Valuations discrètes

Soit $\mathbb{A} = (A, +, \cdot)$ un anneau commutatif. On considère le groupe abélien $(\overline{\mathbb{Z}}, +, >)$ totalement ordonné.
Une valuation discrète est une application $v : A \longrightarrow \overline{\mathbb{Z}}$ vérifiant :

- Valuation infinie : $\forall x \in A, \quad (\, v(x) = +\infty \iff x = 0_{\mathbb{A}} \,)$
- Produit : $\forall x, y \in A, \quad v(x\,y) = v(x) + v(y)$
- Somme : $\forall x, y \in A, \quad v(x+y) \geqslant \min\big(v(x), v(y)\big)$

On a alors les propriétés :

- $v(1_{\mathbb{A}}) = v(-1_{\mathbb{A}}) = 0$ (car $1_{\mathbb{A}} = 1_{\mathbb{A}} \cdot 1_{\mathbb{A}}$)
- $\forall x, y \in A : v(x) \neq v(y), \quad v_p(x+y) = \min\big(v(x), v(y)\big)$ (???)
- L'anneau $\mathbb{A}$ est nécessairement intègre (prop. sur le produit et valuation infinie)

Valuation p-adique sur $\mathbb{Q}$

Soit $p \in \mathbb{P}$. On considère la valuation p-adique $v_p = v_p^{(\mathbb{Z})} : \mathbb{Z} \longrightarrow \overline{\mathbb{N}}$. On l'étend sur $\mathbb{Q}$ par

$$\begin{array}{rccc} v_p = v_p^{(\mathbb{Q})} : & \mathbb{Q} & \longrightarrow & \overline{\mathbb{Z}} \\ & {}^{x}\!/_{y} & \longmapsto & v_p(x) - v_p(y) \end{array}$$

Elle est **bien définie** car indépendante du représentant :

Soit $r \in \mathbb{Q}$ et $r = {}^{x}\!/_{y} = {}^{u}\!/_{v}$ deux représentants. Alors $x\,v = y\,u$. Donc $v_p(x\,u) = v_p(x) + v_p(v)$ $= v_p(y\,u) = v_p(y) + v_p(u)$, donc $v_p({}^{x}\!/_{y}) = v_p(x) - v_p(y) = v_p(u) - v_p(v) = v_p({}^{u}\!/_{v})$.

De plus, elle **coïncide** avec la valuation p-adique de $\mathbb{Z}$:

$\forall x \in \mathbb{Z}$, $v_p^{(\mathbb{Q})}(\iota(x)) = v_p^{(\mathbb{Q})}({}^{x}\!/_{1}) = v_p^{(\mathbb{Z})}(x) - v_p^{(\mathbb{Z})}(1) = v_p^{(\mathbb{Z})}(x)$ avec $\iota : \mathbb{Z} \to \mathbb{Q}$ l'injection canonique.

On vérifie les **propriétés d'une valuation** :

- Valuation infinie : $\forall r \in \mathbb{Q}, \quad (\, v_p(r) = +\infty \iff r = 0_{\mathbb{Q}} \,)$
- Produit : $\forall r = {}^{x}\!/_{y}, s = {}^{u}\!/_{v} \in \mathbb{Q}, \quad v_p(r\,s) = v_p\big(\frac{x\,u}{y\,v}\big) = v_p(x\,u) - v_p(y\,v)$ (produit pour $v_p^{(\mathbb{Z})}$) $= v_p(x) + v_p(u) - (v_p(y) + v_p(v)) = v_p({}^{x}\!/_{y}) + v_p({}^{u}\!/_{v}) = v_p(r) + v_p(s)$.
- Somme : $\forall r = {}^{x}\!/_{y}, s = {}^{u}\!/_{v} \in \mathbb{Q}, \quad v_p(r+s) = v_p\big(\frac{x\,v + u\,y}{y\,v}\big) = v_p(x\,v + u\,y) - v_p(y\,v)$ $(v_p^{(\mathbb{Z})})$ $\geqslant \min\big(v_p(x\,v), v_p(u\,y)\big) - v_p(y\,v) = \min\big(\underbrace{v_p(x\,v) - v_p(y\,v)}_{= v_p\left(\frac{x\,v}{y\,v}\right) = v_p({}^{x}\!/_{y})}, \underbrace{v_p(u\,y) - v_p(y\,v)}_{= v_p\left(\frac{u\,y}{v\,y}\right) = v_p({}^{u}\!/_{v})}\big)$

  donc $v_p(r+s) \geqslant \min(v_p(r), v_p(s))$.

Elle vérifie aussi les propriétés :

- $\forall r \in \mathbb{Q}, \quad (\, r \in \mathbb{Z} \iff \forall p \in \mathbb{P},\ v_p(r) \geqslant 0 \,)$ (dénominateur $=1$)
- $\forall r \in \mathbb{Q}, \quad v_p(r^{-1}) = -v_p(r)$
- **Distance p-adique** sur $(\mathbb{Q}, +, \cdot_{\mathbb{Q}})$: $\forall r, s \in \mathbb{Q}, \quad d_p(r, s) := \mathrm{e}^{-v_p(r-s)}$ définit une distance (ultramétrique).

Anneau de valuation discrète de $\mathbb{Q}$

Soit $p \in \mathbb{P}$ fixé. On considère la valuation p-adique $v_p : \mathbb{Q} \longrightarrow \overline{\mathbb{Z}}$ sur l'anneau $(\mathbb{Q}, +, \cdot)$. On pose

$$A := \{r \in \mathbb{Q} : v_p(r) \geqslant 0\} = \left\{ \tfrac{x}{y}|_{\text{irr}} \in \mathbb{Q} : p \not| \, y \right\} = \left\{ \tfrac{x}{y} : x \in \mathbb{Z},\ y \in \mathbb{Z} \backslash p\mathbb{Z}?? \right\}$$

($\not|$ v $\equiv$ ne divise pas; valuation positive $\Leftrightarrow$ dénominateur du représentant irréductible non divisible par p).

On a que $\mathbb{A} := (A, +|_A, \cdot|_A)$ est un **sous-anneau** de $(\mathbb{Q}, +, \cdot)$:

- $1_{\mathbb{Q}} \in A$ car $v_p(1_{\mathbb{Q}}) = v_p(1/1) = 0 - 0 \geqslant 0$
- $\forall a, b \in A$, $v_p(a-b) \geqslant \min\big(\underbrace{v_p(a)}_{\geqslant 0}, \underbrace{v_p(b)}_{\geqslant 0}\big) \geqslant 0$ et $v_p(a \cdot b) = \underbrace{v_p(a)}_{\geqslant 0} + \underbrace{v_p(b)}_{\geqslant 0} \geqslant 0$
  donc $a - b \in A$ (sous-groupe) et $a \cdot b \in A$ (stable par multiplication).

De plus, il contient $\mathbb{Z}$: Si l'on note $\iota : \mathbb{Z} \hookrightarrow \mathbb{Q}$ l'injection canonique, $\forall x \in \mathbb{Z}$, $v_p(\iota(x)) = v_p^{(\mathbb{Z})}(x) \geqslant 0$ donc $\iota(x) \in A$. Donc $\iota(\mathbb{Z}) \subset A$.

On montre quelques propriétés, qui sont généralisables à tout anneau de valuation discrète.

Inversibles de $\mathbb{A}$:

- Soit $a \in A^\times$. Alors $\exists b \in A : a \cdot b = 1$. Or $v_p(1) = v_p(a\,b) = \overbrace{v_p(a)}^{\geqslant 0} + \overbrace{v_p(b)}^{\geqslant 0} = 0$ donc nécessairement $v_p(a) = v_p(b) = 0$.
- Réciproquement, soit $a \in A \backslash \{0\}$: $v_p(a) = 0$. Alors $v_p(\overbrace{a^{-1}}^{\mathbb{Q}\text{ corps}}) = -v_p(a) = 0 \geqslant 0$ donc $a^{-1} \in A$ donc a admet a^{-1} comme inverse dans A donc $a \in A^\times$.

$$\boxed{A^\times = \{r \in \mathbb{Q} : v_p(r) = 0\}} = \left\{ \tfrac{x}{y}|_{\text{irr}} \in \mathbb{Q} : p \not| \, x \text{ et } p \not| \, y \right\}$$

Théorème fondamental de l'arithmétique dans $\mathbb{A}$:

Soit $a \in A$. Alors on a l'unique décomposition :

$$\boxed{\exists! n \in \mathbb{N},\ \exists! u \in A^\times \quad : \quad a = p^n\, u}$$

Existence : posons $n = v_p(a) \in \mathbb{N}$ et $u = a\, p^{-n}$, alors $a = p^n\, u$ et $v_p(u) = v_p(a) + v_p(p^{-n}) = n - n = 0$ (car $v_p(p^{-n}) = -v_p(p^n) = -n$ par définition) donc $u \in A^\times$ par caractérisation des inversibles de $\mathbb{A}$.

Unicité : soient $n' \in \mathbb{N}$ et $u' \in A^\times$ tels que $p^{n'}\, u' = a = p^n\, u$, alors (puisque $v_p(u) = v_p(u') = 0$)

$$n' + 0 = v_p(p^{n'}) + v_p(u') = v_p(p^{n'}\, u') = v_p(a) = v_p(p^n\, u) = v_p(p^n) + v_p(u) = n + 0$$

donc $p^n\, u' = p^n\, u$ donc $p^n\,(u - u') = 0$ donc ($\mathbb{Q}$ intègre donc $\mathbb{A}$ intègre) $u = u'$.

Anneau principal :

Soit I un idéal de $\mathbb{A}$. Montrons que c'est un idéal principal. On peut supposer que c'est un idéal strict. Alors $\iota^{\leftarrow}(I)$ est un idéal de $\mathbb{Z}$, comme image réciproque d'idéal ($= I \cap \mathbb{Z}$ si on identifie $\mathbb{Z}$ dans $\mathbb{Q}$). Or les idéaux stricts de $\mathbb{Z}$ sont exactement les $\{d\mathbb{Z} : d \in \mathbb{Z}\}$, donc $\exists d \in \mathbb{Z} : \iota^{\leftarrow}(I) = d\mathbb{Z}$. Montrons que

$$I = \left\{\frac{x}{y} \in A : x \in I \cap \mathbb{Z}\right\} = dA$$

en identifiant $\mathbb{Z}$ dans $\mathbb{Q}$:

- Soit ${}^{x}/_{y} \in I$. Alors $x = y \cdot {}^{x}/_{y} \in I$ car I idéal. Or $x \in \mathbb{Z}$, donc $x \in I \cap \mathbb{Z} = d\mathbb{Z}$, donc ${}^{x}/_{y} \in dA$.
- Soit $a = d\frac{x}{y} \in dA$. Alors $d \in d\mathbb{Z} = I \cap \mathbb{Z} \subset I$ et ${}^{x}/_{y} \in A$ donc (puisque I idéal) $a = d\frac{x}{y} \in I$.

Ainsi, I est l'idéal engendré par d, donc c'est un idéal principal. Tout idéal de $\mathbb{A}$ est donc principal.

Cela donne une **caractérisation des idéaux** de $\mathbb{A}$:

Soit $I \neq \{0\}$ un idéal de $\mathbb{A}$. Puisque l'on est dans un anneau principal, $\exists a \in A : I = aA$. Alors par le théorème fondamental de l'arithmétique dans $\mathbb{A}$, $\exists n \in \mathbb{N}$, $\exists u \in A^{\times} : a = p^n u$. Donc $I = p^n uA = p^n A$, car $uA = A$ puisque u est inversible. Donc

$$\boxed{\text{Idéaux}(\mathbb{A}) \;=\; \{aA : a \in A\} \;=\; \{p^n A : n \in \mathbb{N}\} \cup \{\{0\}\}}$$

Idéal maximal unique :

(caractéristique des anneaux à valuation discrète)

$$\boxed{M := \{r \in \mathbb{Q} : v_p(r) > 0\}}$$

C'est un **idéal** de $\mathbb{A}$: M est un sous-groupe de $(A, +|_A)$ car non vide ($v_p({}^{p}/_{1}) = 1 > 0$ donc ${}^{p}/_{1} \in M$) et stable par addition : $\forall r, s \in M,\ v_p(r-s) \geqslant \min\big(\underbrace{v_p(r)}_{>0}, \underbrace{v_p(s)}_{>0}\big) > 0$

et M est stable par multiplication externe : $\forall r \in M,\ \forall a \in A,\ v_p(r \cdot a) = \underbrace{v_p(r)}_{>0} + \underbrace{v_p(a)}_{\geqslant 0} > 0$.

C'est un idéal **maximal** : on remarque que

$${}^{\complement}M = A \backslash M = \{r \in \mathbb{Q} : v_p(r) \geqslant 0 \text{ et } v_p(r) \neq 0\} = \{r \in \mathbb{Q} : v_p(r) = 0\} = A^{\times}$$

donc $\forall I \in \text{Ideal}(\mathbb{A}) : M \subset I$, on a soit $M = I$, soit $M \subsetneq I$ et alors $\varnothing \neq I \cap {}^{\complement}M = I \cap A^{\times}$ donc $I = A$ (si on ajoute un élément, c'est forcément un inversible).

C'est le **seul** idéal maximal : si I est un idéal strict de $\mathbb{A}$, alors $I \cap {}^{\complement}M = I \cap A^{\times} = \varnothing$ donc $I \subset M$.

De plus, puisque les idéaux stricts de $\mathbb{A}$ sont les $\{p^n A : n \in \mathbb{N}\}$, puisque $\forall n \in [\![2, \infty[\![$, $p^n A = p^{n-1} \cdot pA \subset pA$, l'idéal maximal M est nécessairement :

$$\boxed{M = pA}$$

Corps résiduel : (propriété universelle de $\mathbb{A}$)

On définit le corps résiduel comme le quotient par l'idéal maximal M :

$$K := {}^{A}\!/_{M} = {}^{A}\!/_{pA}$$

muni de la structure quotient $(K,+,\cdot)$ qui forme un *corps* puisque M est maximal. Montrons que

$$\boxed{({}^{A}\!/_{pA},+,\cdot) \;\cong\; ({}^{\mathbb{Z}}\!/_{p\mathbb{Z}},+,\cdot)}$$

Notons $\overline{\cdot}\colon \mathbb{Z} \twoheadrightarrow {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$ la projection canonique dans le corps $({}^{\mathbb{Z}}\!/_{p\mathbb{Z}},+,\cdot)$. Posons alors

$$\begin{array}{rccc} \phi : & A & \longrightarrow & {}^{\mathbb{Z}}\!/_{p\mathbb{Z}} \\ & {}^{x}\!/_{y} & \longmapsto & \overline{x}\cdot\overline{y}^{-1} \end{array}$$

C'est un morphisme d'anneau de $\mathbb{A}$ dans $({}^{\mathbb{Z}}\!/_{p\mathbb{Z}},+,\cdot)$:

- Bien défini : soit $a\in A$ et $a = {}^{x}\!/_{y} = {}^{u}\!/_{v}$ deux représentants, alors $x\,v = y\,u$, donc $\overline{x}\cdot\overline{v} = \overline{y}\cdot\overline{u}$, donc (corps) $\overline{x}\cdot\overline{y}^{-1} = \overline{u}\cdot\overline{v}^{-1}$, c'est à dire $\phi({}^{x}\!/_{y}) = \phi({}^{u}\!/_{v})$ par définition.
- $\phi(1_{\mathbb{A}}) = \phi({}^{1}\!/_{1}) = \overline{1}\cdot\overline{1}^{-1} = \overline{1}$
- $\forall a = {}^{x}\!/_{y}, b = {}^{u}\!/_{v} \in A,\quad \phi(a+b) = \phi\big(\frac{x\,v+u\,y}{y\,v}\big) = \overline{x\,v+u\,y}\cdot\overline{y\,v}^{-1} = \overline{x}\,\overline{v}\,\overline{v}^{-1}\,\overline{y}^{-1} + \overline{u}\,\overline{y}\,\overline{y}^{-1}\,\overline{v}^{-1} = \overline{x}\,\overline{y}^{-1} + \overline{u}\,\overline{v}^{-1} = \phi({}^{x}\!/_{y}) + \phi({}^{u}\!/_{v}) = \phi(a)+\phi(b)$ par distributivité dans ${}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$ et car $\overline{\cdot}$ morphisme
- $\forall a = {}^{x}\!/_{y},\, b = {}^{u}\!/_{v} \in A,\quad \phi(a\,b) = \phi\big(\frac{x\,u}{y\,v}\big) = \overline{x\,u}\cdot\overline{y\,v}^{-1} = (\overline{x}\,\overline{y}^{-1})\,(\overline{u}\,\overline{v}^{-1}) = \phi({}^{x}\!/_{y})\,\phi({}^{u}\!/_{v}) = \phi(a)\,\phi(b)$ car $\overline{\cdot}$ morphisme.

Son noyau est $\operatorname{Ker}\phi = M = pA$. En effet,

- $\forall p\,a \in pA,\quad \phi(p\,a) = \phi(\iota(p))\cdot\phi(a) = (\overline{p}\cdot\overline{1}^{-1})\cdot\phi(a) \overset{(p\equiv 0 \bmod p)}{=} \overline{0}\cdot\phi(a) = \overline{0}$. Donc $pA \subset \operatorname{Ker}\phi$.
- $\forall a = \frac{x}{y}|_{\text{irr}} \in \operatorname{Ker}\phi,\ \phi(a) = \overline{x}\cdot\overline{y}^{-1} = \overline{0}$ donc (intégrité d'un corps) $\overline{x} = \overline{0}$ ou $\overline{y} = \overline{0}$. Or ${}^{x}\!/_{y}$ est un représentant irréductive de a et $p \not| y$ par définition de A, donc $y \not\equiv 0 \bmod p$ donc $\overline{y} \neq \overline{0}$. Donc nécessairement $x \equiv 0 \bmod p$, donc $v_p(x) > 0$, donc $v_p({}^{x}\!/_{y}) > 0$, c'est à dire $a = {}^{x}\!/_{y} \in M$.

Factorisation canonique de ϕ par son noyau : en notant $\pi : A \twoheadrightarrow {}^{A}\!/_{pA}$ la projection canonique,

$$\begin{array}{ccc} A & \xrightarrow{\ \phi\ } & {}^{\mathbb{Z}}\!/_{p\mathbb{Z}} \\ \big\downarrow & \nearrow_{\exists!\,\overline{\phi}} & \\ {}^{A}\!/_{pA} & & \end{array} \qquad \text{tel que } \phi = \overline{\phi}\circ\pi$$

On veut montrer que le morphisme d'anneau $\overline{\phi}$ est une bijectif. Considérons le morphisme d'anneau $\varphi := \pi\circ\iota$, avec $\iota : \mathbb{Z} \hookrightarrow A$ l'injection canonique. On a alors $p\mathbb{Z} \subset \operatorname{Ker}\varphi$. En effet $\forall p\,x \in p\mathbb{Z},\ \varphi(p\,x) = (p\,{}^{x}\!/_{1}) \bmod pA = 0 \bmod pA$ car $p\,{}^{x}\!/_{1} \in pA$ donc $p\,\mathbb{Z} \subset \operatorname{Ker}$. Factorisation canonique de φ par $p\mathbb{Z}$:

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{\ \iota\ } & A \\ \big\downarrow{\scriptstyle \overline{\cdot}} & & \big\downarrow{\scriptstyle \pi} \\ {}^{\mathbb{Z}}\!/_{p\mathbb{Z}} & \xrightarrow{\ \exists!\,\overline{\varphi}\ } & {}^{A}\!/_{pA} \end{array} \qquad \text{tel que } \varphi = \pi\circ\iota = \overline{\varphi}\circ\overline{\cdot}$$

Montrons alors que $\overline{\varphi}$ est la bijection réciproque de $\overline{\phi}$. En effet, $\overline{\phi}\circ\overline{\varphi}\circ\overline{\cdot} = \overline{\phi}\circ\varphi = \overline{\phi}\circ\pi\circ\iota = \phi\circ\iota$. Or $\phi\circ\iota = \overline{\cdot}$ car $\forall x\in\mathbb{Z},\ \phi(\iota(x)) = \phi({}^{x}\!/_{1}) = \overline{x}\cdot\overline{1}^{-1} = \overline{x}$. Donc $\overline{\phi}\circ\overline{\varphi}\circ\overline{\cdot} = \overline{\cdot}$, donc par surjectivité de $\overline{\cdot}$,

$$\overline{\phi}\circ\overline{\varphi} = \mathrm{id}_{{}^{\mathbb{Z}}\!/_{p\mathbb{Z}}}$$

Donc $\overline{\phi}$ est nécessairement surjectif, donc bijectif car injectif ($\overline{\varphi}$ est bien sa bijection réciproque). Donc

$$\overline{\phi} \in \mathrm{Iso}\Big(({}^{A}\!/_{pA},+,\cdot),({}^{\mathbb{Z}}\!/_{p\mathbb{Z}},+,\cdot)\Big)$$