x - b_j|_j < \epsilon = e^{-c}$, donc $v_j(x - b_j) > c$. □

Comme une valuation définit un espace ultramétrique, on a :

Proposition 2.10. *Une suite (a_n) d'un corps de valuation K par rapport à v est de Cauchy si et seulement si $v(a_{n+1} - a_n) \xrightarrow[n\to\infty]{} \infty$.*

Démonstration. $v(a_{n+1} - a_n) \xrightarrow[n\to\infty]{} \infty$ si et seulement si $|a_{n+1} - a_n|_v \xrightarrow[n\to\infty]{} 0$. L'application directe est immédiate.

Réciproquement si $|a_{n+1} - a_n|_v \xrightarrow[n\to\infty]{} 0$, alors pour $\epsilon > 0$, $\exists n \in \mathbb{N}\ \forall p \geqslant n\ |a_{p+1} - a_p|_v < \epsilon$. Ainsi pour $q > p \geqslant n$, on a $|a_q - a_p|_v \leqslant \max\{|a_q - a_{q-1}|_v, \ldots, |a_{p+1} - a_p|_v\} < \epsilon$. D'où la suite (a_n) est de Cauchy. □

3 Corps complet et Lemme de Hensel

Un corps de valuation K est dit **complet** si la topologie associée à sa valuation v rend K un espace complet. Dans ce cas, K est appelé corps complet par rapport à la valuation v, ou un **corps complet de valuation**.

Une suite (a_n) d'un corps complet de valuation est convergente si et seulement si $v(a_{n+1} - a_n) \to \infty$, car elle est ainsi une suite de Cauchy.

Exemple 3.1. Soit $\mathbb{Q}$ muni de la valuation p-adique v_p. On définit $\mathbb{Q}_p$ la complété de $\mathbb{Q}$ par la distance associée à v_p. Ses éléments sont les classes d'équivalences des suites de Cauchy, où deux suites sont dites équivalentes si leur différence converge vers zéro. On prolonge v_p par continuité. Alors $\mathbb{Q}_p$ est un corps complet par rapport à la valuation v_p prolongée. On note souvent $\mathbb{Z}_p$ son anneau de valuation.

Exemple 3.2. Soit k un corps. L'anneau des séries formelles $K[[X]]$ muni de l'ordre comme l'exemple 1.4, s'étant sur le corps des séries formelles de Laurent $K((X))$ (qui est son corps de fraction) en un corps complet de valuation. Ce corps est en effet la complétion du corps $K(X)$.

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**. On introduit un lemme qui nous sert à démontrer le lemme de Hensel.

Lemme 3.1. *Soit k un corps, $G, H \in k[X]$ premiers entre eux. Alors pour $P \in k[X]$ tel que $d^\circ P \leqslant d^\circ G + d^\circ H$, il existe $V, W \in k[X]$ vérifiant $P = VG + WH$, $d^\circ V \leqslant d^\circ H$ et $d^\circ W \leqslant d^\circ G$.*

Démonstration. k est un corps donc $k[X]$ est un anneau euclidien par rapport au degré du polynôme. G et H sont premiers entre eux dans un anneau principal, d'après le théorème de Bézout on pose $V, W \in k[X]$ vérifiant $GV + HW = P$. Par la division euclidienne de V par H, on a $V = QH + V'$ avec $d^\circ V' < d^\circ H$. L'égalité dessus s'écrit $P = (V - QH)G + (W + QG)H = V'G + W'H$. En plus $d^\circ(W'H) = d^\circ(P - V'G) \leqslant \max\{d^\circ P, d^\circ V + d^\circ H\} \leqslant d^\circ G + d^\circ H$, donc $d^\circ W' \leqslant d^\circ G$. □

Théorème 3.2 (lemme de Hensel)**.** *Soit K un corps complet par rapport à une valuation discrète v. Soit f un polynôme unitaire dans $A_v[X]$ tel que le polynôme correspondant $\overline{f} \in k_v[X]$ se factorise comme $\overline{f} = GH$ avec G, H unitaire premiers entre eux dans $k_v[X]$. Alors il existe des polynômes unitaires g, h qui sont des représentants de même degrés de G, H tels que $f = gh$.*

Démonstration. Posons $r = d^\circ G$, $s = d^\circ H$, ainsi $d := d^\circ f = r + s$. Construisons récursivement pour $n \in \mathbb{N}$ des représentants g_n, h_n de même degrés de G, H, tels que $f - g_n h_n \in \mathfrak{m}_v^n[X]$.

Pour $n = 1$, on choisit $g_1, h_1 \in A_v[X]$ des représentants de même degrés de G, H. On a $f - g_1 h_1 \in \mathfrak{m}_v[X]$ car $\overline{f} = \overline{g_1}\,\overline{h_1}$.

Supposons que g_n, h_n déjà construit, de sorte que

$$f - g_n h_n = \sum_{i=0}^{d} c_i^n X^i \text{ avec } c_i^n \in (\pi^n)$$

Or G et H sont premiers entre eux, d'après le lemme 3.1, pour chaque $i \in [\![0, d]\!]$ il existe $V_i, W_i \in A_v[X]$ tels que $X^i = V_i G + W_i H$ avec $d^\circ V_i \leqslant s$ et $d^\circ W_i \leqslant r$. Posons v_i, w_i leur représentants de même degrés, ainsi dans A_v on a $X^i - v_i g_n - w_i h_n \in \mathfrak{m}_v[X]$. On pose

$$g_{n+1} = g_n + \sum_{i=0}^{d} c_i^n w_i,\ h_{n+1} = h_n + \sum_{i=0}^{d} c_i^n v_i$$

Or $c_i^n \in (\pi^n) \subset \mathfrak{m}_v$, donc $\overline{g_{n+1}} = \overline{g_n} = G$. Le coefficient de degré r de g_{n+1} est ainsi non nul, en plus pour tout i on a $d^\circ w_i \leqslant r$, donc $d^\circ g_{n+1} = r$. De même $\overline{h_{n+1}} = \overline{h_n} = H$ et $d^\circ h_{n+1} = s$. On vérifie que

$$f - g_{n+1}h_{n+1} = f - \left(g_n + \sum_{i=0}^{d} c_i^n w_i\right)\left(h_n + \sum_{i=0}^{d} c_i^n v_i\right)$$

$$= f - g_n h_n - \sum_{i=0}^{d} c_i^n (v_i g_n + w_i h_n) - \left(\sum_{i=0}^{d} c_i^n w_i\right)\left(\sum_{i=0}^{d} c_i^n v_i\right)$$

$$= \sum_{i=0}^{d} c_i^n (X^i - v_i g_n - w_i h_n) - \left(\sum_{i=0}^{d} c_i^n w_i\right)\left(\sum_{i=0}^{d} c_i^n v_i\right)$$

ce qui justifie que $f - g_{n+1}h_{n+1} \in (\pi^{n+1})[X]$ car $c_i^n \in (\pi^n)$ et $X^i - v_i g_n - w_i h_n \in (\pi)[X]$.

Pour chaque i on a $v(c_i^n) \geqslant n$, la série $\sum_{n \geqslant 1} c_i^n$ est convergente, soit c_i la somme. Comme $g_n = g_1 + \sum_{k=1}^{n-1} \sum_{i=0}^{d} c_i^k w_i = g_1 + \sum_{i=0}^{d} \sum_{k=1}^{n-1} c_i^k w_i$, on pose $g = g_1 + \sum_{i=0}^{d} c_i w_i$. Puisque $\mathfrak{m}_v = B_f(0, |\pi|)$ est un fermé, on a $c_i \in \mathfrak{m}_v$. Par conséquence $\overline{g} = \overline{g_1} = G$, de même $\overline{h} = H$. Par construction $f - g_n h_n \in (\pi^n)$, cette suite converge vers 0, donc $f = gh$. Le polynôme G étant unitaire, 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. □

Si on applique le lemme de Hensel aux cas où G est de degré 1, alors qu'on en obtient une version faible. Cette version est utile pour démontrer le résultat final.

Corollaire 3.3. *Soit f un polynôme unitaire dans $A_v[X]$ tel que le polynôme correspondant $\overline{f}$ admet une racine simple a. Alors f admet une racine simple b telle que $\overline{b} = a$.*

Démonstration. Soit K un corps complet par rapport à une valuation discrète v. a étant une une racine simple, $\overline{f}$ se décompose en $\overline{f} = (X - a)H$ avec $X - a$ et H premiers entre eux. Par la proposition 3.2 il existe $g, h \in A_v[X]$ unitaires tels que $f = gh$, $d^\circ g = 1$, $\overline{g} = X - a$ et $\overline{h} = H$. On pose $g = X - b$, ainsi b est une racine de f et $\overline{b} = a$. En plus si b était une racine de h, alors a serait une racine de H, absurde. Donc b est une racine simple de f. □

4 Unicité de valuation discrète sur un corps complet

Théorème 4.1. *Soit K un corps complet par rapport à une valuation discrète v, alors v est la seule valuation discrète surjective sur K.*

Le théorème s'applique sur tout corps complet de valuation discrète. Pour éviter de parler d'extensions du corps, on se restreint dans le cas où le corps résiduel k_v est algébriquement clos.

Démonstration. (cas k_v algébriquement clos) Soit w une autre valuation discrète surjective sur K distinct de v, soit 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 par le lemme 1.2 $v(a) = v(1) = 0$ et $w(a) = w(\pi) = 1$.

Si le caractéristique du corps résiduel $\mathrm{char}(k_v) = p > 0$, on choisit $m > 1$ un entier premier avec p, sinon un entier $m > 1$ suffit. On applique le lemme de Hensel au polynôme $f = X^m - a$, qui est dans $A_v[X]$ car $v(a) = 0$. Soit r une racine de $\overline{f}$ dans k_v. Si elle est multiple, alors $\overline{f}(r) = r^m - a = 0$ et $\overline{f}'(r) = mr^{m-1} = 0$. Sachant que $m \neq 0$ dans k_v, on a $r = 0$, donc $\overline{a} = 0$. Ce qui est absurde car $v(a) = 0$ implique $a \notin \mathfrak{m}_v$. r étant une racine simple, par le corolaire 3.3 on obtient $b \in A_v$ tel que $b^m = a$. Mais $m \cdot w(b) = w(b^m) = w(a) = 1$, contradiction. □

Exemple 4.1. Soient $p \neq q \in \mathbb{N}$ premiers. On pose $a = \frac{p}{q} \in \mathbb{Q}$, alors $v_p(a) = 1$ et $v_q(a) = -1$. Par le point 2 du corollaire 2.8 v_p et v_q ne sont pas équivalentes.

Nous illustrons un exemple de corps de valuation qui admet des valuations discrètes non équivalentes. L'hypothèse de la complétude est donc nécessaire.