Stage

-

Autour de la factorisation de polynômes sur les corps complets

Par Dounia Darkaoui encadrée par Martin Weimann et Denis Simon

Avril - Juin 2024

Table des matières

Introduction

Ce stage est motivé par l'algorithme OM, un algorithme permettant de factoriser des polynômes dans les corps valués complets tels que les corps de nombres p-adiques, les corps de séries de Laurent ou leurs extensions finies. Cet algorithme, nommé en hommage à ses principaux artisans : Montes, Ore, Mac Lane, et Okutsu, est déterministe. Une de ses applications est le calcul de bases intégrales d'idéaux fractionnaires, ce qui permet de calculer des bases d'espaces de Riemann-Roch.

Pour comprendre l'utilité de se restreindre aux corps valués, on étudiera en Partie 1 les valuations, l'anneau associé à celles-ci et les normes qu'elles induisent. Soient (K, v) un corps valué, L une extension de K, w une valuation de L. On dit que w étend v si $w|_K = v$. Une notion importante étudiée dans ce mémoire est celle d'extension de valuation. En effet, ces extensions et les facteurs d'un polynôme dans le complété d'un corps valué sont en correspondance. La complétion est un outil important, on en parlera en Partie 2. On y verra le théorème suivant :

Théorème 0.1. *Soit $L = K[X]/f$, avec f irréductible et séparable. On note $f = f_1 \cdots f_r$, la factorisation de f dans le complété de K par v. Les extensions de la valuation v dans L sont en correspondance avec les facteurs de f.*

En Partie 3, nous introduirons le polygone de Newton d'un polynôme. Cela nous permet de comprendre que les valuations des coefficients d'un polynôme jouent un rôle important pour en déterminer l'irréductibilité. C'est aussi un outil de l'algorithme OM. Pour démontrer les propriétés du polygone de Newton, les extensions de valuation sont inévitables.

Dans la Partie 4, on considèrera des anneaux particuliers, qui sont les anneaux de Dedekind. C'est une notion plus générale que la principalité mais qui permet d'avoir un cadre plus large et d'être stable par fermeture intégrale dans une extension séparable et finie. Dans ces anneaux, on peut définir des valuations grâce à l'unicité et l'existence de la décomposition d'idéaux en produit d'idéaux premiers. En étudiant la décomposition d'un idéal premier dans une fermeture intégrale, on en déduit les extensions de la valuation qu'il induit.

Considérons A un anneau de Dedekind, par exemple $\mathbb{Z}$, et K son corps des fractions. Soient L une extension séparable finie de K, B la fermeture intégrale de A dans L et $\mathfrak{p}$ un idéal premier de A. Considérons la décomposition de l'idéal $\mathfrak{p}B$ dans B :

$$\mathfrak{p}B = \prod_{\mathfrak{q}} \mathfrak{q}^{e_{\mathfrak{q}}},$$

où les $e_{\mathfrak{q}}$ sont des entiers naturels tous nuls sauf un nombre fini. Les extensions de la valuation $\mathfrak{p}$-adique sur K sont données par le théorème suivant :

Théorème 0.2. *Soient $v_{\mathfrak{p}}$ la valuation associée à $\mathfrak{p}$ dans A et $f \in K[X]$ tel que $L = K[X]/f$. Si $f = f_1 \cdots f_r$ est la factorisation de f dans le complété de K pour $v_{\mathfrak{p}}$, chaque facteur de f correspond à un idéal $\mathfrak{q}$ au dessus de $\mathfrak{p}$, i.e., $e_{\mathfrak{q}} > 0$.*

Ce résultat met en évidence le lien entre la factorisation d'un polynôme dans un complété et la factorisation d'un idéal premier dans une fermeture intégrale.

On souhaite calculer des bases intégrales triangulaires d'idéaux fractionnaires pour faciliter le calcul de bases de Riemann-Roch. C'est le sujet de la Partie 5. On aura besoin de semi-valuation et de trouver des éléments minimaux selon ces semi-valuations. L'algorithme OM nous permet de les obtenir. On se contentera de donner les fondations du raisonnement.

1 Corps valués

On expliquera dans cette partie ce qu'est une valuation sur un corps, les objets qui en découlent et les différents types de valuations.

1.1 Valuations et anneaux de valuation

Définition 1.1. *Une valuation sur un corps K est une application surjective $v : K \to \Gamma \cup \{\infty\}$ avec Γ un groupe abélien totalement ordonné et telle que $\forall x, y \in K$,*

1. $v(x) = +\infty \iff x = 0$,
2. $v(xy) = v(x) + v(y)$,
3. $v(x + y) \geqslant \min(v(x), v(y))$.

On dira que (K, v) est un corps valué avec Γ son groupe de valuation. On notera Γ_v le groupe de valuation de v.

Définition 1.2. *Soit Γ un groupe abélien totalement ordonné. Un sous-groupe Δ de Γ est convexe si pour tout $a \in \Gamma$ on a*

$$0 \leqslant a \leqslant b \text{ et } b \in \Delta \implies a \in \Delta.$$

Le rang de Γ est le nombre de sous-groupes convexes propres de Γ. Le rang d'une valuation est le rang de son groupe de valuation.

Proposition 1.3. *Une valuation est de rang 1 si et seulement si son groupe de valuation est isomorphe (en respectant l'ordre) à un sous-groupe non trivial de $(\mathbb{R}, +)$.*

Définition 1.4. *Une valuation est dicrète si son groupe de valuation est discret.*

Exemple 1.5. *Soit K un corps.*

1. *L'application $v : K \to \{0, \infty\}$ définie par $v(x) = 0$ pour tout $x \in K^*$ et $v(0) = \infty$ est une valuation dite triviale.*
2. *Soit p un nombre premier. On définit l'application $v_p : \mathbb{Q} \to \mathbb{Z}$ par $v_p(\frac{a}{b}) = ord_p(a) - ord_p(b)$ pour tout $a, b \in \mathbb{Z} \times \mathbb{N}^*$, où $ord_p(a)$ est la plus grande puissance de p divisant a. C'est une valuation dite p-adique.*
3. *Soit P un polynôme irréductible sur $K[X]$. L'application v_P est une valuation sur $K(X)$, définie comme précédemment par $v_P(\frac{A}{B}) = ord_P(A) - ord_P(B)$ pour $A, B \in K[X]$ et $B \neq 0$.*
4. *Sur $K(X)$, l'application $-\deg$ est une valuation.*

Remarque 1.6. *Ce sont toutes des valuations discrètes de rang 1.*

Exemple 1.7. *On considère le corps $L = k(t, s)$, avec un k un corps fini ou le corps des rationnels par exemple, muni de la valuation w définie sur $k[t, s]$ par :*

$$w\left(\sum_{i,j} a_{i,j} s^i t^j\right) = \min_{i,j}((i, j), a_{i,j} \neq 0).$$

Le groupe de valuation de w est $\mathbb{Z}^2$ muni de l'ordre lexicographique et son corps résiduel est k. La valuation v est dicrète de rang 2.

On a une notion d'équivalence de valuations.

Définition 1.8. *On dit que deux valuations v et w sur un corps K sont équivalentes s'il existe un isomorphisme ordonné $\gamma : \Gamma_v \to \Gamma_w$ tel que $w = \gamma \circ v$.*

Remarque 1.9. *Une valuation discrète de rang 1 est toujours équivalente à une valuation à valeurs dans* $\mathbb{Z}$.

Définition 1.10. *Un anneau de valuation d'un corps* K *est un anneau* $\mathscr{O} \subset K$ *tel que* $\forall x \in K^*$, *on a* $x \in \mathscr{O}$ *ou* $x^{-1} \in \mathscr{O}$.

Proposition 1.11. *Soit* (K, v) *un corps valué.*

- *L'anneau* $\mathscr{O}_v := \{x \in K \mid v(x) \geqslant 0\}$ *est un anneau de valuation.*
- *Son groupe des unités est* $\mathscr{O}_v^* = \{x \in K \mid v(x) = 0\}$.
- *L'ensemble* $\mathfrak{m}_v := \{x \in K \mid v(x) > 0\}$ *est l'unique idéal maximal de* $\mathscr{O}_v$. *En particulier,* $\mathscr{O}_v$ *est un anneau local.*

Proposition 1.12. *En gardant les notations précédentes, on a pour tout* $x \in K$:

$$x \in \mathfrak{m}_v \Leftrightarrow x^{-1} \notin \mathscr{O}_v.$$

Exemple 1.13. *Les anneaux de valuation correspondant aux valuations de l'Exemple 1.5 sont*

1. *Pour la valuation triviale, on a* $\mathscr{O}_v = K$
2. *Pour* p *un premier,* $\mathscr{O}_{v_p} = \{\frac{a}{b} \mid a, b \in \mathbb{Z} \times \mathbb{N}^*, p \nmid b\}$ *est l'anneau de valuation de* v_p *sur* $\mathbb{Q}$.
3. *De même,* $\mathscr{O}_{v_P} = \{\frac{A}{B} \mid A, B \in K[X], P \nmid B\}$ *est l'anneau de valuation de* v_P *dans* $K(X)$.
4. *Quant à l'anneau de la valuation* $-\deg$ *sur* $K(X)$, *on a* $\mathscr{O}_{-\deg} = K[X^{-1}]_{(X^{-1})}$. *Démontrons cette égalité. Soient* $P, Q \in K[X]$ *tels que* $\deg(Q) - \deg(P) \geqslant 0$. *On note* $P = \sum_{i=0}^{n} a_i X^i$ *et* $Q = \sum_{i=0}^{m} b_i X^i$ *avec* $a_n b_m \neq 0$. *On a*

$$\frac{P}{Q} = X^{n-m} \left(\sum_{i=0}^{n} a_i X^{i-n} \right) \left(\sum_{i=0}^{m} b_i X^{i-m} \right)^{-1}.$$

Comme $n - m \leqslant 0$, *le premier terme appartient à* $K[X^{-1}]$. *Le deuxième appartient clairement à* $K[X^{-1}]$. *Puisque* $b_m \neq 0$, *on a* $\sum_{i=0}^{m} b_i X^{i-m} \notin X^{-1}K[X^{-1}]$ *donc* $\frac{P}{Q} \in K[X^{-1}]_{(X^{-1})}$. *Ce qui démontre l'inclusion* $\mathscr{O}_{-\deg} \subset K[X^{-1}]_{(X^{-1})}$.
Montrons l'inclusion inverse. Soient $P \in K[X^{-1}]$ *et* $Q \in K[X^{-1}] \setminus X^{-1}K[X^{-1}]$. *Notons* $P = \sum_{i=0}^{n} a_i X^{i-n}$ *et* $Q = \sum_{i=0}^{m}$. *On a* $b_m \neq 0$, *car* Q *n'est pas divisible par* X^{-1}. *Cela nous donne*

$$\begin{aligned} \frac{P}{Q} &= \frac{X^{\max(n,m)}}{X^{\max(n,m)}} \frac{\sum_{i=0}^{n} a_i X^{i-n}}{\sum_{i=0}^{m} b_i X^{i-m}} \\ &= \frac{\sum_{i=0}^{n} a_i X^{i+\max(n,m)-n}}{\sum_{i=0}^{m} b_i X^{i+\max(n,m)-m}}. \end{aligned}$$

Le numérateur est de degré au plus $\max(n, m)$ *et le dénominateur est de degré exactement* $\max(n, m)$ *donc* $\deg(P/Q) \leqslant 0$. *On obtient bien l'inclusion voulue.*

Un ensemble important dans le cadre des valuations est le corps résiduel.

Définition 1.14. *Le quotient* $\mathscr{O}_v/\mathfrak{m}_v$ *est le corps résiduel de* (K, v), *souvent noté* κ_v.

En fait, on a correspondance entre les anneaux de valuation et les anneaux associés à une valuation.

Proposition 1.15. *Soit* $\mathscr{O} \subset K$ *un anneau de valuation. Il existe une valuation* v *de* K *telle que* $\mathscr{O} = \mathscr{O}_v$.

Démonstration. On note $\mathscr{O}^*$ le groupe des unités de $\mathscr{O}$ et on considère le groupe quotient

$$\Gamma := K^*/\mathscr{O}^*$$

avec la loi $x\mathscr{O}^* + y\mathscr{O}^* = xy\mathscr{O}^*$. On considère la relation

$$x\mathscr{O}^* \leqslant y\mathscr{O}^* \Leftrightarrow \frac{y}{x} \in \mathscr{O}.$$

C'est une relation d'ordre totale car $\mathscr{O}$ est un anneau de valuation. On considère la valuation $v : K \to \Gamma \cup \{\infty\}$ telle que

$$v(x) = \begin{cases} x\mathscr{O}^*, & \text{si } x \in K^*; \\ \infty, & \text{si } x = 0. \end{cases}$$

On a directement $v(xy) = v(x) + v(y)$. Montrons le point 3 de la Définition 1.1. Supposons que $v(x) \leqslant v(y)$. On a alors $y/x \in \mathscr{O}$ et donc $(x+y)/x = 1 + y/x \in \mathscr{O}$. Cela donne $v(x+y) \geqslant v(y) = \min(v(x), v(y))$. On obtient que v est bien une valuation sur K et, comme $v(1) = 0$, on a $\mathscr{O}_v = \mathscr{O}$. □

Corollaire 1.16. *Les anneaux de valuation sont des anneaux locaux, i.e., possédant un unique idéal maximal.*

Pour montrer que deux valuations sont équivalentes, il suffit de connaître leur anneau de valuation.

Proposition 1.17. *Deux valuations de K sont équivalentes si et seulement si elles ont le même anneau de valuation.*

Proposition 1.18. *Soient $\mathscr{O}$ et $\mathscr{O}'$ deux anneaux de valuation sur un corps K avec les idéaux maximaux respectifs $\mathfrak{m}$ et $\mathfrak{m}'$. Alors $\mathscr{O} = \mathscr{O}'$ si et seulement si $\mathfrak{m} = \mathfrak{m}'$.*

Démonstration. Cela vient de $x \notin \mathscr{O}$ si et seulement si $x^{-1} \in \mathfrak{m}$. □

1.2 Cas des corps de fonctions

On va s'intéresser dans cette partie aux valuations sur les corps de fonctions.

Définition 1.19. *Un corps de fonctions algébriques d'une variable sur K est une extension algébrique finie F de $K(x)$, où $x \in F$ est transcendant sur K.*

On note $\tilde{K}$ le corps des éléments de F algébriques sur K, appelé le corps des constantes.

Lemme 1.20. *Soit $\mathscr{O}$ un anneau de valuation de F tel que $K \subset \mathscr{O}$. Alors $\tilde{K} \subset \mathscr{O}$ et $\tilde{K} \cap P = \{0\}$, où P est l'idéal maximal de $\mathscr{O}$. Autrement dit $\mathscr{O}$ est l'anneau de valuation d'une valuation v, où v est triviale sur $\tilde{K}$.*

En considérant les anneaux des valuations triviales sur K, on obtient qu'ils proviennent de valuations discrètes et de rang 1.

Proposition 1.21. *Soient $\mathscr{O}$ un anneau de valuation du corps de fonctions F et P son idéal maximal. Alors on a :*

1. *P est un idéal principal.*
2. *Si $P = t\mathscr{O}$, alors pour tout $z \in F$ non nul, on a une unique représentation de la forme $z = t^n u$ pour $n \in \mathbb{Z}$ et $u \in \mathscr{O}^*$. L'élément t est appelé une uniformisante de P.*
3. *$\mathscr{O}$ est un anneau principal. Plus précisément, pour $P = t\mathscr{O}$ et $I \subset \mathscr{O}$ un idéal, on a $I = t^n\mathscr{O}$ pour un certain $n \in \mathbb{N}$.*

Pour démontrer cette proposition, on utilise le lemme suivant :

Lemme 1.22. *Soient $\mathscr{O}$ un anneau de valuation du corps de fonctions algébriques, P son idéal maximal et x un élément de P non nul. Supposons qu'il existe des élements $x_1, \dots, x_n \in P$ tels que $x_1 = x$ et $x_i \in x_{i+1}P$ pour $i = 1, \dots, n-1$. On a alors*

$$n \leqslant [F : K(x)] < \infty.$$

Démonstration. On sait que $F/K(x)$ est une extension finie car $x \notin \tilde{K}$ d'après le Lemme 1.20 et car le degré de transcendance de F/K est égal à 1. Montrons que $x_1, \dots, x_n$ sont indépendants sur $K(x)$. Supposons qu'il existe une combinaison linéaire

$$\sum_{i=1}^{n} \varphi_i(x) x_i = 0,$$

avec $\varphi_i(x) \in K(x)$. On peut supposer que les φ_i sont des polynômes en x et tels que x ne divise pas tous les φ_i. Posons $a_i := \varphi_i(0)$ le terme constant de $\varphi_i(x)$. On définit $j \in \{1, \dots, n\}$ par $a_j \neq 0$ et $a_i = 0$ pour tout $i > j$. On obtient :

$$-\varphi_j(x) x_j = \sum_{i \neq j} \varphi_i(x) x_i.$$

Or, $\varphi_i(x) \in \mathscr{O}$ car $x \in P$. D'après les hypothèses, $x_i \in x_j P$ pour $i < j$ et $\varphi_i(x) = x g_i(x)$ pour $i > j$, où $g_i(x)$ est un polynôme en x. On peut alors réécrire l'égalité précédente comme suit :

$$-\varphi_j(x) = \sum_{i<j} \varphi_i(x) \frac{x_i}{x_j} + \sum_{i>j} \frac{x}{x_j} g_i(x) x_i.$$

Cela montre que $\varphi_j(x) \in P$. On a $\varphi_j(x) = a_j + x g_j(x)$ avec $g \in K[x] \subset \mathscr{O}$, donc $a_j \in P \cap K$. Comme $a_j \neq 0$, cela contredit le Lemme 1.20 □

Démonstration. Démontrons l'affimation 1. de la Proposition 1.21. Supposons par l'absurde que P n'est pas principal et prenons $x_1 \in P$ non nul. Il existe $x_2 \in P \setminus x_1 \mathscr{O}$. Comme $x_2 x_1^{-1} \notin \mathscr{O}$, on a $x_2^{-1} x_1 \in P$ donc $x_1 \in x_2 P$. De la même manière pour $x_i \in P$ on peut construire x_{i+1} tel que $x_i \in x_{i+1} P$. Par induction, on obtient une suite infinie $x_1, x_2, x_3, \dots$ dans P telle que $x_i \in x_{i+1} P$ pour tout $i \geqslant 1$. C'est impossible d'après le lemme précédent.

□

Dans l'Exemple 1.5.3, la valuation v_Q sur $K(X)$ est triviale sur K et une uniformisante de son idéal maximal est Q.

Corollaire 1.23. *Tout anneau de valuation d'un corps de fonctions algébriques qui contient K provient d'une valuation discrète et de rang 1.*

1.3 Normes et valuations

Dans cette partie, on va normer des corps valués pour pouvoir considérer leur complété. Pour cela, on se contente des valuations de rang 1 que l'on suppose à valeurs dans $\mathbb{R}$.

Définition 1.24 (Norme)**.** *Soit K un corps. On appelle $|.| : K \to \mathbb{R}$ une norme de K si $|.|$ vérifie :*

- *$|x| \geqslant 0$ pour tout $x \in K$ et $|x| = 0 \iff x = 0$.*
- *$|xy| = |x||y|$ pour tout $x, y \in K$.*
- *$|x + y| \leqslant |x| + |y|$ pour tout $x, y \in K$.*

Définition 1.25. *On dit que la norme est non archimédienne si $|n|$ reste bornée pour tout $n \in \mathbb{N}$. Dans le cas contraire, on dit que la norme est archimédienne.*

Proposition 1.26. *La norme est non archimédienne si et seulement si elle vérifie l'inégalité ultramétrique : $|x+y| \leqslant \max(|x|,|y|)$ pour tout $x, y \in K$.*

Démonstration. La réciproque est évidente. On note N une borne de $|\mathbb{N}|$. Soient $x, y \in K$ tels que $|x| \geqslant |y|$. Alors $|x|^e|y|^{n-e} \leqslant |x|^n$ pour $0 \leqslant e \leqslant n$. On obtient que

$$|x+y|^n \leqslant \sum_{e=0}^{n} |\binom{e}{n}||x|^e|y|^{n-e} \leqslant N(n+1)|x|^n.$$

Donc $|x+y| \leqslant N^{1/n}(1+n)^{1/n}|x| = N^{1/n}(1+n)^{1/n}\max(|x|,|y|)$, et en prenant la limite de n en $+\infty$, on trouve bien l'inégalité voulue. □

Exemple 1.27. *La valeur absolue réelle est archimédienne.*

On note $|x|_p = p^{-v_p(x)}$ la norme p-adique qui est une norme non archimédienne.

Définition 1.28. *Deux normes sont équivalentes sur K si elles définissent la même topologie.*

Proposition 1.29. *Deux normes $|.|_1$ et $|.|_2$ sont équivalentes sur K si et seulement s'il existe $s > 0$ tel que $|x|_1 = |x|_2^s$ pour tout $x \in K$.*

On pose E l'ensemble des classes d'équivalence des valuations par la Définition 1.8 et F l'ensemble des classes d'équivalence des normes non archimédiennes par l'équivalence de la Définition 1.28.

Proposition 1.30. *On a une bijection entre E et F. La bijection est donnée par $[v] \in E \mapsto [\alpha^{-v(.)}] \in F$ où $\alpha > 1$.*

On peut donc donner la notation suivante :

Définition 1.31. *Soit (K, v) un corps valué, supposons que v est discrète. On note K_v le complété de K par la topologie induite par une norme associée à la valuation v.*

On verra dans la sous-partie 2.1 l'existence du complété pour une valuation. Ce complété ne dépend que de la classe d'équivalence de la valuation, tout comme le complété d'un espace normé ne dépend que de la classe de la norme.

Le complété de $\mathbb{Q}$ par la norme p-adique est le corps $\mathbb{Q}_p$. Le complété de $\mathbb{F}_p(X)$ pour la valuation v_X est le corps des séries de Laurent en X à coefficients dans $\mathbb{F}_p$, noté $\mathbb{F}_p[[X]]$.

Théorème 1.32 (Théorème d'Ostrowski)**.** *Soit $|\ |$ une norme non triviale sur $\mathbb{Q}$, où la norme triviale vérifie $|x| = 0$ si $x = 0$ et $|x| = 1$ sinon. On a*

- *S'il existe un entier n tel que $0 < |n| < 1$, alors il existe un nombre premier p et un réel a, tels que $0 < a < 1$ et pour tout $x \in \mathbb{Q}^*$, $|x| = a^{v_p(x)}$.*
- *Sinon, il existe α réel tel que $0 < \alpha \leqslant 1$ et pour tout $x \in \mathbb{Q}$, $|x| = |x|_\infty^\alpha$.*

Démonstration. Il suffit de montrer les égalités sur $\mathbb{N}$ et on peut alors étendre sur $\mathbb{Q}$.

- Soit $n \in \mathbb{N}$ tel que $0 < |n| < 1$. Il existe alors p premier divisant n tel que $0 < |p| < 1$ par multiplicativité de la norme.

  Montrons que pour $b \in \mathbb{N}$, on a $|b| \leqslant 1$. On écrit b en base p, $b = b_0 + b_1 p + \cdots + b_h p^h$, alors $|b| \leqslant (1+h)M$, où $M = \sup(1, |2|, \ldots, |p-1|)$. De même, pour les puissances de b on note h_k la plus grande puissance de p dans le développement en base p de b^k. On obtient

$|b|^k \leqslant (1+h_k)M$. On pose $B = \ln(b)/\ln(p)$, on a $h_k \leqslant kB$. Ce qui donne $|b| \leqslant M^{1/k}(1+kB)^{1/k}$ pour tout $k \geqslant 1$. En faisant tendre k vers $+\infty$, on obtient $|b| \leqslant 1$.

En utilisant cela, on montre que si q est premier avec p, alors $|q| = 1$. Pour tout $k \in \mathbb{N}^*$, il existe u_k et v_k des entiers tels que $u_k p^k + v_k q^k = 1$ et on a alors

$$1 = |1| \leqslant |u_k||p^k| + |v_k||q^k| \leqslant |p|^k + |q|^k.$$

Si on avait $|q| < 1$, à partir d'un certain rang le membre de droite serait strictement inférieur à 1, ce qui est impossible.

Grâce à la décomposition en nombres premiers et en posant $a = |p|$, on obtient bien le résultat attendu.

— Dans le second cas, on veut montrer que $\ln(|x|)/\ln(x)$ est constant sur $\mathbb{N} \setminus \{0, 1\}$. D'abord, si $a \in \mathbb{N}$ tel que $a > 1$, on a $|a| \geqslant 1$, en réalité on a même $|a| > 1$. En effet en reprenant le calcul fait dans la première partie pour $|p| < 1$ on aboutirait à la trivialité de la norme. Posons $\alpha = \ln(|a|)/\ln(a)$ pour un tel entier $a > 1$. On peut facilement montrer que $0 < \alpha < 1$. On prend $c > 1$ un entier et on écrit c^k en base a, on a alors

$$|c|^k \leqslant M\frac{|a|^{h_k+1} - 1}{|a| - 1},$$

où $M = \sup(1, |2|, \ldots, |a-1|)$. Or, $|h_k| \leqslant kC$, avec $C = \ln(c)\ln(a)$. On a donc

$$|c| \leqslant M^{1/k}(\frac{|a|^{Ck+1} - 1}{|a| - 1})^{1/k}.$$

En faisant tendre k vers $+\infty$, on obtient $|c| \leqslant |a|^C = c^\alpha$. Cela donne $\ln(|c|)/\ln(c) \leqslant \ln(|a|)/\ln(a)$. Par symétrie, on obtient la réciproque et on peut donc retrouver le résultat souhaité.

□

Les seules normes non archimédiennes de $\mathbb{Q}$ sont de la forme $|.| = a^{v_p(.)}$, avec $0 < a < 1$ donc les seules valuations non-triviales de $\mathbb{Q}$ sont les valuations p-adiques (à équivalence près). En effet, pour p et q deux nombres premiers différents, les valuations v_p et v_q ne sont pas équivalentes.

De plus, le théorème d'Ostrowski assure que les seuls complétés de $\mathbb{Q}$ sont les $\mathbb{Q}_p$ pour tout p premier et $\mathbb{R}$.

1.4 Extensions de valuation

Dans le cas des corps de fonctions, on a vu comment peut s'étendre une valuation triviale du corps des constantes à une valuation non triviale sur le corps des fonctions.

L'objectif dans la suite de ce mémoire sera de comprendre comment les valuations peuvent s'étendre sur un sur-corps. Nous verrons que cela dépend du type de l'extension.

Définition 1.33. *Soient (K, v) un corps valué, L une extension de K et w une valuation de L. On dit que la valuation w est une extension de v si v et w coïncident sur K.*

On pose (K, v) un corps valué et L une extension de K. A-t-on toujours une extension de la valuation v sur L ? Le théorème suivant assure l'existence :

Théorème 1.34 (Théorème de Chevalley)**.** *Soient K un corps, $R \subset K$ un sous-anneau et p un idéal premier de R. Alors il existe $\mathcal{O}$ un anneau de valuation de K tel que*

$$R \subset \mathcal{O} \text{ et } m \cap R = p,$$

où m est l'idéal maximal de $\mathcal{O}$.

Corollaire 1.35. *Il existe une valuation w qui étend v sur L*

Démonstration. Pour démontrer le corollaire, on utilise le théorème précédent. On prend $R = \mathscr{O}_v$. Il existe w une valuation de L tel que $\mathscr{O}_v \subset \mathscr{O}_w$ et $\mathfrak{m}_w \cap \mathscr{O}_v = \mathfrak{m}_v$.

Montrons que l'idéal maximal de $\mathscr{O}_w \cap K$ est $\mathfrak{m}_w \cap \mathscr{O}_v$. Il suffit de montrer que pour tout $x \in K$, $x \in \mathfrak{m}_w \cap \mathscr{O}_v$ si et seulement si $x^{-1} \notin \mathscr{O}_w \cap K$.

Soit $x \in K$ tel que $x \in \mathfrak{m}_w \cap \mathscr{O}_v$. D'après la Proposition 1.12, on a $x^{-1} \notin \mathscr{O}_w$, donc $x^{-1} \notin \mathscr{O}_w \cap K$. Soit $x \in K$ tel que $x^{-1} \notin \mathscr{O}_w \cap K$ alors $x \in \mathfrak{m}_w$. Comme $\mathscr{O}_v \subset \mathscr{O}_w \cap K$, on a $x^{-1} \notin \mathscr{O}_v$ donc $x \in \mathfrak{m}_v$ d'après la Proposition 1.12. Cela nous donne $x \in \mathfrak{m}_w \cap \mathscr{O}_v$. Les idéaux maximaux de $\mathscr{O}_w \cap K$ et $\mathscr{O}_v$ coïncident, ce qui montre par caractérisation des valuations par leur anneau de valuation que w est une extension de v. □

Dans la suite, on veut décrire l'ensemble des valuations de L dont la restriction à K coïncide avec v à équivalence près. C'est un problème fondamental, par exemple pour calculer des anneaux d'entiers.

Exemple 1.36. *Prenons l'extension quadratique $\mathbb{Q}(\theta) = \mathbb{Q}[X]/(X^2-2)$ et cherchons les extensions de la valuation 2-adique. Soit w une extension de v_2 sur $\mathbb{Q}(\theta)$. On a $w(\theta^2) = w(2) = v_2(2) = 1$ donc $w(\theta) = \frac{1}{2}$. Soient $a, b \in \mathbb{Q}$. On a $w(a\theta + b) \geqslant \min(v_2(a) + \frac{1}{2}, v_2(b))$. Or pour tous rationnels a et b, on a toujours $v_2(a) + \frac{1}{2} \neq v_2(b)$. On est dans le cas d'égalité, on a alors*

$$w(a\theta + b) = \min(v_2(a) + 1/2, v_2(b)).$$

On a montré qu'il existe une unique extension de la valuation v_2 sur $\mathbb{Q}(\theta)$.

Que se passe-t-il si on considère w une extension de la valuation 3-adique ? L'égalité $\theta^2 = 2$ nous donne $w(\theta) = 0$. Soient $a, b \in \mathbb{Q}$. On a $w(a\theta + b) \geqslant \min(v_3(a), v_3(b))$. Comme précédemment, on veut montrer qu'on a forcément égalité. Si $v_3(a) \neq v_3(b)$, on a bien égalité. Sinon supposons que $v_3(a) = v_3(b)$ et $w(a\theta + b) > \min(v_3(a), v_3(b))$. En multipliant par une certaine puissance de 3, on obtient $w(a'\theta + b') > 0$ et $v_3(a') = v_3(b') = 0$. En regardant la classe de a', b' et θ dans le corps résiduel de w, on a $\overline{a'}\overline{\theta} + \overline{b'} = 0$, $\overline{a'} \neq 0$ et $\overline{b'} \neq 0$. Or, $\overline{a'}, \overline{b'} \in \mathbb{F}_3$, ce qui donne $\overline{\theta} \in \mathbb{F}_3$. C'est impossible puisque $\overline{\theta}^2 = -1$, mais -1 n'est pas un carré modulo 3. Cela démontre que pour tout $a, b \in \mathbb{Q}$, on a

$$w(a\theta + b) = \min(v_3(a), v_3(b)).$$

Dans les deux exemples précédents, nous n'avons trouvé qu'une seule extension. Lorsque l'on a une extension transcendante, il existe une infinité d'extensions d'une valuation. Supposons que $L = K(X)$ avec X transcendant sur K et que v est une valuation discrète à valeurs dans $\mathbb{R}$. Le groupe de valuation est de la forme $\alpha\mathbb{Z}$ avec $\alpha \in \mathbb{R}^+$.

Commençons par les extensions de la valuation triviale. On a vu des exemples de valuations sur $K(X)$ qui sont triviales sur K dans l'Exemple 1.5. Montrons que ce sont les seules.

Proposition 1.37. *Soit w une extension de la valuation triviale de K sur $K(X)$. S'il existe $f \in K[X]$ tel que $w(f) > 0$, alors il existe P irréductible sur $K[X]$ tel que w est équivalente à v_P. Sinon, w est équivalente à la valuation $-deg$.*

Démonstration. Dans le premier cas, l'ensemble $\mathfrak{m}_w \cap K[X]$ est non nul et possède donc un élément de degré minimal. On notera cet élément $P = \sum_{i=0}^{d} a_i X^i$. Puisque $w(P) \geqslant \min(iw(X))$ et que w est triviale sur K, on peut déduire que $w(X) \geqslant 0$, sinon le minimum serait atteint et serait strictement négatif. On a alors $K[X] \subset \mathscr{O}_w$. Soit $f \in \mathfrak{m}_w \cap K[X]$. On fait la division euclidienne de f par P dont on note Q et R respectivement le quotient et le reste. On a alors $w(f) \geqslant \min(w(P) + w(Q), w(R))$. Comme $\deg(R) < \deg(P)$, si R était non nul, on aurait $w(R) \leqslant 0$. C'est impossible puisque $w(f) > 0$ et $w(P) + w(Q) > 0$. Donc f est divisible par P. Tout polynôme Q premier avec P vérifie donc $w(Q) = 0$. De plus P est premier car si on pouvait écrire $P = Q_1 Q_2$ avec $Q_1, Q_2 \in K[X]$, on aurait

$w(Q_1) \geqslant 0$, $w(Q_2) \geqslant 0$, et $w(Q_1)+w(Q_2) = w(P)$. L'un des deux est de degré 0, car sinon on aurait un élément de degré strictement inférieur à P et de valuation inférieure à $w(P)$. Cela démontre que pour tout $f \in K[X]$, $w(f) = v_P(f)w(P)$. Donc w est équivalente à v_P sur $K(X)$.

Supposons maintenant que $\mathfrak{m}_w \cap K[X] = \{0\}$. Rappelons que l'on a pour tout $x \in K(X)$, $x \notin \mathfrak{m}_w$ si et seulement si $x^{-1} \in \mathscr{O}_w$ grâce à la Proposition 1.12. Montrons que $K[X^{-1}]_{(X^{-1})}$. D'abord, $X \notin \mathfrak{m}_w$ d'après l'hypothèse donc $X^{-1} \in \mathscr{O}_w$, ce qui nous donne $K[X^{-1}] \subset \mathscr{O}_w$. Prenons $\sum_{i=0}^n a_i X^{-i} \in K[X^{-1}] \setminus (X^{-1})$, on a $a_0 \neq 0$. Supposons par l'absurde que $\sum_{i=0}^n a_i X^{-i} \in \mathfrak{m}_w$.

— Si $w(X) = 0$ alors $X \in \mathscr{O}_w$ et on aurait $(\sum_{i=0}^n a_i X^{-i})X^n \in \mathfrak{m}_w \cap K[X]$. C'est impossible.

— Sinon $w(X) < 0$, on aurait $\sum_{i=1}^n a_i X^{-i} \in \mathfrak{m}_w$ et donc $a_0 \in \mathfrak{m}_w \cap K[X]$. C'est impossible car $a_0 \neq 0$.

Cela démontre que $\sum_{i=0}^n a_i X^{-i} \notin \mathfrak{m}_w$, donc $(\sum_{i=0}^n a_i X^{-i})^{-1} \in \mathscr{O}_w$. On rappelle que $\mathscr{O}_{-\deg} = K[X^{-1}]_{(X^{-1})}$. On a montré que $\mathscr{O}_{-\deg} \subset \mathscr{O}_w$. Si l'inclusion est stricte alors il existe $f \in \mathscr{O}_w$ tel que $\deg(f) > 0$. Il existe donc $g \in K(X)$ de degré nul et $n \in \mathbb{N}^*$ tels que $f = X^n g$. On a

$$fX^{-(n-1)}g^{-1} = X \in \mathscr{O}_w,$$

car $\deg(g) = \deg(g^{-1}) = 0$. L'uniformisante de $\mathscr{O}_{-\deg}$ est X^{-1} et on en conclut que $K(X) \subset \mathscr{O}_w$. Comme w est supposée non triviale, on a $\mathscr{O}_w \subsetneq K(X)$ donc $\mathscr{O}_w = \mathscr{O}_{-\deg}$. Par égalité des anneaux de valuation, on en conclut que w est équivalente à $-\deg$. □

On a donc décrit l'ensemble des extensions de la valuation triviale de K sur $K(X)$.

Lorsque la valuation v n'est pas triviale sur K, on peut l'étendre de la manière suivante. On suppose ici que le groupe de valuation de v est de la forme $\alpha\mathbb{Z}$ avec $\alpha \in \mathbb{R}_+^*$.

Proposition 1.38. *Soit $\lambda \in \mathbb{R}$. L'application v_λ, définie par $v_\lambda(f) := \min_j(v(f_j) + j\lambda)$ pour $f = \sum_j f_j X^j$ et par $v_\lambda(f/g) = v_\lambda(f) - v_\lambda(g)$ pour tout $f, g \in K[X]$, définit une valuation sur $K(X)$.*

Démonstration. Soient $f(X), g(X) \in K[X]$. On a clairement $v_\lambda(f+g) \geqslant \min(v_\lambda(f), v_\lambda(g))$. Montrons que $v_\lambda(fg) = v_\lambda(f) + v_\lambda(g)$: on a déjà $v_\lambda(fg) \geqslant v_\lambda(f) + v_\lambda(g)$.

Il existe I un entier tel que $v_\lambda(f_I X^I) = v_\lambda(f)$ et $v_\lambda(f_i X^i) > v_\lambda(f)$ pour tout $i < I$. On définit un indice J pour g de la même manière.

Le coefficient devant X^{I+J} dans $h = fg$ est $h_{I+J} = \sum_{i+j=I+J} f_i g_j$. Dans le cas où $i < I$, $v_\lambda(f_i X^i) > v_\lambda(f)$, ce qui donne $v(f_i) > v_\lambda(f) - i\lambda$. Comme $v_\lambda(g_j X^j) \geqslant v(g)$, on a alors $v(f_i g_j) > v_\lambda(f) + v_\lambda(g) - (i+j)\lambda$.

Si $j < J$, on obtient la même inégalité.

Si $i = I$ et $j = J$ alors $v(f_I g_J) = v_\lambda(f) + v_\lambda(g) - (I+J)\lambda$.

On a donc $v(h_{I+J}) = v_\lambda(f) + v_\lambda(g) - (I+J)\lambda$. Comme $v_\lambda(fg) \leqslant v(h_{I+J}) + (I+J)\lambda$, on a $v_\lambda(fg) \leqslant v_\lambda(f) + v_\lambda(g)$. D'où l'égalité.

Ainsi, v_λ est une valuation sur $K[X]$ et on peut l'étendre à $K(X)$ par la formule de l'énoncé. □

Remarque 1.39. *La valuation v_λ est de rang 1.*

Pour montrer que v_λ est une valuation sur $K(X)$, il n'était pas nécessaire de supposer v discrète de rang 1. Il suffisait de prendre λ dans un groupe ordonné contenant le groupe de valuation de v. Cependant cette hypothèse est utile pour montrer la proposition suivante :

Proposition 1.40. *Soient λ_1, λ_2 deux réels distincts. Les valuations v_{λ_1} et v_{λ_2} ne sont pas équivalentes.*

Démonstration. Supposons que $\lambda_1 > \lambda_2$. Montrons qu'il existe f un polynôme de $K[X]$ tel que $f \in \mathscr{O}_{v_{\lambda_1}}$ et $f \notin \mathscr{O}_{v_{\lambda_2}}$. Cela est équivalent à $v_{\lambda_1}(f) \geqslant 0$ et $v_{\lambda_2}(f) < 0$. On cherchera f de la forme aX^n avec $a \in K$ et $n \in \mathbb{N}^*$. Pour vérifier les inégalités précédentes, il faut que n et a vérifient

$-n\lambda_2 > v(a) \geqslant -n\lambda_2$. Puisque $|\lambda_1 - \lambda_2| > 0$, il existe $n \in \mathbb{N}^*$ tel que $n|\lambda_1 - \lambda_2| > \alpha$. Il existe alors $b \in \alpha\mathbb{Z}$ tel que $-n\lambda_2 > b > -n\lambda_1$. Par surjectivité de la valuation v, il existe a tel que $v(a) = b$. Avec de tels a et n, le polynôme $f = aX^n$ vérifie bien les propriétés voulues. Les valuations v_{λ_1} et v_{λ_2} n'ont pas les mêmes anneaux de valuation, elles ne peuvent donc pas être équivalentes. □

Remarque 1.41. *Si λ n'appartient pas au groupe de valuation, alors on augmente strictement le groupe de valuation.*

La valuation v_0 sur $K(X)$ est appelée la valuation de Gauss. On a la propriété suivante :

Proposition 1.42. *La valuation de Gauss, notée ici w, vérifie $\Gamma_w = \Gamma_v$ et $\kappa_w = \kappa_v(\overline{X})$ où $\overline{X}$ est transcendant sur κ_v.*

Démonstration. On comprend aisément que $\Gamma_w = \Gamma_v$. Montrons que $\overline{X} \in \kappa_w$ est transcendant sur κ_v. Pour cela, on considère des éléments $a_0, \ldots, a_n \in \mathscr{O}_v$ tels que $\sum_{i=0}^n \overline{a_i}\overline{X}^i = 0$. On obtient alors $w(\sum_{i=0}^n a_i X^i) > 0$ ce qui implique $v(a_i) > 0$ pour tout $i = 0, \ldots, n$ et donc $\overline{a_i} = 0$. Cela prouve la transcendance de $\overline{X}$.

L'inclusion $\kappa_v(\overline{X}) \subset \kappa_w$ est claire. Montrons l'inclusion réciproque. Soit $h = f_1/f_2 \in \mathscr{O}_w^*$ avec $f_1, f_2 \in K[X]$. On peut écrire $f_1 = c_1 g_1$ avec $c_1 \in K^*$ et $g_1 \in \mathscr{O}_w^*$ en prenant c_1 le coefficient de f_1 de valuation minimale. De même, on a $f_2 = c_2 g_2$ avec $c_2 \in K^*$ et $g_2 \in \mathscr{O}_w^*$. On obtient $h = cg_1/g_2$ avec $c = c_1/c_2 \in K^*$. Comme $h, g_1, g_2 \in \mathscr{O}_w^*$, on a $c \in \mathscr{O}_w^*$ et donc $\overline{h} = \overline{cg_1}/\overline{g_2} \in \kappa_v(\overline{X})$. Cela démontre l'égalité $\kappa_v(\overline{X}) = \kappa_w$. □

La valuation de Gauss nous a permis de garder le même groupe de valuation bien que le corps de résiduel soit aggrandi. Considérons un exemple où l'on est dans le cas contraire.

Supposons maintenant que le groupe de valuation de v est $\mathbb{Z}$ et considérons la valuation associée à $\lambda = \sqrt{2}$. On pose $w = v_{\sqrt{2}}$.

Proposition 1.43. *Le groupe de valuation associé à w est $\Gamma_w = \mathbb{Z} \bigoplus \sqrt{2}\mathbb{Z}$ et son corps résiduel est $\kappa_w = \kappa_v$.*

Démonstration. La première égalité est claire, démontrons la seconde. Pour $f = \sum_{i=0}^n a_i X^i \in K[X]$, considérons l'unique indice m tel que $w(f) = w(a_m X^m)$. En effet, on ne peut pas avoir deux indices qui atteignent le minimum, car cela contredirait l'irrationalité de $\sqrt{2}$. On a $f = a_m X^m(1+u)$ avec $u \in \mathfrak{m}_w$. Si $h = f/g \in K(X)$ alors il existe $c \in K^*, r \in \mathbb{Z}$ et $u, u' \in \mathfrak{m}_w$ tels que $h = cX^r \frac{1+u}{1+u'}$. Si $h \in \mathscr{O}_w^*$, alors $w(cX^r) = 0$, ce qui donne $v(c) + r\sqrt{2} = 0$. Comme $\sqrt{2}$ est irrationnel on a $v(c) = 0$ et $r = 0$. Donc $c \in \mathscr{O}_v^*$ et comme $\overline{u} = \overline{u'} = 0$, on a $\overline{h} = \overline{c} \in \kappa_v$. Cela montre l'égalité recherchée. □

Remarque 1.44. *La valuation w n'est pas discrète. En effet, le groupe de valuation est dense dans $\mathbb{R}$, mais elle a le même corps résiduel.*

On expliquera ce phénomène dans le cas des extensions finies grâce aux indices de ramification et aux degrés d'inertie.

1.5 Ramification et inertie

Soient (K, v) un corps valué, L une extension de K et w une extension de v sur L.

Définition 1.45. *L'entier $e_w = [\Gamma_w : \Gamma_v]$ est l'indice de ramification de l'extension et l'entier $f_w = [\kappa_w : \kappa_v]$ est le degrée d'inertie de l'extension. Si $e_w = f_w = 1$, on dira que l'extension est immédiate.*

Les entiers e_w et f_w peuvent être infinis.

Exemple 1.46. — *Dans l'extension $(\mathbb{Q}(\theta), w)$ de $(\mathbb{Q}, v_2)$ dans l'Exemple 1.36, on a $e_w = 2$ car $\Gamma = \frac{1}{2}\mathbb{Z}$ et $\Gamma_v = \mathbb{Z}$. De plus, grâce à l'égalité $\theta^2 = 2$, on obtient $\kappa_w = \kappa_v$, donc $f_w = 1$.*

— *Pour la valuation de Gauss $(K(X), w)$ qui étend (K, v), où v est la valuation triviale, on a $e_w = 1$ et $f_w = \infty$.*

— *Alors que pour l'extension $(K(X), w = v_{\sqrt{2}})$ de (K, v), on a $e_w = \infty$ et $f_w = 1$.*

Lorsque l'extension est algébrique, les indices de ramification et les degrés d'inertie ne peuvent pas être aussi élevés qu'on le souhaite. C'est ce que nous dit le théorème suivant, que l'on admettra :

Théorème 1.47 (Inégalité fondamentale)**.** *Supposons que L est une extension finie de K. La valuation v de K admet un nombre fini d'extensions $w_1, \dots, w_r$ sur L et on a*

$$\sum_{i=1}^{r} e_{w_i} f_{w_i} \leqslant [L : K].$$

Exemple 1.48. *Dans l'extension $(\mathbb{Q}(\theta), w)$ de $(\mathbb{Q}, v_3)$ de l'Exemple 1.36, on avait $\kappa_v \subsetneq \kappa_w$ car $\theta^2 = 2$ et -1 n'est pas un carré dans $\mathbb{F}_3$. D'après l'inégalité, on a immédiatement $\Gamma_v = \Gamma_w$ et il n'y a pas d'autre extension de v_3 sur $\mathbb{Q}(\theta)$.*

Exemple 1.49. *On considère le polynôme $g = X^p - X - t^{-1} \in K[X]$ avec $K = \bigcup_{n\geqslant 1} \overline{\mathbb{F}_p}((t^{1/n}))$, le corps des séries de Puiseux muni de la valuation t-adique, notée v. Le polynôme g est irréductible dans $K[X]$. On le remarque en trouvant que $\alpha = t^{-1/p} + t^{-1/p^2} + t^{-1/p^3} + \cdots$ est une racine de g tel que $\alpha \notin K$. De plus, les autres racines de g sont les $\alpha+1, \dots, \alpha+p-1$. Si $h \in K[X]$ est un diviseur de g de degré $1 \leqslant d < p$, alors h est de la forme $x^d + (d\alpha + c)x^{d-1} + \cdots$ où $c \in K$ et $d \neq 0$. On aurait $\alpha \in K$ si h existait, c'est imposible. Le polynôme g est donc irréductible sur K. Soit $L = K(\alpha)$. L'extension L/K est galoisienne de degré p. On note w une extension de la valuation v sur L. On a $w(\alpha) = -1/p$. Or, le groupe de valuation de v sur K est $\mathbb{Q}$ et $\kappa_v = \overline{F_p}$ est algébriquement clos donc on a $e_w = f_w = 1$. De plus, on admet que w est l'unique extension de v dans L. On a alors*

$$1 = \sum_{w} e_w f_w < [L : K] = p,$$

où w parcourt les extensions de v dans L. Dans ce cas là, l'inégalité fondamentale est stricte.

Dans le cas d'une extension séparable et d'une valuation discrète, on a toujours égalité.

Théorème 1.50 (Égalité fondamentale)**.** *Soit L une extension séparable finie de K. Supposons que la valuation v est dicrète de rang 1, alors v a un nombre fini d'extensions notées $w_1, \dots w_r$ et on a l'égalité :*

$$\sum_{i=1}^{r} e_{w_i} f_{w_i} = [L : K].$$

On verra dans la Section 4 une démonstration de cette égalité en utilisant les indices de ramification et les degrés d'inertie d'idéaux dans les anneaux de Dedekind.

Exemple 1.51. *Considérons $\mathbb{Q}(\theta) = \mathbb{Q}[X]/(X^2+5)$ et w une extension de la valuation v_2 sur $\mathbb{Q}(\theta)$. Quel est l'indice de ramification de w ? L'égalité $\theta^2 = -5$ nous donne $w(\theta) = 0$ mais cela ne nous permet pas de conclure. On remarque que $(1+\theta)(1-\theta) = 6$ nous donne $w(1+\theta) + w(1-\theta) = 1$. En plongeant l'égalité $\theta^2 = -5$ dans le corps résiduel, on obtient $\overline{\theta^2} = 1$ et donc $\overline{\theta} = 1 \in \mathbb{F}_2$. On a $\overline{1+\theta} = \overline{1-\theta} = 0$ ce qui nous donne $w(1+\theta) > 0$ et $w(1-\theta) > 0$. Comme $1 - \theta = 1 + \theta - 2\theta$ on a $w(1-\theta) = w(1+\theta)$. On obtient $w(1-\theta) = \frac{1}{2}$ et par conséquent $\frac{1}{2}\mathbb{Z} \subset \Gamma_w$, ce qui implique $e_w \geqslant 2$. D'après l'égalité fondamentale, on a $e_w = 2$, $f_w = 1$ et w est la seule extension de v_2 sur $\mathbb{Q}(\theta)$.*

Une extension de la valuation v dans L une extension transcendente de K n'est pas forcément discrète, comme nous le montre la Proposition 1.43. Lorsque L est une extension finie de K et w une extension de v sur L, on a $[\Gamma_w : \Gamma_v] < \infty$. Si Γ_v est discret, alors Γ_w est discret. Par exemple, si $\Gamma_v = \mathbb{Z}$, il existe $g_1, \ldots, g_r \in \Gamma_w$ tels que $\Gamma_w = \bigcup_{i=1}^{r} g_i\mathbb{Z}$ et on comprend que Γ_w est discret.

Corollaire 1.52. *Soient L une extension finie de K et w une extension de la valuation v sur L. Si v est une valuation discrète alors w l'est aussi.*

Dans la prochaine partie, on se concentrera sur les corps complets et on verra que l'extension de v au complété K_v est immédiate.

2 Cas complet

Dans le reste de ce mémoire, on ne considérera plus que des valuations de rang 1. On pourra donc les supposer à valeurs réelles.

Lorsque le corps valué est complet, on peut obtenir des résultats sur la factorisation de polynômes en étudiant leur image dans le corps résiduel. De plus, il n'y a qu'une seule extension de la valuation v sur L lorsque K est complet et L est algébrique sur K. Cela nous permettra de relier la notion de factorisation à celle des extensions de valuation.

2.1 Complétion

On commence par expliquer le procédé de complétion qui nous permettra de comprendre l'extension de la valuation sur le complété.

Définition 2.1. *Un corps valué (K, v) est complet si $(K, |.|)$ est complet pour $|.|$ une norme associée à la valuation v.*

Théorème 2.2. *De tout corps valué (K, v), on peut construire $(\hat{K}, \hat{v})$ un corps valué complet, où K y est dense.*

Démonstration. Prenons R l'anneau des suites de Cauchy de (K, v) et considérons l'idéal maximal m des suites convergeantes vers 0 selon la valuation v. La suite $(a_n)_{n\in\mathbb{N}} \subset K$ converge vers 0 si $v(a_n)$ tend vers $+\infty$ lorsque n tend vers $+\infty$. Définissons le quotient $\hat{K} = R/m$. Le corps K se plonge dans $\hat{K}$ en envoyant chaque élément $a \in K$ sur la classe de la suite constante égale à a. La valuation v s'étend sur $\hat{K}$ de la manière suivante. Pour $a \in \hat{K}$ et $(a_n)_{n\in\mathbb{N}}$ un représentant de a, on pose

$$\hat{v}(a) = \lim_{n\to\infty} v(a_n).$$

C'est équivalent à poser $|a| = \lim_{n\to\infty} |a_n|$,. Cette limite est bien définie. En effet, on a $||a_n| - |a_m|| \leqslant |a_n - a_m|$ pour $|.|$ une norme associée à v. La suite $(|a_n|)_n \subset \mathbb{R}$ est de Cauchy. Par complétude de $\mathbb{R}$, elle converge. Par équivalence, la suite $(v(a_n))_n$ converge dans $\mathbb{R}\cup\{\infty\}$. De plus, $\hat{v}$ est une valuation. En effet, $\hat{v}(0) = +\infty$ et si pour $a = (a_n)_n \in \hat{K}$ on a $\hat{v}(a) = +\infty$ alors $\lim_{n\to\infty} a_n = 0$. D'après la définition de $\hat{K}$ on a alors $a = 0$. Prenons $a = (a_n)_n$ et $b = (b_n)_n$ dans $\hat{K}$. On a

$$\hat{v}(ab) = \lim_n v(a_n b_n) = \lim_n v(a_n) + v(b_n) = \lim_n v(a_n) + \lim_n v(b_n) = \hat{v}(a) + \hat{v}(b).$$

Supposons que $\hat{v}(a) < \hat{v}(b)$. À partir d'un certain rang, on aura $\min(v(a_n), v(b_n)) = v(a_n)$. Dans le cas où $\hat{v}(a) = \hat{v}(b)$ on a $\min(v(a_n), v(b_n)) \to_n \hat{v}(a)$. On en déduit que $\lim_n \min(v(a_n), v(b_n)) = \min(\hat{v}(a), \hat{v}(b))$. On obtient

$$\hat{v}(a+b) = \lim_n v(a_n + b_n) \geqslant \lim_n \min(v(a_n), v(b_n)) = \min(\hat{v}(a), \hat{v}(b)).$$

L'application $\hat{v}$ est bien défini et est une valuation éténdant v sur $\hat{K}$.

Montrons que K est dense dans $\hat{K}$, puis que $\hat{K}$ est complet. Soient $\alpha \in \hat{K}$ et $(a_n)_n \in K^{\mathbb{N}}$ un représentant de la classe de a. Pour tout $n \in \mathbb{N}$, on pose $\alpha_n \in \hat{K}$ la classe de la suite constante égale à a_n. Soit $\epsilon > 0$. Il existe $N \in \mathbb{N}$ tel que $|a_n - a_m| \leqslant \epsilon$ pour tout $m, n \geqslant N$. Pour $n \geqslant N$ fixé, la suite $(\epsilon - |a_n - a_m|)_m$ est une suite réelle de Cauchy, donc elle converge. De plus, la suite est positive donc elle converge vers un réel positif. Cela nous donne $|\alpha_n - \alpha| < \epsilon$. On a démontré que K est dense dans $\hat{K}$.

Il reste à montrer que $\hat{K}$ est complet. Soit $(\alpha_n)_n$ une suite de Cauchy à valeurs dans $\hat{K}$. Pour tout $n \in \mathbb{N}$, par densité, il existe $a_n \in K$ tel que $|\alpha_n - a_n| < \frac{1}{n}$. Comme la suite $(\alpha_n)_n$ est de Cauchy et que $\lim_{n\to\infty}(\alpha_n - a_n) = 0$, la suite $(a_n)_n$ est aussi de Cauchy. Prenons $\alpha \in \hat{K}$ la classe de $(a_n)_n$. La suite $(a_n)_n$ tend vers α donc $(\alpha_n)_n$ tend vers α. Cela démontre la complétude de $\hat{K}$.

□

Proposition 2.3. *La valuation v s'étend de manière unique dans $\hat{K}$.*

Démonstration. Cela vient de la densité de K dans $\hat{K}$. Prenons w une extension de v dans $\hat{K}$. Soit $\alpha \in \hat{K}$. Il existe $(a_n)_n$ une suite de K convergeant vers α. On a donc $\lim_{n\to\infty} w(a_n - \alpha) = +\infty$. Il existe $N \in \mathbb{N}$ tel que pour tout $n \geqslant N$, on ait $w(\alpha - a_n) > w(\alpha)$. On obtient $w(\alpha) = v(a_n)$ puisque le minimum est atteint dans $w(\alpha) \geqslant \min(w(\alpha - a_n), v(a_n))$. Cela démontre que la suite $(v(a_n))_n$ est stationnaire,converge vers $w(\alpha)$ et que $w(\alpha) = \hat{v}(\alpha)$. □

De plus, la démonstration précédente nous donne que le groupe de valuation de $\hat{v}$ est égal à celui de v. Quant au corps résiduel, on a la proposition suivante, que l'on admettra :

Proposition 2.4. *Soient $\mathcal{O}$ l'anneau de valuation de K, $\hat{\mathcal{O}}$ celui de $\hat{K}$, et $\mathfrak{m}$ et $\hat{\mathfrak{m}}$ leur idéal maximal respectif. On a $\hat{\mathcal{O}}/\hat{m} \cong \mathcal{O}/\mathfrak{m}$.*

L'extension de v sur $\hat{K}$ est donc immédiate. Dans la suite, on notera K_v le complété de K pour la valuation v et on gardera la notation v pour désigner l'extension de v sur K_v.

2.2 Méthode de Hensel-Newton

La méthode de Newton nous permet d'approximer des zéros de fonctions à condition que la dérivée ne s'annule pas proche du zéro. Pour les corps valués complets, nous avons une méthode similaire pour approximer les racines de polynômes à coefficients dans leur anneau de valuation. Dans cette partie on supposera toujours que les corps valués sont complets pour la norme associée à leur valuation.

Proposition 2.5 (Méthode de Hensel)**.** *Si (K, v) est un corps valué où v est une valuation discrète de rang 1 et P un polynôme à coefficients dans $\mathcal{O}$, l'anneau de valuation. On note p l'idéal maximal de $\mathcal{O}$. Alors, on peut approximer une racine de P grâce à la méthode de Hensel dans le cas où il existe $x_0 \in \mathcal{O}$ tel que $P(x_0) \equiv 0 \pmod{p}$ et $P'(x_0) \not\equiv \pmod{p}$.*

Détaillons d'abord la méthode de Hensel pour $K = \mathbb{Q}_p$, le corps des nombres p-adiques.

On considère P un polynôme dans $\mathbb{Z}[X]$ et $x_0 \in \mathbb{Z}$ une racine de $P \pmod{p}$, donc telle que $P(x_0) \equiv 0 \pmod{p}$.

On suppose que $P'(x_0) \not\equiv 0 \pmod{p}$. On pose $x_1 \in \mathbb{Z}$ tel que $x_1 \equiv \frac{-P(x_0)}{P'(x_0)} + x_0 \pmod{p^2}$. D'après la formule de Taylor, il existe $C \in \mathbb{Z}$ tel que $P(x_1) = P(x_0) + (x_1 - x_0)P'(x_0) + (x_1 - x_0)^2 C$. Comme $x_1 - x_0 \equiv 0 \pmod{p}$ on a $P(x_1) \equiv 0 \pmod{p^2}$.

Dans le cas général, si $P(x_i) \equiv 0 \pmod{p^n}$, en posant $x_{i+1} \in \mathbb{Z}$ tel que $x_{i+1} \equiv x_i - \frac{P(x_i)}{P'(x_i)} \pmod{p^{2n}}$, on obtient $P(x_{i+1}) \equiv 0 \pmod{p^{2n}}$ en procédant comme précédemment. Il reste à comprendre pourquoi on peut toujours diviser par $P'(x_i)$. En utilisant une formule de Taylor, on trouve

$P'(x_i) \equiv P'(x_{i+1}) \pmod{p}$. Par récurrence, on obtient $P'(x_i) \not\equiv 0 \pmod{p}$, donc $P'(x_i)$ est premier avec p et inversible modulo p^n pour tout n entier.

On obtient une suite de Cauchy $(x_i)_{i\in\mathbb{N}}$ qui approxime une racine de P. En effet, puisque $\mathbb{Q}_p$ est complet, la suite $(x_i)_{i\in\mathbb{N}}$ converge dans $\mathbb{Q}_p$ vers une racine de P. Plus précisément, $(x_i)_{i\in\mathbb{N}}$ approxime une racine modulo p^{2^i}.

On peut reprendre le même procédé pour $K = k((t))$, avec k un corps fini ou $\mathbb{Q}$, $P \in k[t][X]$ et $x_0 \in k[t]$ tel que $P(x_0) \equiv 0 \pmod{t}$. Montrons ce que cette méthode donne sur un exemple.

Exemple 2.6. *On prend $P(X) = X^2 - t - 1$, on se place dans le complété de $\mathbb{Q}(t)$ pour la valuation t-adique qui est $\mathbb{Q}[[t]]$.*

- *P se factorise sur le corps résiduel : $P(X) \equiv (X-1)(X+1) \pmod{t}$, on prend alors $x_0 = 1$. C'est une racine simple de $P \bmod t$. On peut donc utiliser la méthode de Hensel pour trouver une racine de P.*
- *D'après la méthode, on pose $x_1 \equiv 1 + \frac{t}{2} \pmod{t^2}$. Ce qui nous donne $P(x_1) \equiv t^2/2 \pmod{t^4}$ et $P'(x_1) \equiv 2 + t \pmod{t^4}$.*
- *On a $x_2 \equiv 1 + \frac{t}{2} - \frac{t^2}{8} + \frac{t^3}{16} \pmod{t^4}$.*

En continuant le procédé, on remarque que l'on obtient la série $1 + \frac{t}{2} + \sum_{n=2}^{\infty} (-1)^{n-1} \frac{1\times3\times\cdots\times(2n-3)}{2\times4\times\cdots\times2n} t^n$, ce qui correspond au développement en série entière de $\sqrt{t+1}$.

On a besoin de se restreindre à des valuations afin d'utiliser les modulo. En effet, si la valuation n'est pas discrète cette méthode ne fonctionne plus.

Exemple 2.7. *Prenons $K = \bigcup_{n\geqslant 1} \mathbb{F}_p((t^{1/n}))$ muni de la valuation t-adique. On note $\mathfrak{m}$ l'idéal maximal de l'anneau de valuation. On a $\mathfrak{m}^2 = \mathfrak{m}$. Dans cet exemple $v(x) \geqslant n$ n'est pas équivalent avec $x \in \mathfrak{m}^n$. Or l'équivalence est vraie pour une valuation discrète. C'est ce qu'on utilise dans la première méthode.*

En utilisant le même polynôme que dans l'exemple précédent, on peut prendre $x_0 = 1$ et puis $x_i = 1$ pour tout $i \geqslant 1$ qui vérifie bien les hypothèses demandées et la relation de récurrence. Or, la suite $(x_i)_i$ ne tend pas vers une racine de P.

Pour pouvoir raisonner sur les valuations non discrètes, il est important d'étudier les suites de fonctions grâce à leur valuation et non modulo des puissances de l'idéal maximal, comme démontrer dans la proposition suivante :

Proposition 2.8. *Soient v la valuation de K supposée de rang 1, $\mathscr{O}$ son anneau de valuation et $P \in \mathscr{O}[X]$. Supposons qu'il existe $x_0 \in \mathscr{O}$ tel que $v(P(x_0)) - 2v(P'(x_0)) > 0$. La suite définie par $x_{i+1} = x_i - P(x_i)/P'(x_i) \in \mathscr{O}$ pour $i \geqslant 0$ converge vers une racine de P dans $\mathscr{O}$.*

Démonstration. On pose $\delta = v(P(x_0)) - 2v(P'(x_0))$. On a $v(P(x_0)) \geqslant 0$ et $v(P'(x_0)) \geqslant 0$, ce qui donne $v(P(x_0)) - v(P'(x_0)) > 0$ grâce à l'hypothèse de départ. L'élément $\frac{P(x_0)}{P'(x_0)}$ est de valuation positive, donc il appartient à l'anneau de valuation. On pose $x_1 = x_0 - \frac{P(x_0)}{P'(x_0)} \in \mathscr{O}$. Montrons les assertions suivantes :

1. $v(x_1 - x_0) \geqslant \delta + v(P'(x_0))$.
2. $v(P(x_1)) - 2v(P'(x_0)) \geqslant 2\delta$.
3. $v(P'(x_0)) = v(P'(x_1))$.
4. $v(P(x_1)) - 2v(P'(x_1)) \geqslant 2\delta$.

La quatrième assertion est directement donnée par les trois premières. La première assertion se déduit directement de la définition de x_1. D'après une formule de Taylor, il existe $C \in \mathscr{O}$ tel que $P(x_1) = P(x_0)+(x_1-x_0)P'(x_0)+(x_1-x_0)^2C$ (voir Remarque 2.8). Comme $P(x_0)+(x_1-x_0)P'(x_0) = 0$, on a

$$v(P(x_1)) = v((x_1 - x_0)^2C) \geqslant 2v(x_1 - x_0) = 2\delta + 2v(P'(x_0)).$$

De plus, par le même raisonnement sur P', il existe $C \in \mathscr{O}$ tel que $P'(x_1) = P'(x_0) + (x_1 - x_0)C$. Or, on a

$$v(P'(x_0)) < v(P(x_0)) + v(P'(x_0)) = v(x_1 - x_0) \geqslant v((x_1 - x_0)C),$$

donc $v(P'(x_1)) = v(P'(x_0))$. On itère le processus de sorte à obtenir une suite. Soit $i \in \mathbb{N}$. En effet, si on a $x_i \in \mathscr{O}$ tel que $\Delta = v(P(x_i))-2v(P'(x_i)) > 0$ et que l'on pose $x_{i+1} = x_i - P(x_i)/P'(x_i) \in \mathscr{O}$, alors les assertions suivantes sont vérifiées

— $v(x_{i+1} - x_i) \geqslant \Delta + v(P'(x_i))$.
— $v(P(x_{i+1})) - 2v(P'(x_i)) \geqslant 2\Delta$.
— $v(P'(x_i)) = v(P'(x_{i+1}))$.
— $v(P(x_{i+1})) - 2v(P'(x_{i+1})) \geqslant 2\Delta$.

On peut les démontrer de la même manière que pour $i = 0$.

Par, récurrence, on obtient que la suite $(x_i)_{i\in\mathbb{N}}$ à valeurs dans $\mathscr{O}$ est bien définie et vérifie :

— $v(P(x_n)) \geqslant 2^n\delta + 2v(P'(x_0))$.
— $v(x_{n+1} - x_n) \geqslant 2^n\delta + v(P'(x_0))$.

La suite $(x_i)_i$ est de Cauchy, puisque K est complet, elle converge vers $x \in K$ une racine de P. Puisque la suite $(v(x_n))_n$ est positive, on obtient $v(x) \geqslant 0$ et donc $x \in \mathscr{O}$.

□

Remarque 2.9. *La constante C issue de la formule de Taylor est de valuation positive car $\frac{(P)^{(k)}(x)}{k!} \in \mathscr{O}$. En effet, on a $\frac{(X^a)^{(n)}}{n!} \in \mathbb{Z}[X]$ car $\frac{n(n-1)\cdots(n-k+1)}{k!} = \binom{n}{k}$*

Contrairement à la méthode précédente, on ne se contente pas d'une valuation discrète. Mais l'hypothèse du rang est importante.

Si la valuation v était de rang supérieur ou égal à 2, alors les assertions données dans la méthode précédente resteraient vraies mais on ne pourrait pas conclure que $(x_n)_n$ est une suite de Cauchy. C'est ce qu'on verra dans l'exemple suivant.

Exemple 2.10. *Reprenons les notations de l'Exemple 1.7 et prenons $P = X^2 - t - 1$. L'élément x_0 vérifie bien l'hypothèse de départ. En effet, $v(P(x_0)) - v(P'(x_0)) = (0, 1) > (0, 0)$. On a donc $\delta = (0, 1)$, mais l'inégalité $v(x_{i+1} - x_i) \geqslant 2^i\delta$ ne nous permet pas de conclure car $2^i\delta < (1, 0)$. La méthode de Hensel ne nous permet pas de conclure. De plus, la suite $(x_i)_i$ ne converge pas car $v(x^2 - 1 - t) < (1, 0)$ pour tout $x \in L$. Si $v_s(x) \neq 0$ alors c'est clair, sinon on utilise le fait que $1 + t$ n'est pas un carré dans $k(t)$.*

2.3 Lemme de Hensel

Les valuations sont toujours supposés de rang 1 et à valeurs réelles. Lorsque (K, v) est complet, nous avons un résultat de factorisation des polynômes en étudiant leur image dans le corps résiduel. Si $K = \mathbb{Q}_p$, alors le corps résiduel est le corps fini $\mathbb{F}_p$. Étudier la factorisation sur le corps résiduel est souvent plus simple.

Théorème 2.11 (Lemme de Hensel)**.** *Soient K un corps valué complet, $\mathscr{O}$ l'anneau de valuation de K, p son idéal maximal et κ le corps résiduel. Soit un polynôme primitif $f(x) \in \mathscr{O}[x]$,i.e., tel que $f(x) \not\equiv 0 \pmod{p}$), admettant une factorisation modulo p*

$$f(x) \equiv \overline{g}(x)\overline{h}(x) \pmod{p},$$

où $\overline{g}, \overline{h} \in \kappa[x]$ sont premiers entre eux. Alors $f(x)$ admet une factorisation $f(x) = g(x)h(x)$ où $g, h \in \mathscr{O}[x]$, $\deg(g) = \deg(\overline{g})$, $g(x) \equiv \overline{g}(x) \pmod{p}$ et $h(x) \equiv \overline{h}(x) \pmod{p}$.

Le Lemme de Hensel permet de démontrer le théorème suivant : une valuation d'un corps complet possède une unique extension dans une extension algébrique.

Théorème 2.12. *Soit K complet par rapport à la valuation v. Alors v ne s'étend que d'une seule manière sur les extensions algébriques. Prenons L/K une extension algébrique de degrée fini n. L'unique extension de v sur L, notée w, est donnée par la formule*

$$w(\alpha) = v(N_{L/K}(\alpha))/n, \quad \forall \alpha \in L.$$

Le complété K_v possède une unique extension de la valuation v, comme expliqué dans la sous-partie 2.1. Elle est notée v. Prenons $\overline{K_v}$ une clôture algébrique de K_v. L'extension $\overline{K_v}/K_v$ est algébrique et d'après le Théorème 2.12, il existe une unique extension de v sur $\overline{K_v}$ que l'on note $\overline{v}$.

Soient L/K une extension algébrique finie et w une valuation de L qui étend la valuation v de K. Alors, on a $L_w = LK_v$. En effet, LK_v est une extension finie de K_v donc LK_v est complet. De plus, LK_v est contenu dans L_w donc par minimalité de L_w, on a $L_w = LK_v$. On en déduit que L_w/K_v est finie et algébrique.

Tout K-plongement $\tau : L \to \overline{K_v}$ nous donne une extension $w = \overline{v} \circ \tau$ de v. De plus, pour tout K_v-automorphisme σ de $\overline{K_v}$, la composition $\sigma \circ \tau$ nous donne un nouveau K-plongement τ'. On dira alors que τ et τ' sont conjugués.

Proposition 2.13. *1. Toute extension w de la valuation v vient de la composition $w = v \circ \tau$ pour τ un K-plongement de L dans $\overline{K_v}$.*

2. Deux extensions $\overline{v} \circ \tau$ et $\overline{v} \circ \tau'$ sont égales si et seulement si τ et τ' sont conjugués sur K_v.

Démonstration. 1. Soient w une extension de v dans L et L_w le complété de L pour w. Comme L_w/K_v est finie et algébrique, w est l'unique extension de v. Si on prend $\tau : L_w \to \overline{K_v}$ un K-plongement, alors $\overline{v} \circ \tau$ est aussi une valuation de L_w. Elle coïncide avec w. On obtient bien $w = v \circ (\tau|_L)$ sur L et que $\tau|_L$ est un K-plongement de L dans $\overline{K_v}$.

2. Soient τ et $\sigma \circ \tau$, avec $\sigma \in Gal(\overline{K_v}/K_v)$, deux plongements de L conjugués sur K_v. La valuation $\overline{v}$ est l'unique extension de v dans $\overline{K_v}$, car $\overline{K_v}/K_v$ est algébrique. On a par unicité $\overline{v} = \overline{v} \circ \sigma$, donc $\overline{v} \circ \tau = \overline{v} \circ \sigma \circ \tau$. Les valuations de L induites par τ et $\sigma \circ \tau$ sont donc les mêmes. Réciproquement, si $\tau, \tau' : L \to \overline{K_v}$ sont deux K-plongements tels que $\overline{v} \circ \tau = \overline{v} \circ \tau'$, alors on pose $\sigma : \tau L \to \tau' L$ le K-isomorphisme $\sigma = \tau' \circ \tau^{-1}$. On peut l'étendre en un K_v-isomorphisme

$$\sigma : \tau L.K_v \to \tau' L.K_v$$

par densité et en utilisant l'égalité $\overline{v} \circ \tau = \overline{v} \circ \tau'$. On obtient un isomorphisme σ qui fixe K_v. En étendant σ en un K_v-automorphisme de $\overline{K_v}$, noté $\tilde{\sigma}$, on a $\tau' = \tilde{\sigma} \circ \tau$. On retrouve bien que τ et τ' sont conjugués.

□

Grâce aux résultats dans le cas complet, on obtient un résultat dans le cas général :

Théorème 2.14. *On suppose que l'extension L/K est engendrée par une racine, notée θ, d'un polynôme irréductible $f(X) \in K[X]$. Les valuations $w_1, \ldots, w_r$ étendant sur L la valuation v sont en correspondance avec les facteurs irréductibles de f dans le complété K_v :*

$$f(X) = f_1(X)^{m_1} \cdots f_r(X)^{m_r}.$$

En effet, soit $\overline{K_v}$ une clôture algébrique du complété de K par v. Les valuations w_i étendant v sont $w_i = \overline{v} \circ \tau_i$ pour $i \in \{1, \ldots, r\}$, où $\tau_i : L \to \overline{K_v}$ est un K-plongement qui envoie θ sur θ_i une racine de f_i et où $\overline{v}$ est l'extension de la valuation v de K_v sur la clôture algébrique $\overline{K_v}$. Ces valuations sont distinctes deux à deux.

Démonstration. Les extensions de v s'écrivent $\overline{v} \circ \tau$ avec $\tau : L \to \overline{K_v}$, un K-plongement. On comprend que $\tau, \tau' : L \to \overline{K_v}$ sont conjugués si et seulement si $\tau(\theta)$ et $\tau'(\theta)$ sont conjugués dans K_v, i.e., s'ils sont racines du même facteur de f dans $\overline{K_v}$. Cela nous donne bien la correspondance souhaitée. □

Remarque 2.15. *Si f est séparable, les m_i sont égaux à 1.*

3 Factorisation dans les corps complets

Le dernier résultat de la partie précédente donne le lien entre la factorisation dans le complété et l'ensemble des extensions de valuations. Un outil permettant d'obtenir des résultats sur cette factorisation est le polygone de Newton. On verra dans cette partie le lien entre le polygone de Newton, la factorisation d'un polynôme et ses racines.

3.1 Polygones de Newton

On supposera K complet pour la valuation v. On considère le polynôme $f(X) = f_0 + \cdots + f_n X^n \in K[X]$, avec $f_0 \neq 0$ et $f_n \neq 0$.

Pour construire le polygone de Newton associé à f, on construit les points $P_j = (j, v(f_j))$ pour tout $j = 1, \ldots, n$ tels que $f_j \neq 0$. Le polygone de Newton est la borne inférieure de l'enveloppe convexe de ces points (voir Figure 1). Il est composé d'un ensemble de segments σ_s, pour $1 \leqslant s \leqslant r$, où σ_s est le segment $[P_{m_{s-1}}, P_{m_s}]$ et $0 = m_0 < m_1 < \cdots < m_r = n$.

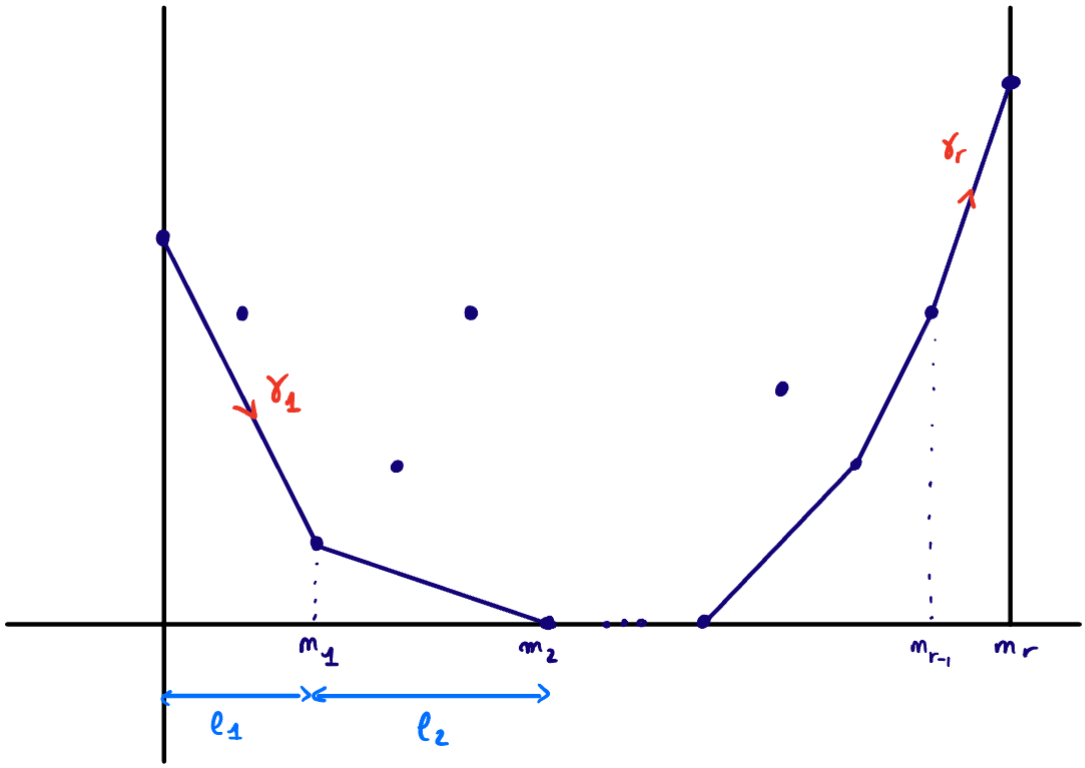

FIGURE 1

La pente de σ_s est $\gamma_s = \frac{v(f_{m_s}) - v(f_{m_{s-1}})}{m_s - m_{s-1}}$ et on a $\gamma_1 < \gamma_2 < \cdots < \gamma_r$. On note $l_1 = m_1$ et $l_s = m_s - m_{s-1}$ pour $s > 1$. On dira alors que f est de type $(l_1, \gamma_1; l_2, \gamma_2; \ldots, l_r, \gamma_r)$. Si $r = 1$, on dira que f est pur.

Le polygone de f peut nous donner des informations quant à sa factorisation. Cela nous est donné par le théorème suivant :

Théorème 3.1. *Supposons que $f(X) \in K[X]$ est de type $(l_1, \gamma_1; l_2, \gamma_2; \ldots, l_r, \gamma_r)$. Alors, il existe des polynômes $g_1, \ldots, g_r \in K[X]$ tel que $f(X) = g_1(X) \cdots g_r(X)$, où g_s est pur de type (l_s, γ_s) pour $1 \leqslant s \leqslant r$.*

Remarque 3.2. *Les g_s ne sont pas forcément irréductible.*

Pour démontrer ce théorème nous aurons besoin de quelques lemmes. On note v_s la valuation associée à $\lambda = -\gamma_s$ introduite à la Proposition 1.38.

Lemme 3.3. *1. $v_s(f) = v_s(f_j X^j)$ pour $j = m_s$ et $j = m_{s-1}$.*

2. $v_s(f(X) - \sum_{m_{s-1} \leqslant j \leqslant m_s} f_j X^j) > v_s(f)$.

3. Si $\lambda \neq -\gamma_s$ pour tout s, alors $v_\lambda(f) = v_\lambda(f_j X^j)$ pour un seul j et ce j fait partie des m_s.

Démonstration. 1) Il suffit de montrer que $\forall i \neq m_s$ on a $v_s(f_i X^i) \geqslant v_s(f_{m_s} X^{m_s})$ et $v_s(f_{m_s} X^{m_s}) = v_s(f_{m_{s-1}} X^{m_{s-1}})$. L'inégalité peut s'écrire :

$$v_s(f_i X^i) - v_s(f_{m_s} X^{m_s}) = (i - m_s)\left(\frac{v_s(f_i) - v(f_{m_s})}{i - m_s} - \gamma_s\right)$$

Si $i \leqslant m_s$, on voit bien que $\frac{v_s(f_i) - v(f_{m_s})}{i - m_s} \leqslant \gamma_s$ et inversement si $i \geqslant m_s$.

2) On peut montrer que l'inégalité

$$v_s(f_i X^i) - v_s(f_{m_s} X^{m_s}) \geqslant 0$$

est stricte pour $i \notin [m_{s-1}, \ldots, m_s]$, ce qui justifie l'inégalité.

3) On peut faire un dessin pour s'en convaincre. Le j correspond à $\gamma_j < -\lambda < \gamma_{j+1}$ si $-\lambda$ est coincé entre deux pentes. Si $-\lambda$ est inférieur à toutes les pentes alors $j = 0$. Si $-\lambda$ est supérieur à toutes les pentes alors $j = m_r$. □

On comprend alors que pour un λ quelconque, selon si $v_\lambda(f)$ est atteint en un ou plusieurs indices, on peut déterminer si $-\lambda$ est une pente ou non du polygone de Newton de f. Selon les indices auxquels la pente est atteinte on peut aussi en déduire la longueur de la pente (ou au moins une minoration de la longueur).

Lemme 3.4. *Si $f(X), g(X) \in K[X]$ sont purs de pente γ, alors $f(X)g(X)$ est pur de pente γ.*

Démonstration. On a, d'après le lemme précédent, $v_{-\gamma}(f) = v_{-\gamma}(f_0) = v_{-\gamma}(f_n X^n)$ et idem pour g avec $v_{-\gamma}(g) = v_{-\gamma}(g_0) = v_{-\gamma}(g_N X^N)$, où N est le degré de g.

On obtient $v_{-\gamma}(fg) = v_{-\gamma}(f_0 g_0) = v_{-\gamma}(f_n g_N X^{n+N})$, ce qui implique fg est pur de type $(n + N, \gamma)$. □

Lemme 3.5. *Supposons que f est de type $(l_1, \gamma_1; l_2, \gamma_2; \ldots; l_r, \gamma_r)$ et g est pur de type (N, γ) où $\gamma > \gamma_r$. Alors que fg est de type*

$$(l_1, \gamma_1; l_2, \gamma_2; \ldots; l_r, \gamma_r; N, \gamma).$$

Démonstration. Comme $\gamma > \gamma_s$ pour tout $1 \leqslant s \leqslant r$, alors $v_s(g(x) - g_0) > v(g)$. Soit $1 \leqslant s \leqslant r$, on rappelle que v_s correspond à la valuation $v_{-\gamma_s}$.

$$\begin{aligned}
V &:= v_s\left(f(X)g(X) - g_0 \sum_{m_{s-1} \leqslant j \leqslant m_s} f_j X^j\right) \\
&= v_s\left(f(X)g(X) - f(X)g_0 + f(X)g_0 + g_0 \sum_{m_{s-1} \leqslant j \leqslant m_s} f_j X^j\right) \\
&\geqslant \min\left(v_s(f(X)(g(X) - g_0)), v_s\left(g_0\left(f(X) - \sum_{m_{s-1} \leqslant j \leqslant m_s} f_j X^j\right)\right)\right) \\
&> v_s(f(X)g(X))
\end{aligned}$$

De plus, si on note $h(X) = f(X)g(X)$ alors le $m_s$ième coefficient de h est

$$h_{m_s}X^{m_s} = g_0 f_{m_s}X^{m_s} + g_1 X f_{m_{s-1}}X^{m_{s-1}} + \cdots + g_{m_s}X^{m_s} f_0.$$

Comme $v_s(g_iX^i) > v_s(g_0)$ pour tout $i > 0$ et que $v_s(f_iX^i) \geqslant v_s(f_{m_s}X^{m_s})$, en utilisant la propriété ultramétrique de la valuation on obtient $v_s(h_{m_s}X^{m_s}) = v_s(g_0 f_{m_s}X^{m_s})$. Ce qui donne :

$$\begin{aligned} v_s(f(X)g(X)) &= v_s\left(g_0 \sum_{m_{s-1}\leqslant j\leqslant m_s} f_j X^j\right) \\ &= v_s(g_0)v_s(f_{m_s}X^{m_s}) \\ &= v_s(h_{m_s}X^{m_s}) \end{aligned}$$

De même, on peut montrer que $v_s(f(X)g(X)) = v_s(h_{m_{s-1}}X^{m_{s-1}})$. Ce qui nous donne que γ_s est une pente de fg et qu'elle est au moins de longueur $l_s = m_s - m_{s-1}$.

Montrons que γ est une pente du polygone de Newton de fg. Comme γ est strictement supérieure à toutes les pentes de f, on a $v_{-\gamma}(f) = v_{-\gamma}(f_nX^n)$ et $v_{-\gamma}(f_iX^i) > v_{-\gamma}(f_nX^n)$. On a donc $v_{-\gamma}(f(X)g(X) - f_nX^n g(X)) > v_{-\gamma}(fg)$.

$$\begin{aligned} v_{-\gamma}(f(X)g(X)) &= v_{-\gamma}(f_nX^n g(X)) \\ &= v_{-\gamma}(f_nX^n g_0) \\ &= v_{-\gamma}(h_nX^n) \quad \text{(se démontre comme précédemment)} \end{aligned}$$

On a aussi

$$\begin{aligned} v_{-\gamma}(f(X)g(X)) &= v_{-\gamma}(f_nX^n g(X)) \\ &= v_{-\gamma}(f_nX^n g_NX^N) \\ &= v_{-\gamma}(h_{n+N}X^{n+N}) \end{aligned}$$

Donc γ est une pente de fg de longueur minorée par N. Par maximalité, comme $\deg(fg) = n+N$, on a forcément que fg est de type $(l_1, \gamma_1; l_2, \gamma_2; \ldots; l_r, \gamma_r; N, \gamma)$. □

Lemme 3.6. *Soit $\lambda \in \mathbb{R}$. On considère v la valuation associé à λ. Soient $F(X) \in K[X]$ et $G(X) = G_0 + \cdots + G_NX^N \in K[X]$ qui vérifie $v(G_NX^N) = v(G)$ et $N \leqslant \deg(F)$. On note respectivement Q et R le quotient et le reste de la division euclidienne de F par G. Alors, on a $v(Q) + v(G) \geqslant v(F)$ et $v(R) \geqslant v(F)$.*

Démonstration. On note $\deg(F) = n$. On a $\deg(Q) = n - N$ et $\deg(R) < N$.

Pour tout $k \geqslant N$ on a

$$F_k = \sum_{\substack{i+j=k \\ 0\leqslant i\leqslant N \\ 0\leqslant j\leqslant n-N}} G_iQ_j.$$

Pour $k = n$, on a $F_n = G_NQ_{n-N}$ donc $v(F_nX^n) = v(G_NX^N) + v(Q_{n-N}X^{n-N})$. On a alors $v(G) + v(Q_{n-N}X^{n-N}) \geqslant v(R)$. Puis, on procède par induction. Soit $j' \geqslant N$. On suppose que $\forall j > j'$ $v(G) + v(Q_jX^j) \geqslant v(R)$. En considérant le $N + j'$-ième coefficient de F, on obtient

$$\begin{aligned} v(G_NX^NQ_{j'}X^{j'}) &\geqslant \min(v(F_{N+j'}X^{N+j'}), v(G_iX^iQ_jX^j)) \text{ avec } j \text{ tel que } \ j' \leqslant j \leqslant N) \\ &\geqslant v(F) \quad \text{(par induction.)} \end{aligned}$$

On trouve

$$v(G) + v(Q_{j'}X^{j'}) \geqslant v(F) \text{ pour tout } 0 \leqslant j' \leqslant n - N.$$

On obtient $v(G) + v(Q) \geqslant v(F)$ en prenant le j' où le minimum est atteint. On obtient alors directement la deuxième inégalité en utilisant l'inégalité ultramétrique sur $R = F - QG$. □

Lemme 3.7. *Soient $\lambda \in \mathbb{R}$, v la valuation associée à λ et $f = f_0 + f_1 X + \cdots + f_n X^n \in K[X]$, avec $f_0 \neq 0$ et $f_n \neq 0$. On suppose qu'il existe $0 < N < n$ tel que $v(f_N X^N) = v(f)$ et $v(f_j X^j) > v(f)$ $\forall j < N$. Alors $f = gh$, où $g, h \in K[X]$ ont les degrés respectifs n et $n - N$.*

Démonstration. Il existe $\Delta > 0$ tel que

$$v\left(f(X) - \sum_{i=0}^{N} f_i\right) = v(f) + \Delta.$$

On considère $G, H \in K[X]$ tels que

$$\deg(G) = N \text{ et } \deg(H) \leqslant n - N, \tag{1}$$

et

$$v(f - G) \geqslant v(f) + \Delta, \quad v(H - 1) \geqslant \Delta. \tag{2}$$

On définit δ par $v(f - GH) = v(f) + \delta$. On a $\delta \geqslant \Delta$. En effet $v(G) = v(G - f + f) = v(f)$ car $v(G - f) > v(f)$ ce qui donne $v(f - GH) \geqslant \min(v(f - G), v(G - GH)) \geqslant v(f) + \Delta$.

On considère G, H qui vérifient (1) et (2) et on cherche G^*, H^* qui les vérifient aussi et tels que $\delta^* \geqslant \Delta + \delta$.

On a $v(f_N X^N) = v(f)$, $v(f_j X^j) > v(f)$ pour tout $j < N$ et $v(f - g) \geqslant v(f) + \Delta$, on peut montrer que $v(G_N X^N) = v(G)$.

On pose $L = f - GH$. On fait la division euclidienne de L par G et on obtient

— $L = QG + R$,

— $\deg(Q) \neq n - N$ et $\deg(R) < N$,

— $v(Q) \geqslant \delta$ et $v(R) \geqslant v(f) + \delta$.

On pose alors $G^* = G + R$ et $H^* = H + Q$. On voit que G^* et H^* vérifient bien (1) et (2).

$$\begin{aligned} \delta^* + v(f) &= v(f - G^* H^*) \\ &= v((H - 1)R + RQ) \\ &\geqslant \min(v(H - 1) + v(R), v(R) + v(Q)) \\ &\geqslant v(f) + \delta + \Delta, \text{ car } \Delta \leqslant \delta. \end{aligned}$$

Pour commencer, on peut prendre $G^0 := \sum_{i=0}^{N} f_i$, $H^0 := 1$ et $\delta^0 = \Delta$ et on construit la suite comme précédemment en itérant tant que $\delta < +\infty$. On obtient une suite de polynômes G, H convergeant vers des polynomes g, h (on utilise la complétude de K) tels que $f = gh$. □

Démonstration du théorème. Le Lemme 3.7 nous permet de factoriser f, tant que son polygone de Newton ne se résume pas à un segment. Les Lemmes 3.4 et 3.5 nous permettent de comprendre la forme des polygones de Newton de la factorisation de f. □

Exemple 3.8. *Le polynôme $f(X) = 5^2 X^5 + 30X^4 + 5^{-2} X^2 + 3X + 5 \in \mathbb{Q}_5[X]$ a un polygone de Newton composé de deux segments (voir Figure 2). Il est donc réductible dans $\mathbb{Q}_5[X]$.*

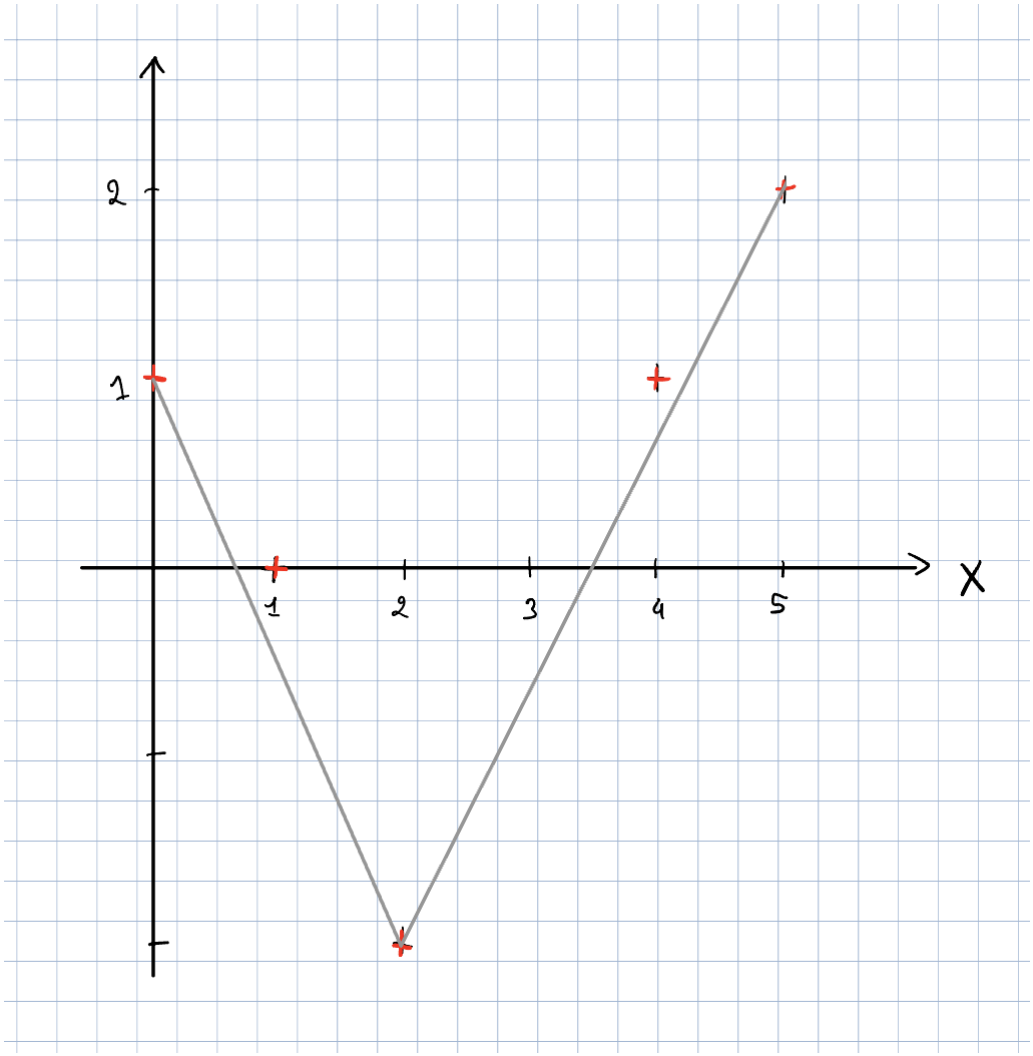

FIGURE 2

3.2 Conséquences

On considère toujours K complet.

Proposition 3.9. *Un polynôme irréductible dans $K[X]$ est pur.*

Remarque 3.10. *Un polynôme pur n'est pas forcément irréductible. En effet si on prend le polynôme $f(X) = X^2 - 4 \in \mathbb{Q}_2[X]$ (voir Figure 3), il est pur mais réductible.*

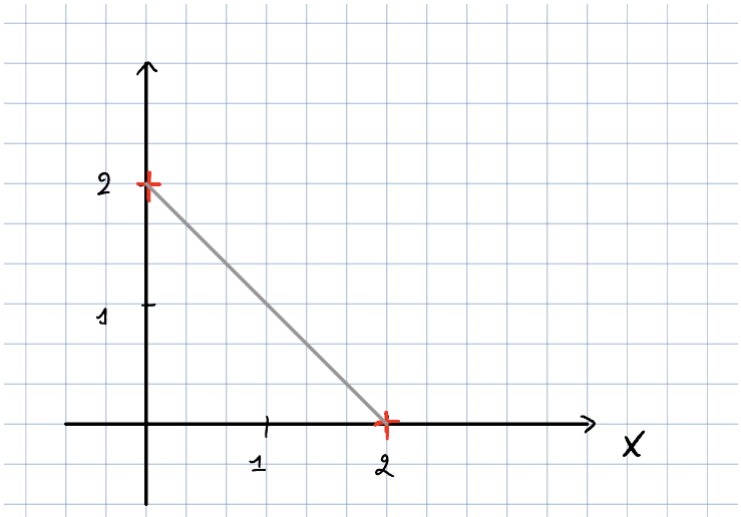

FIGURE 3

Proposition 3.11. *Un polynôme pur dont le polygone de Newton ne passe pas par un point entier, sauf aux extrémités, est irréductible.*

Corollaire 3.12 (Critère d'Eisenstein)**.** *Soient A un anneau factoriel, K son corps des fractions et $P(X) = \sum_{i=0}^{n} a_i X^i$ un polynôme à coefficents dans A. On suppose qu'il existe un élément premier p de A tel que*

- *p divise a_i pour $i \in \{1, \dots, n-1\}$,*
- *p ne divise pas a_n,*
- *p^2 ne divise pas a_0.*

Alors $P(X)$ est irréductible dans $K[X]$.

C'est une application directe de la Proposition 3.11, en traçant le polygone de Newton on remarque que, hormis aux extrémités, il ne passe par aucun point entier.

3.3 Lien entre polygone de Newton et valuations des racines

On a vu précédemment le lien entre extensions d'une valuation et factorisation d'un polynôme. Dans cette partie on verra le lien entre le polygone de Newton et les valuations de ses racines.

Proposition 3.13. *Soient $f(X) = a_0 + a_1 x + \cdots + a_n x^n$, $a_0 a_n \neq 0$, un polynôme à valeurs dans K, v une valuation sur K et w une extension de v sur L le corps de décomposition de f. Si f est de type $(l_1, \gamma_1; l_2, \gamma_2; \dots; l_r, \gamma_r)$ alors f a précisément l_i racines de valuation $-\gamma_i$.*

Démonstration. Diviser f par a_n revient à décaler le polygone vers le haut ou vers le bas. On supposera que $a_n = 1$. On note $\alpha_1, \dots, \alpha_n \in L$ les racines de f et $m_1 < \cdots < m_{t+1}$ tels que :

$$\begin{aligned} w(a_1) = \cdots = w(a_{s_1}) &= m_1 \\ w(a_{s_1+1}) = \cdots = w(a_{s_2}) &= m_2 \\ &\cdots \\ w(a_{s_t+1}) = \cdots = w(a_n) &= m_{t+1} \end{aligned}$$

En utilisant les relations entre les coefficients et les racines, on obtient :

$$\begin{aligned} v(a_n) &= v(1) = 0 \\ v(a_{n-1}) &\geqslant \min_i(w(a_i)) = m_1 \\ v(a_{n-2}) &\geqslant \min_{i,j}(w(a_i a_j)) = 2m_1 \\ &\cdots \\ v(a_{n-s_1}) &= \min_{i_1,\dots,i_{s_1}} (w(a_{i_1} \dots a_{s_1})) = s_1 m_1 \end{aligned}$$

Dans la dernière ligne, on a égalité car le terme $\alpha_1 \cdots \alpha_{s_1}$ est de valuation strictement plus petite que tous les autres.

$$\begin{aligned} v(a_{n-s_1-1}) &\geqslant \min_{i_1,\dots,i_{s_1+1}} (w(a_{i_1} \dots a_{i_{s_1+1}})) = s_1 m_1 + m_2, \\ v(a_{n-s_1-2}) &\geqslant \min_{i_1,\dots,i_{s_1+2}} (w(a_{i_1} \dots a_{i_{s_1+2}})) = s_1 m_1 + 2m_2, \\ &\cdots \\ v(a_{n-s_2}) &= \min_{i_1,\dots,i_{s_2}} (w(a_{i_1} \dots a_{i_{s_2}})) = s_1 m_1 + m_2 s_2 \end{aligned}$$

Grâce à cela, on en déduit que les sommets du polygone de Newton sont (de droite à gauche)

$$(n, 0), (n - s_1, s_1 m_1), (n - s_2, s_1 m_1 + (s_2 - s_1)m_2), \dots$$

Et on peut montrer que les pentes (de droite à gauche) sont bien les $-m_1, \dots, -m_r$. Ce qui démontre bien le résultat. □

4 Anneaux de Dedekind

Les propriétés des anneaux de Dedekind permettent de définir des valuations sans devoir se contenter du cadre factoriel ou principal. De plus, cette notion est stable par fermeture intégrale dans une extension séparable et finie, contrairement à la principalité.

4.1 Clôture intégrale

Définition 4.1. *Soient R un anneau et A un sous-anneau de R. On pose C l'ensemble des éléments de R qui sont entiers dans A, i.e., qui sont annulés par un polynôme unitaire à coefficients dans A. On appelle C la fermeture intégrale de A dans R.*

Lemme 4.2. *Soient R un anneau, A un sous anneau de R et x un élément de R. Les conditions suivantes sont équivalentes :*

1. *x est entier sur A.*
2. *$A[x]$ est un A-module de type fini.*
3. *Il existe B un sous-anneau tel que $A \subset B \subset R$, $x \in B$ et B est un A-module de type fini.*

Démonstration. Les implications 1. $\implies$ 2. et 2. $\implies$ 3. sont directes. Démontrons que 3. implique 1. Si x est inclus dans un A-module de type fini, notons le B, alors $A[x] \subset B$. On en déduit que $A[x]$ est de type fini. L'ensemble $\{x^i \mid i \in \mathbb{N}\}$ engendre $A[x]$. Puisque $A[x]$ est de type fini, on peut en extraire une famille génératrice finie, disons $\{x^i \mid 0 \leqslant i \leqslant N\}$ pour $N \in \mathbb{N}$. On a alors l'existence de $\alpha_0, \dots, \alpha_N \in A$ tels que $x^{N+1} = \alpha_N x^N + \dots + \alpha_1 x + \alpha_0$. Le polynôme $X^{N+1} - \alpha_N X^N - \dots - \alpha_1 X - \alpha_0$ est unitaire et à coefficients dans A et annule x. L'élément x est donc entier sur A. □

Proposition 4.3. *La fermeture intégrale de A dans R est un anneau.*

C'est une conséquence du lemme précédent, on utilise la 3-ième caractérisation.

Remarque 4.4. *Si A est intègre et $R = Frac(A)$, on parle de clôture intégrale. Si A est égal à sa propre clôture intégrale, on dit qu'il est intégralement clos.*

Proposition 4.5. *Un anneau de valuation est intégralement clos.*

Démonstration. Soient $\mathscr{O}$ un anneau de valuation et K son corps des fractions. Soit $x \in K$ entier sur $\mathscr{O}$. Montrons que $x \in \mathscr{O}$. On suppose par l'absurde que $x \notin \mathscr{O}$. Par la Proposition 1.12, on a $x^{-1} \in \mathfrak{m}$, où $\mathfrak{m}$ est l'idéal maximal de $\mathscr{O}$. Soit $P = X^n + a_{n-1}X^{n-1} + \dots + a_0 \in \mathscr{O}[X]$ un polynôme unitaire annulant x. En multipliant $P(x)$ par x^{-n}, on obtient $1 \in \mathfrak{m}$. C'est impossible, donc forcément $x \in \mathscr{O}$. □

Dans la suite, on notera A un anneau intègre, K son corps des fractions, L une extension de K et B la fermeture intégrale de A dans L.

Lemme 4.6. *Si L est une extension finie de K, alors $L = KB$.*

Démonstration. On a clairement l'inclusion $KB \subset L$. Pour la réciproque, on prend $y \in L$. Comme l'extension est finie, il existe $P \in K[X]$ unitaire tel que $P(y) = 0$. Or, il existe $a \in A$ tel que $aP(X) \in A[X]$. Notons $P = \sum_{i=1}^{d} a_i X^i$ avec $a_i \in K$. On a $a^d P = a^d X^d + aa_{d-1}(a^{d-1}X^{d-1}) + \cdots + a^d a_0$. En posant $Q = X^d + aa_{d-1}X^{d-1} + a^2 a_{d-2}X^{d-2} + \cdots + a^d a_0$, on obtient $a^d P(X) = Q(aX)$. Cela montre que $ay \in B$, car ay est annulé par Q un polynôme unitaire à valeurs dans A. Cela nous donne $y \in KB$. On a bien montré l'égalité des deux ensembles. □

Remarque 4.7. *Comme $K = Frac(A)$ et $A \subset B$, on a aussi $Frac(B) = L$.*

On rappelle que pour tout $x \in L$, $\mathrm{Tr}_{L/K}(x)$ est la trace de l'endomorphisme

$$T_x : \begin{cases} L \longrightarrow L \\ y \longmapsto xy. \end{cases}$$

Si L est une extension séparable et S l'ensemble des K-plongements de L dans $\overline{K}$ une clôture algébrique de K, alors on admet que $\mathrm{Tr}_{L/K}(x) = \sum_{\sigma \in S} \sigma(x)$ (voir [9]). De plus le discriminant d'une famille $(x_1, \ldots, x_n) \in L^n$ est $d(x_1, \ldots, x_n) := \det((\mathrm{Tr}_{L/K}(x_i x_j))_{1 \leqslant i,j \leqslant n})$.

Lemme 4.8. *Supposons A intégralement clos. Si $x \in B$, i.e., x est entier sur A, alors $\mathrm{Tr}_{L/K}(x) \in A$.*

Démonstration. Pour tout $\sigma \in S$, $\sigma(x)$ est entier sur A, car il est annulé par le polynôme unitaire à coefficients dans A qui annule x. On trouve $\mathrm{Tr}_{L/K}(x) \in K \cap B$ et, puisque A est intégralement clos, on a $K \cap B = A$. □

Grâce à ce lemme, on peut montrer que la notion d'anneau noethérien est stable par passage à la fermeture intégrale dans le cas d'une extension séparable.

Proposition 4.9. *On suppose A intégralement clos et L/K séparable de degré m. Il existe alors deux sous A-modules libres M et M' de L tels que*

$$M \subset B \subset M'.$$

En particulier, B est un A-module de type fini si A est noethérien, et est libre de rang m si A est principal.

Démonstration. Soient $\alpha_1, \ldots, \alpha_m \in L$ formant une base de L/K. On peut les prendre dans B à multiplication par un élément de A près. Si $d = d(\alpha_1, \ldots, \alpha_m)$ est le discriminant des α_i dans L/K, on a $dB \subset A\alpha_1 + \cdots + A\alpha_m$. En effet, soit $\alpha \in B$, on peut écrire $\alpha = a_1\alpha_1 + \cdots + a_m\alpha_m$ avec $a_i \in K$. On a

$$\mathrm{Tr}_{L/K}(\alpha_i \alpha) = \sum_{j=1}^{m} \mathrm{Tr}_{L/K}(\alpha_i \alpha_j) a_j.$$

En posant $N = (\mathrm{Tr}_{L/K}(\alpha_i \alpha_j))_{1 \leqslant i,j \leqslant n}$, on obtient

$${}^t(\mathrm{Tr}_{L/K}(\alpha_1 \alpha), \ldots, \mathrm{Tr}_{L/K}(\alpha_m \alpha)) = N\,{}^t(a_1, \ldots, a_m).$$

En multipliant par la transposée de la comatrice de N, on obtient que $da_i \in A$ pour tout i, puisque N est à valeurs dans A et que $Tr_{L/K}(\alpha_i \alpha) \in A$, d'après le lemme précédent.

On a $M := A\alpha_1 + \cdots + A\alpha_m \subset B \subset M' := A\alpha_1/d + \cdots + A\alpha_m/d$. Si A est noethérien, alors M' est un A-module noethérien, donc B est un A-module de type fini d'après [10]. Si A est principal, alors B est libre de rang m d'après [6]. □

Corollaire 4.10. *Soient A un anneau noethérien et intégralement clos, K son corps des fractions, L/K une extension finie et séparable, et B la fermeture intégrale de A dans L. Alors B est un A-module de type fini, et c'est donc un annneau noethérien.*

Un résultat important est qu'une fermeture intégrale est intégralement close lorsque l'extension est finie.

Théorème 4.11. *Soient A un anneau, K son corps des fractions, L/K une extension finie et B la fermeture intégrale de A dans L. Alors B est intégralement clos.*

Démonstration. On a $L = Frac(B)$ d'après la Remarque 4.7. Soit $x \in L$ entier sur B. On veut montrer que $x \in B$. Soit $P(X) = \sum_{i=0}^{n} b_i X^i \in B[X]$ un polynôme unitaire qui annule x. On pose $B' = A[b_1, \ldots, b_n]$ le sous-anneau engendré par les coefficients de P. C'est un A-module de type fini puisque les coefficients sont entiers sur A, d'après le Lemme 4.2. De plus, $B'[x]$ est un B'-module de type fini grâce au Lemme 4.2, donc $B'[x]$ est un A-module de type fini. On en déduit donc que x est entier sur A, i.e., $x \in B$. □

De plus, on peut déterminer la fermeture intégrale d'un anneau dans un corps à l'aide des anneaux de valuation. Ce résultat est donné par le théorème suivant :

Théorème 4.12. *On utilise les mêmes notations que dans le théorème précédent. Soit V l'ensemble des anneaux de valuation $\mathscr{O}$, dans L avec un idéal maximal M tels que $A \subset \mathscr{O}$ et $M \cap A$ est un idéal maximal de A. Alors la fermeture intégrale B de A dans L est égale à l'intersection :*

$$R := \bigcap_{\mathscr{O} \in V} \mathscr{O}.$$

Démonstration. D'après la Proposition 4.5, $\mathscr{O}$ est intégralement clos pour tout $\mathscr{O} \in V$ car $\mathscr{O}$ est un anneau de valuation. De plus, $A \subset \mathscr{O}$ donc $B \subset \mathscr{O}$. Ceci prouve $B \subset R$. Démontrons l'inclusion $L \setminus B \subset L \setminus R$. Soit $x \in L \setminus B$. On a $x \notin B[x^{-1}]$, sinon il existerait $a_0, \ldots, a_m \in B$ tels que $x = a_m + \cdots + a_0 x^{-m}$. En multipliant par x^m, on obtient que x est entier sur B. Or, B est intégralement clos d'après le théorème précédent. Par conséquent x^{-1} n'est pas inversible dans $B[x^{-1}]$, il est alors contenu dans $\mathfrak{m}$ un idéal maximal de $B[x^{-1}]$. Par le théorème de Chevalley, il existe un anneau de valuation $\mathscr{O}$ de L tel que $B[x^{-1}] \subset \mathscr{O}$ et $M \cap B[x^{-1}] = \mathfrak{m}$, où M est l'idéal maximal de $\mathscr{O}$. Puisque $x^{-1} \in M$, $x \notin \mathscr{O}$. Il suffit de comprendre que $\mathscr{O} \in V$, i.e., que $M \cap A$ est un idéal maximal de A. On a $M \cap A = \mathfrak{m} \cap A$ car $A \subset B[x^{-1}]$. D'abord, comme $x^{-1} \in \mathfrak{m}$ on a $B/\mathfrak{m} \cap B \simeq B[x^{-1}]/\mathfrak{m}$. L'idéal $\mathfrak{m} \cap B$ est maximal dans B. Et on a l'inclusion $A/\mathfrak{m} \cap A \subset B/\mathfrak{m} \cap B$. Or, B est entier sur A et $B/\mathfrak{m} \cap B$ est un corps, donc $A/\mathfrak{m} \cap A$ est un corps et $\mathfrak{m} \cap A$ est bien un idéal maximal de A. □

4.2 Anneaux de Dedekind

Définition 4.13. *Un anneau de Dedekind est un anneau noethérien, intégralement clos et tel que tout idéal premier non nul est un idéal maximal.*

On considère A un anneau de Dedekind et K son corps des fractions. Avant d'énoncer les propriétés d'un anneau de Dedekind, on remarque un résultat important :

Théorème 4.14. *Si L est une extension finie et séparable de K, et B la fermeture intégrale de A dans L, alors B est un anneau de Dedekind.*

Démonstration. Pour montrer que B est un anneau noethérien et intégralement clos, on utilise le Corollaire 4.10 et le Théorème 4.11. Soit $\mathfrak{p}$ un idéal premier non nul de B. Alors $p := \mathfrak{p} \cap A$ est un idéal premier non nul de A. La primalité est claire. De plus, p est non nul. En effet, si on prend $y \in \mathfrak{p}$ tel que $y \neq 0$, par définition de B, il existe $a_0, \ldots, a_n \in A$ tels que $a_n \neq 0$ et $y^n + a_1 y^{n-1} + \cdots + a_n = 0$ et on obtient alors que $a_n \in \mathfrak{p}$. Cela nous donne $a_n \in p$. Comme p est un idéal premier non nul de A, c'est un idéal maximal car A est un anneau de Dedekind. On trouve que $B/\mathfrak{p}$ est une extension algébrique de A/p. C'est donc un corps, et $\mathfrak{p}$ est maximal. On a montré que B est un anneau de Dedekind. □

Théorème 4.15. *Chaque idéal $\mathfrak{a}$ de A différent de (0) et A admet une factorisation $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ en idéaux premiers non nuls de A qui est unique à l'ordre des facteurs près.*

Pour montrer ce théorème, on introduit deux lemmes :

Lemme 4.16. *Pour tout idéal $\mathfrak{a} \neq (0)$ de A, il existe des idéaux premiers non nuls $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$ tels que $\mathfrak{a} \supseteq \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r$.*

Démonstration. Pour montrer ce lemme, on considère l'ensemble des $\mathfrak{a}$ qui ne vérifient pas cette condition. Comme A est noethérien, il existe $\mathfrak{a}$ un élément maximal de cet ensemble. Il ne peut pas être premier, donc il existe $b_1, b_2 \in A$ tels que $b_1 b_2 \in \mathfrak{a}$, mais $b_1, b_2 \notin \mathfrak{a}$. Si on note $\mathfrak{a}_1 = (b_1) + \mathfrak{a}$ et $\mathfrak{a}_2 = (b_2) + \mathfrak{a}$, alors $\mathfrak{a} \subsetneq \mathfrak{a}_1$, et de même pour $\mathfrak{a}_2$ et $\mathfrak{a}_1\mathfrak{a}_2 \subseteq \mathfrak{a}$. Par maximalité de $\mathfrak{a}$, les idéaux $\mathfrak{a}_1$ et $\mathfrak{a}_2$ contiennent un produit d'idéaux premiers. Il n'existe donc pas de $\mathfrak{a}$ ne vérifiant pas la propriété du lemme. □

Lemme 4.17. *Soit $\mathfrak{p}$ un idéal premier de A. On définit $\mathfrak{p}^{-1} = \{x \in K \mid x\mathfrak{p} \subseteq \mathscr{O}\}$. Alors $\mathfrak{a}\mathfrak{p}^{-1} \neq \mathfrak{a}$ pour tout idéal $\mathfrak{a} \neq (0)$.*

Démonstration. Soient $a \in \mathfrak{p}$, $a \neq 0$, et $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subset (a) \subset \mathfrak{p}$ avec r le plus petit possible. Alors, un des $\mathfrak{p}_i$ est contenu dans $\mathfrak{p}$ (sinon il existe $p_1 \cdots p_r \in \mathfrak{p}$ avec $p_i \in \mathfrak{p}_i \backslash \mathfrak{p}$, impossible car $\mathfrak{p}$ est premier).

On peut supposer $i = 1$. On a donc $\mathfrak{p}_1 \subset \mathfrak{p}$ et même $\mathfrak{p}_1 = \mathfrak{p}$, car $\mathfrak{p}_1$ est maximal et A est un anneau de Dedekind.

Puisque $\mathfrak{p}_2 \cdots \mathfrak{p}_r \nsubseteq (a)$ par minimalité de r, il existe $b = \mathfrak{p}_2 \cdots \mathfrak{p}_r$ tel que $b \notin (a)$, i.e., $a^{-1}b \notin A$. Or, on a $b\mathfrak{p} \subset (a)$, i.e., $a^{-1}b\mathfrak{p} \subset A$ et $a^{-1}b \in \mathfrak{p}^{-1}$. Il suit que $\mathfrak{p}^{-1} \neq A$.

Prenons maintenant $\mathfrak{a}$ un idéal non nul de A et $\alpha_1, \ldots, \alpha_n \in A$ formant un système de générateurs. Supposons par l'absurde que $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{a}$. Pour $x \in \mathfrak{p}^{-1}$, on pose $(a_{i,j})_{1 \leqslant i,j \leqslant n} \subset A$ tel que :

$$x\alpha_i = \sum_{j=1}^{n} a_{i,j}\alpha_j.$$

En posant la matrice $M = (x\delta_{i,j} - a_{i,j})_{1 \leqslant i,j \leqslant n}$, on obtient $M^t(\alpha_1, \ldots, \alpha_n) = 0$. Si on multiplie l'égalité précédente par la transposée de la comatrice de M, on trouve que le déterminant $d = \det(M)$ satisfait $d\alpha_1 = \cdots = d\alpha_n = 0$, et donc que $d = 0$.

D'où, x est entier sur A. Puisque c'est une racine de $P(X) = \det((X\delta_{i,j} - a_{i,j})_{1 \leqslant i,j \leqslant n}) \in A[X]$, on en déduit que $x \in A$, ce qui signifie que $\mathfrak{p}^{-1} = A$. C'est une contradiction, donc $\mathfrak{a}\mathfrak{p}^{-1} \neq \mathfrak{a}$. □

Démonstration du théorème.

1. Existence de la factorisation :

   Soit M l'ensemble des idéaux non triviaux de A n'admettant pas de décomposition en idéaux premiers. Supposons que $M \neq \emptyset$. Alors, il existe un élément maximal $\mathfrak{a}$ dans M (car A est un anneau de Dedekind) contenu dans un idéal maximal $\mathfrak{p}$ de A. On a

   $$\mathfrak{a} \subset \mathfrak{a}\mathfrak{p}^{-1} \subset \mathfrak{p}\mathfrak{p}^{-1} \subset A.$$

   Par le lemme précédent, $\mathfrak{a} \nsubseteq \mathfrak{a}\mathfrak{p}^{-1}$ et $\mathfrak{p} \nsubseteq \mathfrak{p}\mathfrak{p}^{-1}$. Comme $\mathfrak{p}$ est maximal, on a $\mathfrak{p}\mathfrak{p}^{-1} \subset A$. Par maximalité de $\mathfrak{a}$, et comme $\mathfrak{a}\mathfrak{p}^{-1} \neq A$, l'idéal $\mathfrak{a}\mathfrak{p}^{-1}$ admet une décomposition en idéaux premiers : $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$. Cela donne $\mathfrak{a} = \mathfrak{a}\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}_1 \cdots \mathfrak{p}_r\mathfrak{p}$. C'est absurde, donc $M = \emptyset$.

2. Unicité :

   Pour un idéal premier $\mathfrak{p}$, si $\mathfrak{a}\mathfrak{b} \subset \mathfrak{p}$ alors $\mathfrak{a} \subset \mathfrak{p}$ ou $\mathfrak{b} \subset \mathfrak{p}$. Donc si $\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s$, alors $\mathfrak{p}_1$ contient un $\mathfrak{q}_i$, disons $\mathfrak{q}_1$, et par maximalité des idéaux, ils sont égaux. Comme $\mathfrak{p}_1 \nsubseteq \mathfrak{p}_1\mathfrak{p}_1^{-1}$, on a $\mathfrak{p}_1\mathfrak{p}_1^{-1} = A$, toujours par maximalité. On multiplie $\mathfrak{a}$ par $\mathfrak{p}^{-1}$. On obtient $\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_2 \cdots \mathfrak{q}_s$ et on raisonne par induction.

On a donc prouvé l'unicité et l'existence de la décomposition en idéaux premiers. □

Pour définir une valuation $\mathfrak{p}$-adique sur K nous avons besoin d'introduire la définition d'idéal fractionnaire de A.

Définition 4.18. *On appelle idéal fractionnaire de A tout sous A-module I de K tel qu'il existe $d \in A$ non nul satisfaisant $I \subset d^{-1}A$.*

Remarque 4.19. *Les idéaux de A sont des idéaux fractionnaires.*

Proposition 4.20. *Soit J_K l'ensemble des idéaux fractionnaires non nuls de A. On munit J_K du produit de A-modules, i.e., II' est le A-module de K engendré par les produits d'éléments de I et I'. L'ensemble J_k muni de cette loi est un groupe abélien. L'élément neutre est $(1) = A$ et l'inverse de $\mathfrak{a}$ un idéal fractionnaire est $\mathfrak{a}^{-1} = \{x \in K \mid x\mathfrak{a} \subset A\}$.*

Démonstration. L'associativité et la commutativité sont claires. On comprend facilement que A est l'élément neutre et que le produit de deux idéaux fractionnaires reste un idéal fractionnaire. Pour $\mathfrak{p}$ un idéal premier non nul de A, on a bien $\mathfrak{p}\mathfrak{p}^{-1} = A$ car $\mathfrak{p} \subsetneq \mathfrak{p}\mathfrak{p}^{-1}$ (Lemme **??**) et $\mathfrak{p}$ est maximal. Par conséquent, si $\mathfrak{a}$ est un idéal de A, on note $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ la décompositon de $\mathfrak{a}$ en produit d'idéaux premiers. On pose $\mathfrak{b} = \mathfrak{p}_1^{-1} \cdots \mathfrak{p}_r^{-1}$. On a alors $\mathfrak{b}\mathfrak{a} = A$ donc $\mathfrak{b} \subset \mathfrak{a}^{-1}$. Réciproquement, si $x \in K$ vérifie $x\mathfrak{a} \subset A$, alors $x\mathfrak{a}\mathfrak{b} \subset \mathfrak{b}$. Ce qui donne $x \in \mathfrak{b}$ puisque $\mathfrak{a}\mathfrak{b} = A$. Cela démontre que $\mathfrak{b}$, l'inverse de $\mathfrak{a}$, est égal à $\mathfrak{a}^{-1}$. Le A-module $\mathfrak{a}^{-1}$ est un idéal fractionnaire, il suffit de prendre un élément non nul $d \in \mathfrak{a}$ et on obtient $d\mathfrak{a}^{-1} \subset A$. Dans le cas général, si $\mathfrak{a}$ est un idéal fractionnaire et $d \in A \setminus \{0\}$ est un élément tel que $d\mathfrak{a} \subset A$, alors $d\mathfrak{a}$ est un idéal de A. L'idéal fractionnaire $(d\mathfrak{a})^{-1} = d^{-1}\mathfrak{a}^{-1}$ est l'inverse de $d\mathfrak{a}$ et donc $\mathfrak{a}\mathfrak{a}^{-1} = A$. Le A-module $\mathfrak{a}^{-1}$ est bien un idéal fractionnaire de A. □

Corollaire 4.21. *Tout idéal fractionnaire $\mathfrak{a}$ de A admet une unique décomposition en produit d'idéaux premiers*

$$\mathfrak{a} = \prod_{\mathfrak{p} \text{ idéal premier de } A} \mathfrak{p}^{n_\mathfrak{p}}$$

où $n_\mathfrak{p} \in \mathbb{Z}$ est nul pour presque tout $\mathfrak{p}$. Autrement dit, J_K est un groupe abélien libre engendré par les idéaux premiers non nul de A.

Démonstration. Soient $\mathfrak{a}$ un idéal fractionnaire de A et $d \in A$ tel que $d\mathfrak{a}$ est un idéal de A. On a alors $\mathfrak{a} = (d\mathfrak{a})(dA)^{-1}$. Cette égalité nous donne une décomposition de $\mathfrak{a}$ en idéaux premiers de A. Pour l'unicité, il suffit de se ramener à l'unicité de la décomposition pour les idéaux de A. □

Grâce à la décomposition des idéaux fractionnaires en produit d'idéaux premiers, on peut définir une valuation p-adique. C'est le sujet de la sous-partie suivante. On y verra aussi les extensions de ces valuations.

4.3 Valuations dans les anneaux de Dedekind

Définition 4.22. *Soit I un idéal fractionnaire non nul de A. On note*

$$I = \prod_{\mathfrak{p} \text{ idéal premier de } A} \mathfrak{p}^{n_\mathfrak{p}}$$

sa décomposition en produit d'idéaux premiers. On pose $v_\mathfrak{p}(I) := n_\mathfrak{p}$ pour $\mathfrak{p}$ un idéal premier de A. Pour tout $x \in K^*$, on pose $v_\mathfrak{p}(x) := v_\mathfrak{p}((x))$, où (x) est l'idéal fractionnaire de A engendré par x. On pose aussi $v_\mathfrak{p}(0) = \infty$.

Proposition 4.23. *L'application $v_\mathfrak{p} : K \to \mathbb{Z} \cup \{\infty\}$ est une valuation sur K.*

Proposition 4.24. *Soit $\mathfrak{p}$ un idéal premier de A. L'anneau de valuation de $v_\mathfrak{p}$ est A_p, le localisé de A en $\mathfrak{p}$. De plus, $v_\mathfrak{p}$ est une valuation discrète de rang 1 dont le groupe de valuation est $\mathbb{Z}$.*

Lemme 4.25. *Soit R un anneau intègre qui n'est pas un corps. L'anneau R est local et principal si et seulement si c'est un anneau de valuation associé à une valuation discrète à valeurs dans $\mathbb{R}$.*

Démonstration. Montrons d'abord le sens direct de l'équivalence. Soit $\mathfrak{m}$ l'unique idéal maximal de R et m un générateur de $\mathfrak{m}$ dans R. L'élément m est irréductible puisqu'il engendre un idéal maximal. Comme R est principal, il est factoriel et on a l'existence et l'unicité de la décomposition en produit d'éléments irréductibles. La valuation v_m est donc bien définie sur $Frac(R)$. Supposons qu'il existe $x \in Frac(R) \setminus R$ tel que $v_m(x) \geqslant 0$. On a que m est le seul élément irréductible de R car l'anneau est local. Par définition de $Frac(R)$, et par décomposition en produit d'irréductibles dans R, on peut écrire $x = m^n u/v$ avec $n \in \mathbb{Z}$ et $u, v \in R \setminus \mathfrak{m}$. Comme x est de valuation positive, on a $n \geqslant 0$. Puisque R est local et que $v \in R \setminus \mathfrak{m}$, on a $v^{-1} \in R$. On obtient que $x \in R$. Ceci démontre que R est l'anneau de valuation associé à v_m. Or, v_m est une valuation discrète à valeurs dans $\mathbb{R}$, on obtient bien ce que l'on cherchait.

Pour la réciproque, il suffit d'utiliser l'existence d'un élément de valuation positive minimale pour montrer la principalité. □

Corollaire 4.26. *L'anneau de valuation $A_\mathfrak{p}$ est un anneau principal.*

Remarque 4.27. *De plus, il est local, donc il possède un unique idéal maximal. Tout élément de A de $\mathfrak{p}$-valuation égale à 1 est un générateur de l'idéal maximal de A_p. On l'appelle uniformisante de $\mathfrak{p}$ ou de $A_\mathfrak{p}$ ou générateur local.*

La propriété du corollaire précédent est même une caractérisation des anneaux de Dedekind.

Théorème 4.28. *Soit A un anneau intègre et noethérien. Si pour tout idéal maximal $\mathfrak{m}$ de A le localisé $A_\mathfrak{m}$ est principal, alors A est un anneau de Dedekind.*

Démonstration. On a

$$A = \bigcap_{\mathfrak{m} \text{ idéal maximal de } A} A_\mathfrak{m}.$$

Comme les $A_\mathfrak{m}$ sont des anneaux de valuation, ils sont intégralement clos, par la Proposition 4.5. Cette propriété est stable par intersection, donc A est intégralement clos. Soit $\mathfrak{p}$ un idéal premier de A. Montrons qu'il est maximal. Soit $\mathfrak{m}$ un idéal maximal de A qui contient $\mathfrak{p}$. Comme l'idéal $\mathfrak{p}A_\mathfrak{m}$ est premier dans $A_\mathfrak{m}$, il suit qu'il est maximal et que $\mathfrak{p}A_\mathfrak{m} = \mathfrak{m}A_\mathfrak{m}$. Ceci nous donne $\mathfrak{p} = \mathfrak{m}$. D'où, A est un anneau de Dedekind. □

Soient L une extension séparable et finie de K, et B la fermeture intégrale de A. D'après le Théorème 4.14, B est un anneau de Dedekind. Soit $\mathfrak{p}$ un idéal premier de A non nul. Considérons la décomposition de l'idéal $\mathfrak{p}B$ en idéaux premiers de B :

$$\mathfrak{p}B = \prod_\mathfrak{q} \mathfrak{q}^{e_\mathfrak{q}}.$$

On dira que l'idéal premier $\mathfrak{q}$ de B divise $\mathfrak{p}$ si $e_\mathfrak{q} \geqslant 1$. On peut aussi dire que $\mathfrak{q}$ est au dessus de $\mathfrak{p}$. L'entier $e_\mathfrak{q}$ est l'indice de ramification de $\mathfrak{p}$ sur $\mathfrak{q}$ et l'entier $f_\mathfrak{q} := [B/\mathfrak{q} : A/\mathfrak{p}]$ est le degré d'inertie de $\mathfrak{p}$ sur $\mathfrak{q}$.

Définition 4.29.
— *Si $r \geqslant 2$, alors on dit que $\mathfrak{p}$ se décompose dans L.*
— *Si $e_\mathfrak{q} = 1$ pour tout les idéaux $\mathfrak{q}$ au dessus de $\mathfrak{p}$ on dit que $\mathfrak{p}$ est inerte dans L. Dans le cas contraire on dit que $\mathfrak{p}$ se ramifie dans L.*

Dans le cas d'une extension quadratique de $\mathbb{Z}$, on verra qu'on peut déterminer les nombres premiers qui se décomposent, qui sont inerte et qui se ramifient dans la sous-partie 4.4.

Remarque 4.30. *Si $\mathfrak{q}$ est au dessus de $\mathfrak{p}$, alors $\mathfrak{q} \cap A = \mathfrak{p}$. En effet, $\mathfrak{p}B \subset \mathfrak{q}$ donc $\mathfrak{p} \subset \mathfrak{q} \cap A \subsetneq A$. Par maximalité, on obtient $\mathfrak{p} = \mathfrak{q} \cap A$. On en déduit que si $\mathfrak{q}$ divise $\mathfrak{p}$, alors il ne divise aucun autre idéal premier de A.*

Lemme 4.31. *Si deux valuations discrètes de K à valeurs dans $\mathbb{R}$ (donc de rang 1) sont équivalentes et coïncident sur un élément de valuation strictement positive, alors elle sont égales.*

Démonstration. Pour démontrer le lemme, il suffit de comprendre que le seul isomorphisme ordonné entre deux sous-groupes discrets de $\mathbb{R}$ est une homotéthie. Pour $\alpha, \beta \in \mathbb{R}_+^*$, on considère les sous-groupes discrets $\alpha\mathbb{Z}$ et $\beta\mathbb{Z}$. Si $\psi : \alpha\mathbb{Z} \to \beta\mathbb{Z}$ est un isomorphisme ordonné, alors $\psi(\alpha) = \beta$ par minimalité de α et β en tant que qu'éléments strictement positifs de leur groupe respectif. Par les propriétés des morphismes de groupes, on obtient $\psi(\alpha x) = \beta x$ pour tout $x \in \mathbb{Z}$ et donc $\psi(x) = cx$, où $c = \beta/\alpha$ pour tout $x \in \alpha\mathbb{Z}$.

Si v et v' sont équivalentes alors l'isomorphisme ordonné entre v et v' est une homotéthie de la forme $c \cdot \mathrm{Id}$. Prenons $x \in K$ tel que $v(x) = v(x') > 0$. On a $cv(x) = v'(x)$ et donc $c = 1$. Les valuations v et v' sont bien égales. □

Proposition 4.32. *Soit $\mathfrak{p}$ un idéal premier de A. Pour tout idéal premier $\mathfrak{q}$ de B tel que $\mathfrak{q}|\mathfrak{p}$, la valuation discrète $v_\mathfrak{q}/e_\mathfrak{q}$ étend $v_\mathfrak{p}$, et toute valuation étendant $v_\mathfrak{p}$ se construit de cette manière. On a une bijection*

$$\varphi : \begin{cases} \{\mathfrak{q} \text{ idéal premier de } B \mid \mathfrak{q}|\mathfrak{p}\} \longrightarrow \{w \text{ valuation de } L \text{ étendant } v\} \\ \mathfrak{q} \longmapsto v_\mathfrak{q}/e_\mathfrak{q}. \end{cases}$$

Démonstration. Soit $\mathfrak{q}$ un idéal premier de B au-dessus de $\mathfrak{p}$. On a $v_\mathfrak{q}(\mathfrak{p}B) = e_\mathfrak{q}$ par définition de l'indice de ramification. D'après la Remarque 4.30, $v_\mathfrak{q}(\mathfrak{r}B) = 0$ pour tout idéal premier de A différent de $\mathfrak{p}$. Soit I un idéal fractionnaire de A. Notons $I = \prod_\mathfrak{r} \mathfrak{r}^{n_\mathfrak{r}}$ la décomposition de I en produit d'idéaux premiers de A. On a

$$v_\mathfrak{q}(IB) = v_\mathfrak{q}\left(\prod_\mathfrak{r} \mathfrak{r}^{n_\mathfrak{r}} B\right) = v_\mathfrak{q}(\mathfrak{p}^{n_\mathfrak{p}} B) = v_\mathfrak{q}(\mathfrak{p}B) n_\mathfrak{p} = e_\mathfrak{q} n_\mathfrak{p} = e_\mathfrak{q} v_\mathfrak{p}(I).$$

On obtient $v_\mathfrak{q}(x) = e_\mathfrak{q} v_\mathfrak{p}(x)$ pour tout $x \in K^*$. La valuation $v_\mathfrak{q}/e_\mathfrak{q}$ étend donc $v_\mathfrak{p}$. L'application φ est bien définie.

Si $\mathfrak{q}$ et $\mathfrak{q}'$ sont deux idéaux distincts de B divisant $\mathfrak{p}$, alors aucun ne contient l'autre par maximalité. Prenons $x \in \mathfrak{q} \setminus \mathfrak{q}'$. Alors x vérifie $v_\mathfrak{q}(x) > 0 \geqslant v_{\mathfrak{q}'}(x)$. Cela prouve que $v_\mathfrak{q}$ et $v_{\mathfrak{q}'}$ ne sont pas équivalentes et que φ est injective.

Démontrons la surjectivité. Soit w une extension de $v_\mathfrak{p}$. On note W son anneau de valuation et $\mathfrak{m}$ son idéal maximal. Puisque $w|_K = v_\mathfrak{p}$, on a $A \subset W$ et $\mathfrak{m} \cap A = \mathfrak{p}$. Un anneau de valuation est intégralement clos. Comme L est le corps de fonctions de W, et que $A \subset B$, on a $B \subset W$. Posons $\mathfrak{q} = \mathfrak{m} \cap B$. C'est un idéal premier de B car $\mathfrak{m}$ l'est. On a aussi $\mathfrak{p} = \mathfrak{q} \cap A$, donc $\mathfrak{q}$ est au dessus de $\mathfrak{p}$. L'anneau W contient $B_\mathfrak{q}$. En effet, $\mathfrak{q} = \mathfrak{m} \cap B$, donc les éléments de $B \setminus \mathfrak{q}$ sont de valuations négatives. On obtient $B_\mathfrak{q} \subset W \subset Frac(B_\mathfrak{q}) = L$. Supposons que la première inclusion est stricte. Il existe $x \in W$ tel que $v_\mathfrak{q}(x) < 0$. Soit q une uniformisante de $B_\mathfrak{q}$. Il existe $n \in \mathbb{N}^*$ et $u \in B_\mathfrak{q}^*$ tels que $x = q^{-n}u$. En multipliant x par $q^{n-1}u^{-1}$, on montre que $q^{-1} \in W$. Cela nous donne $W = L$, ce qui est impossible car w n'est pas triviale. On a $W = B_\mathfrak{q}$ et donc w est équivalente à $v_\mathfrak{q}$. D'après le lemme précédent, on a en réalité $w = v_\mathfrak{q}/e_\mathfrak{q}$, car $w(\mathfrak{p}) = 1 = v_\mathfrak{q}(\mathfrak{p})/e_\mathfrak{q}$. □

Soient $\mathfrak{q}$ un idéal premier de B au dessus de $\mathfrak{p}$, $w = v_\mathfrak{q}/e_q$ la valuation associée qui étend $v = v_\mathfrak{p}$, et e_w, f_w les indice de ramification et degré d'inertie respectifs de l'extension w sur v. Montrons que $e_\mathfrak{q} = e_w$ et $f_\mathfrak{q} = f_w$. Le groupe de valuation de v est $\mathbb{Z}$, et celui de w est $\frac{1}{e_q}\mathbb{Z}$, donc $e_w = e_q$. Le corps résiduel de v est $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$, et celui de w est $B_\mathfrak{q}/\mathfrak{q}B_\mathfrak{q}$. Montrons que $A/\mathfrak{p} = A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$. On a

$A/\mathfrak{p} \subset A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$. Pour montrer l'inclusion inverse, prenons $x \in A_\mathfrak{p}$ et montrons qu'il existe $y \in A$ tel que $x - y \in \mathfrak{p}A_\mathfrak{p}$. Il existe $a \in A$ et $b \in A \setminus \mathfrak{p}$ tels que $x = \frac{a}{b}$. L'élément b n'appartient pas à l'idéal maximal $\mathfrak{p}$, donc $bA + \mathfrak{p} = A$ et il existe donc $c \in A \setminus \mathfrak{p}$ tel que $1 - bc \in \mathfrak{p}$. Posons $y = ac$. On obtient $x - y = \frac{ac(1-bc)}{bc} \in \mathfrak{p}A_\mathfrak{p}$. Cela nous donne $A_\mathfrak{p} = A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$. De même, $B_\mathfrak{q} = B_\mathfrak{q}/\mathfrak{q}B_\mathfrak{q}$. Cela démontre que $f_w = f_\mathfrak{q}$.

Il y a correspondance entre les indices de ramification et les degrés d'inertie des extensions de $v_\mathfrak{p}$ et ceux des idéaux au dessus $\mathfrak{p}$. On montrera l'égalité fondamentale dans le cas des idéaux d'un anneau de Dedekind. Grâce à la correspondance démontrée ci-dessus, on obtient une preuve du Théorème 1.50.

Il nous faut le Théorème des restes chinois pour démontrer l'égalité fondamentale.

Théorème 4.33 (Théorème des restes chinois)**.** *Soient $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ des idéaux dans un anneau $\mathscr{O}$ tels que $\mathfrak{a}_i + \mathfrak{a}_j = \mathscr{O}$ pour tout $i \neq j$. Alors si $\mathfrak{a} = \cap_{i=1}^n \mathfrak{a}_i$, on a*

$$\mathscr{O}/\mathfrak{a} \cong \bigoplus_{i=1}^{n} \mathscr{O}/\mathfrak{a}_i.$$

Démonstration. L'homomorphisme canonique

$$a \in \mathscr{O} \mapsto (a \bmod \mathfrak{a}_1, \ldots, a \bmod \mathfrak{a}_n) \in \bigoplus \mathscr{O}/\mathfrak{a}_i$$

a comme noyau $\bigcap_{i=1}^n \mathfrak{a}_i$. Il nous suffit de montrer qu'il est bien surjectif. Prenons $x_i \mod \mathfrak{a}_i \in \mathscr{O}/\mathfrak{a}_i$ pour $i = 1, \ldots, n$. Pour tout $i = 2, \ldots, n$, il existe $a_i \in \mathfrak{a}_i$ tel que $a_i \equiv 1 \pmod{\mathfrak{a}_1}$. C'est possible car $\mathfrak{a}_i + \mathfrak{a}_1 = \mathscr{O}$. On pose $y_1 = a_2 \cdots a_n$. Alors y_1 vérifie $y_1 \equiv 1 \pmod{\mathfrak{a}_1}$ et $y_1 \equiv 0 \pmod{\bigcap_{i=2}^n \mathfrak{a}_i}$. De même, on construit y_i pour tout $i = 2, \ldots, n$ tel que $y_i \equiv 1 \pmod{\mathfrak{a}_i}$ et $y_i \equiv 0 \pmod{\mathfrak{a}_j}$ pour $j \neq i$.

On pose $x = x_1 y_1 + \cdots + x_n y_n$. On trouve $x \equiv x_i \pmod{\mathfrak{a}_i}$ pour tout i. Cela prouve la surjectivité et on trouve bien l'isomorphisme recherché. □

Théorème 4.34. *Soient $\mathfrak{p}$ un idéal premier de A non nul et n le degré de l'extension L/K. Considérons la décomposition de l'idéal $\mathfrak{p}B$ en idéaux premiers de B :*

$$\mathfrak{p}B = \prod_{\mathfrak{q}} \mathfrak{q}^{e_\mathfrak{q}}.$$

On a l'égalité fondamentale :

$$\sum_{\mathfrak{q}} e_\mathfrak{q} f_\mathfrak{q} = n.$$

Démonstration. On peut utiliser le Théorème des restes chinois :

$$B/\mathfrak{p}B \cong \bigoplus_{\mathfrak{q}} B/\mathfrak{q}^{e_\mathfrak{q}}.$$

Les quotients $B/\mathfrak{p}B$ et $B/\mathfrak{q}^{e_\mathfrak{q}}$ sont des espaces vectoriels sur le corps $\kappa = A/\mathfrak{p}$. Pour montrer l'égalité fondamentale, on raisonnera sur la dimension de ces espaces vectoriels.

— Montrons que $[B/\mathfrak{q}^{e_\mathfrak{q}} : A/\mathfrak{p}] = e_\mathfrak{q} f_\mathfrak{q}$.
On a $f_\mathfrak{q} = [B/\mathfrak{q} : A/\mathfrak{p}]$. Pour chaque $r = 0, \ldots, e_\mathfrak{q} - 1$, le quotient $\mathfrak{q}^r/\mathfrak{q}^{r+1}$ est un $B/\mathfrak{q}$-module de dimension 1.
On considère la chaîne descendante :

$$B/\mathfrak{q}^{e_\mathfrak{q}} \supseteq \mathfrak{q}/\mathfrak{q}^{e_\mathfrak{q}} \supseteq \cdots \supseteq \mathfrak{q}^{e_\mathfrak{q}-1}/\mathfrak{q}^{e_\mathfrak{q}} \supseteq (0).$$

Comme $(\mathfrak{q}^r/\mathfrak{q}^{e_\mathfrak{q}})/(\mathfrak{q}^{r+1}/\mathfrak{q}^{e_\mathfrak{q}}) \cong \mathfrak{q}^r/\mathfrak{q}^{r+1} \cong B/\mathfrak{q}$, et $\dim_\kappa(B/\mathfrak{q}) = f_\mathfrak{q}$, on a $\dim_\kappa(B/\mathfrak{q}^{e_\mathfrak{q}}) = e_\mathfrak{q} f_\mathfrak{q}$.

— Montrons que $[B/\mathfrak{p}B : A/\mathfrak{p}] = n$.

Si B est un A-module libre, par exemple si A est principal, alors on a un isomorphisme de A-module : $A^m \to B$. En tensorisant par K on obtient un isomorphisme $K^m \to L$, ce qui montre que $n = m$. Puis, en tensorisant par $A/\mathfrak{p}$, on a un isomorphisme de $A/\mathfrak{p}$-module $(A/\mathfrak{p})^m \to (B/\mathfrak{p}B)$, ce qui montre que $[B/\mathfrak{p}B : A/\mathfrak{p}] = m = n$.

Dans le cas général, on se ramène au localisé. On note $B_\mathfrak{p} := B[A_\mathfrak{p}]$. L'anneau $B_\mathfrak{p}$ est la fermeture intégrale de $A_\mathfrak{p}$ dans L et $\mathfrak{p}B_\mathfrak{p} = \prod_\mathfrak{q}(\mathfrak{q}B_\mathfrak{p})^{e_\mathfrak{q}}$. Comme $\dim_{A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}}(B_\mathfrak{p}/(\mathfrak{q}B_\mathfrak{p})^{e_\mathfrak{q}}) = \dim_\kappa(B/\mathfrak{q}^{e_\mathfrak{q}}) = e_\mathfrak{q} f_\mathfrak{q}$, et grâce à l'égalité précédente, on obtient $\sum_\mathfrak{q} e_\mathfrak{q} f_\mathfrak{q} = [B_\mathfrak{p}/\mathfrak{p}B_\mathfrak{p} : A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}]$. Or $A_\mathfrak{p}$ est principal (Corollaire 4.26) donc $[B_\mathfrak{p}/\mathfrak{p}B_\mathfrak{p} : A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}] = n$. Cela démontre l'égalité fondamentale.

□

Ce théorème nous est utile pour déterminer une majoration du nombre d'extensions de valuations grâce au degré de l'extension. Dans la partie suivante, on en déduira un théorème sur la décomposition des nombres premiers dans un corps quadratique.

En combinant le Théorème 4.34 avec le Théorème 2.14, on obtient une correspondance entre la factorisation du polynôme engendrant l'extension L et les idéaux de B au-dessus d'un idéal premier de A.

Théorème 4.35. *Soient $\mathfrak{p}$ un idéal premier de A et $v_\mathfrak{p}$ la valuation qui lui est associée. On note $f \in K[X]$ le polynôme engendrant l'extension L/K et θ une racine de f dans L. On considère $f = f_1 \cdots f_r$ la factorisation de f dans le complété de K pour la valuation $v_\mathfrak{p}$. Chaque extension de $v_\mathfrak{p}$, de la forme $v_\mathfrak{q}/e_\mathfrak{q}$ avec $\mathfrak{q}$ un idéal de B au dessus de $\mathfrak{p}$, correspond à un facteur de f. Soit $\overline{K_{v_\mathfrak{p}}}$ une clôture algébrique du complété de K par $v_\mathfrak{p}$. Il existe $i \in \{1, \dots, r\}$ et un plongement $\tau_i : L \to \overline{K_{v_\mathfrak{p}}}$ qui envoie θ sur θ_i une racine de f_i tels que $v_\mathfrak{q}/e_\mathfrak{q}$ est égale à $\overline{v_\mathfrak{p}} \circ \tau_i$, où $\overline{v}$ est l'extension de la valuation $v_\mathfrak{p}$ de K_v sur la clôture algébrique $\overline{K_{v_\mathfrak{p}}}$.*

Par bijection des facteurs de f aux extensions de $v_\mathfrak{p}$, on comprend bien l'équivalence entre $v_\mathfrak{q}/e_\mathfrak{q}$ et $\overline{v} \circ \tau_i$. L'égalité est obtenue grâce au Lemme 4.31.

4.4 Corps de nombres quadratiques

L'anneau $\mathbb{Z}$ est un anneau de Dedekind. Soient L un corps de nombres et B la fermeture intégrale de $\mathbb{Z}$ dans L. L'anneau B est de Dedekind . On l'appelera anneau des entiers de L.

Soient d un entier sans facteur carré et B l'anneau des entiers du corps quadratique $L = \mathbb{Q}(\sqrt{d})$. On admettra la proposition suivante :

Proposition 4.36. *On a*

— *Si $d \equiv 1 \pmod 4$, alors $B = \mathbb{Z} + \frac{1+\sqrt{d}}{2}\mathbb{Z}$.*

— *Sinon, $B = \mathbb{Z} + \sqrt{d}\mathbb{Z}$.*

Soit p un nombre premier. On va étudier la décomposition en idéaux premiers de l'idéal pB. On note $e_1, \dots, e_r, f_1, \dots, f_r$ respectivement les indices de ramification et les degrés d'inertie de $\mathfrak{p}$ dans B. D'après l'égalité fondamentale, on a $\sum_{i=1}^r e_i f_i = 2$, ce qui montre que $r \leqslant 2$ et que seuls trois cas peuvent survenir :

1. Si $r = 2, e_1 = e_2 = f_1 = f_2 = 1$, alors p se décompose dans L.
2. Si $r = 1, e_1 = 1, f_1 = 2$, alors p est inerte dans L.
3. Si $r = 1, e_1 = 2, f_1 = 1$, alors p se ramifie dans L.

On a le théorème suivant, qui nous donne la décomposition des premiers dans L. On le démontrera à l'aide des outils introduits dans les parties précédentes.

Théorème 4.37. *Soient d un entier sans facteur carré et B l'anneau des entiers du corps quadratique $L = \mathbb{Q}(\sqrt{d})$.*

- *Les nombres premiers qui sont ramifiés dans L sont ceux divisant d, ainsi que 2 si $d \equiv 3 \pmod 4$.*
- *Ceux qui sont décomposés dans L sont les nombres premiers impairs p tels que d est un résidu quadratique modulo p, ainsi que 2 si $d \equiv 1 \pmod 8$.*
- *Pour finir, ceux qui sont inertes dans L sont les nombres premiers impairs p tels que d n'est pas un résidu quadratique modulo p, ainsi que 2 si $d \equiv 5 \pmod 8$.*

Démonstration. Commençons par montrer quels sont les premiers se ramifiant dans L.

- Soit p un nombre premier divisant d. On a $v_p(d) = 1$ puisque d n'a pas de facteur carré. On note θ une racine de $X^2 - d$ dans L. On a $\theta^2 = d$, donc si on considère w une extension de v_p, on a forcément $w(\theta) = 1/2$. On a alors $e_w \geqslant 2$. D'après l'égalité fondamentale et par la correspondance de l'indice de ramification de w sur v avec celui d'un idéal au dessus de (p), on obtient que p se ramifie.
- Supposons que $d \equiv 3 \pmod 4$. Montrons que 2 se ramifie dans L. Le polynôme $f = X^2 - d \in \mathbb{Z}[X]$ est irréductible sur $\mathbb{Q}_2$. En effet, si on trace le polygone de Newton de $f(X+1)$, il est pur et ne passe par aucun point entier hormis ses deux extrémités. Par la Proposition 3.11, on obtient que f est irréductible dans $\mathbb{Q}_2$. Grâce au Théorème 2.14, cela nous donne que v_2 ne possède qu'une unique extension sur L et donc que 2 ne se décompose pas dans L. De plus, l'idéal 2 n'est pas premier dans l'anneau des entiers $B = \mathbb{Z} + \sqrt{d}\mathbb{Z}$. En effet le produit $(1+\theta)$ et $(1-\theta)$ est dans (2), mais aucun de ces éléments ne l'est. Ceci démontre que 2 se ramifie sur L.

Soit p un nombre premier impair ne divisant pas d.

- Supposons que d est un carré modulo p. On a alors $f \equiv (X-\alpha)(X+\alpha) \pmod p$ pour α une racine carré de d modulo p. D'après le Lemme de Hensel, f se factorise en deux facteurs distincts de degré 1. D'après le Théorème 2.14, on a exactement deux extensions de la valuation v_p. D'après le Théorème 4.35, on a deux idéaux premiers de l'anneau des entiers au-dessus de (p). Le premier p se décompose dans L.
- Supposons que d n'est pas un carré modulo p. Pour démontrer que p est inerte, on utilise la correspondance des indices de ramification des extensions de v_p avec les idéaux au-dessus de (p). Soit w une extension de v_p. On a $w(\theta) = v_p(d)/2 = 0$. En considérant l'image de l'égalité $\theta^2 = d$ dans le corps résiduel de w, on obtient $\overline{\theta^2 - d} = 0$. Cela nous donne $\overline{\theta}^2 = d$. Comme d n'est pas un carré modulo p, on obtient que $f_w \geqslant 2$. On en déduit que p est inerte dans L.

Il reste à montrer comment 2 se décompose selon la reste de d modulo 8.

- Supposons que $d \equiv 1 \pmod 8$. Grâce à une méthode de Hensel, on va montrer que $f = X^2 - d$ se factorise sur $\mathbb{Q}_2$. On pose $x_0 = 1$. On a $f(x_0) \equiv 0 \pmod 2$. L'élément x_0 n'est pas une racine simple, donc on ne peut pas utiliser la première méthode. Or, $v(f(x_0)) - 2v(f'(x_0)) > 0$ car $d \equiv 1 \pmod 8$. On peut alors utiliser la méthode de Newton pour trouver une racine de f dans $\mathbb{Q}_2$. Le polynôme f a forcément deux facteurs distincts sinon f serait de la forme $f = X^2 - 2\alpha X + \alpha^2$ ce qui est impossible car $\alpha \neq 0$ et que $\mathbb{Q}_2$ est de caractéristique nulle. D'après le Théorème 2.14, le premier 2 se décompose dans L.
- Supposons que $d \equiv 5 \pmod 8$. D'après le Théorème 4.34, l'élément $\frac{1+\theta}{2}$ est entier et il est annulé par $X^2 - X - \frac{d-1}{4}$. Or, $X^2 - X - 1$ est irréductible sur $\mathbb{F}_2$ et annule l'image de $\frac{1+\theta}{2}$ dans le corps résiduel d'une extension w de la valuation v_2. On en déduit que $f_w \geqslant 2$ et donc que 2 est inerte dans L.

□

On remarque que le lemme de Hensel et l'égalité fondamentale sont des outils très utiles pour déterminer les extensions d'une valuation.

5 Bases intégrales

Lorsque l'on a un anneau d'entiers B, il est intéressant d'avoir une base de A-module, si B est entier sur l'anneau A. On appelle cette base une base intégrale ou une base d'entiers. Dans cette partie, notre objectif est de donner des éléments permettant de trouver des bases triangulaires d'entiers de B, ou, plus généralement, d'idéaux fractionnaires de B. On utilisera le passage du local au global.

5.1 Quelques propriétés des modules

Soient A un anneau de Dedekind, $\mathfrak{p}$ un idéal maximal de A et K le corps des fractions de A. On note $A_\mathfrak{p}$ le localisé de A en $\mathfrak{p}$. Pour M un A-module, on considère le $A_\mathfrak{p}$-module $M_\mathfrak{p} := M[(A\backslash\mathfrak{p})^{-1}] \simeq M \otimes_A A_\mathfrak{p}$.

Définition 5.1. *Soit E un K-espace vectoriel de dimension finie n. Un A-réseau de E est un A-module qui engendre E en tant que K-espace vectoriel. C'est donc un A-module libre de rang n.*

Proposition 5.2. *Soient A un anneau intègre et K son anneau des fractions. Soit L un K-espace vectoriel de dimension n. On suppose que M et N sont des A-réseaux de L. Alors il existe $a \in A$ non nul tel que $aM \subset N$.*

Par exemple, si on suppose A principal, $L = K[\theta]$ une extension finie de K, et B la fermeture intégrale de A, alors I un idéal fractionnaire de B et $A[\theta]$ sont des A-réseaux de L. Il existe donc $a \in A$ tel que $aI \subset A[\theta]$.

Lemme 5.3 (Un lemme de Nakayama faible)**.** *Soient $A_\mathfrak{p}$ le localisé de A en $\mathfrak{p}$ et $M_\mathfrak{p}$ un $A_\mathfrak{p}$-module libre de rang n. Alors on a équivalence entre*

- *$(e_1, \dots, e_n)$ est une $A_\mathfrak{p}$-base de M_p.*
- *L'image de $(e_1, \dots, e_n)$ dans $M_\mathfrak{p}/\mathfrak{p}M_\mathfrak{p}$ est une $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$-base de $M_\mathfrak{p}/\mathfrak{p}M_\mathfrak{p}$.*

On peut trouver la preuve de ce lemme dans [4].

Lemme 5.4. *Soit $b' \in A_\mathfrak{p}$ et soit $N \in \mathbb{N}$. Il existe $b \in A$ tel que $b - b' \in \pi^N A_\mathfrak{p}$, pour $\pi \in \mathfrak{p}$ un générateur local de $\mathfrak{p}$.*

Démonstration. Il existe $x, y \in A$ tels que $\text{pgcd}(\pi, y) = 1$ et $b' = \frac{x}{y}$. Soient $u, v \in A$ tels que $u\pi + vy = 1$. On a alors $b' = \frac{xv}{yv} = \frac{xv}{1-u\pi} = xv(1 + u\pi + \cdots + u^{N-1}\pi^{N-1} + r)$, où $r = \frac{u^N\pi^N}{1-u\pi} \in \pi^N A_\mathfrak{p}$. En prenant $b = xv(1 + u\pi + \cdots + u^{N-1}\pi^{N-1})$, on obtient ce que l'on voulait. □

5.2 Localisations et valuations

Si on utilise la valuation $\mathfrak{p}$-adique dans A (définie à la Définition 4.22), on a $A_\mathfrak{p} = \{x \in K \mid v_p(x) \geqslant 0\} \subset K$. C'est un anneau principal, par la Proposition 4.26.

Comme précédemment, on considère $f \in A[x]$ unitaire, séparable, irréductible et de degré $n \geqslant 1$, $L := K[x]/f$ et θ une racine de f dans L. On pose B la fermeture intégrale de A dans L. C'est un anneau de Dedekind d'après le Théorème 4.14.

Dans la suite, on considère toujours I un idéal fractionnaire de B.

Définition 5.5. *Une $\mathfrak{p}$-base de I est une $A_\mathfrak{p}$-base de $I_\mathfrak{p}$.*

Définition 5.6. *On considère l'application $w := w_{\mathfrak{p},I} : \alpha \in L \mapsto \min_{\mathfrak{q}|\mathfrak{p}}\{(v_\mathfrak{q}(\alpha) - v_\mathfrak{q}(I))/e(\mathfrak{q}/\mathfrak{p})\}$*

Ce n'est pas forcément une valuation, mais elle possède certaines propriétés des valuations. On appelera w une semi-valuation.

Lemme 5.7. *Pour tout $a \in K$ et $\alpha, \beta \in L$ on a :*

1. $w(a\alpha) = v_{\mathfrak{p}}(a) + v(\alpha)$,
2. $w(\alpha + \beta) \geqslant \min\{w(\alpha), w(\beta)\}$ *et l'égalité est vraie si* $w(\alpha) \neq w(\beta)$.

Démonstration. 1. La première égalité vient du fait que pour $\mathfrak{q}|\mathfrak{p}$, la valuation $\frac{v_{\mathfrak{q}}}{e(\mathfrak{q}/\mathfrak{p})}$ est une extension de la valuation $v_{\mathfrak{p}}$ et, comme $a \in K$, on a bien $\frac{v_{\mathfrak{q}}(a)}{e(\mathfrak{q}/\mathfrak{p})} = v_{\mathfrak{p}}(a)$.

2. On pose $a_{\mathfrak{q}} := v_{\mathfrak{q}}(I)/e(\mathfrak{q}/\mathfrak{p})$ pour tout $\mathfrak{q}|\mathfrak{p}$.
On suppose $w(\beta) \geqslant w(\alpha)$ et on pose $\mathfrak{q}|\mathfrak{p}$ tel que $w(\beta) = w_{\mathfrak{q}}(\beta) - a_{\mathfrak{q}} \leqslant \min_{\mathfrak{q}|\mathfrak{p}}\{w_{\mathfrak{q}}(\alpha) - a_{\mathfrak{q}}\}$.
On prend $\mathfrak{q}'|\mathfrak{p}$ tel que $w(\alpha + \beta) = w_{\mathfrak{q}'}(\alpha + \beta) - a_{\mathfrak{q}'}$. On obtient :

$$\begin{aligned} w(\alpha + \beta) &= w_{\mathfrak{q}'}(\alpha + \beta) - a_{\mathfrak{q}'} \\ &\geqslant \min\{w_{\mathfrak{q}'}(\beta), w_{\mathfrak{q}'}(\beta)\} \\ &\geqslant w(\beta). \end{aligned}$$

On a donc bien l'inégalité.
Si en plus $w(\beta) < w(\alpha)$, on a $w_{\mathfrak{q}}(\beta) - a_{\mathfrak{q}} < w_{\mathfrak{q}}(\alpha) - a_{\mathfrak{q}}$ pour tout $\mathfrak{q}|\mathfrak{p}$. On a

$$w(\beta) = w_{\mathfrak{q}}(\beta) - a_{\mathfrak{q}} = w_{\mathfrak{q}}(\beta + \alpha) - a_{\mathfrak{q}} \geqslant w(\alpha + \beta) \geqslant w(\beta).$$

Ce qui donne l'égalité attendue.

□

Comme $I_{\mathfrak{p}} = \{x \in L \mid w_{\mathfrak{p},I}(x) \geqslant 0\}$, l'application w est utile pour détecter quels sont les éléments de L appartenant à $I_{\mathfrak{p}}$.

5.3 Bases triangulaires et réduites

On suppose que A est principal. Ainsi, B et I sont des A-modules libres de rang n. On considère la chaîne de K-espaces vectoriels :

$$\{0\} = V_0 \subset V_1 \subset \cdots \subset V_n = L,$$

où, pour tout $1 \leqslant i \leqslant n$, V_i est le sous-espace vectoriel engendré par $1, \theta, \ldots, \theta^{i-1}$.

Définition 5.8. *Soit $(\alpha_0, \ldots, \alpha_{n-1}) \in L^n$ une A-base d'un idéal fractionnaire I de B. On dit que la base est triangulaire si elle satisfait*

1. *Pour $0 \leqslant j \leqslant n$, $\alpha_j = d_j g_j(\theta)$, où $d_j \in K^*$ et*

$$g_j(x) = x^j + a_{j-1,j}x^{j-1} + \cdots + a_{0,j} \in A[x]$$

est un polynôme unitaire de degré j.

2. $d_0 A \subset d_1 A \subset \cdots \subset d_{n-1}A$.

Notre objectif est de montrer que tout idéal fractionnaire possède une base triangulaire.

Lemme 5.9. *Soit I un idéal fractionnaire de B. Pour tout $0 \leqslant m < n$, on note $I_m := \{d \in K \mid d\theta^m \in I + V_m\}$. On a alors :*

— *I_m est un idéal fractionnaire non nul de A. En particulier, il existe $d_m \in K^*$ (unique à unité près) tel que $I_m = d_m A$.*

— *$I_0 = I \cap K$.*

— *$I_0 \subset I_1 \subset \cdots \subset I_{n-1}$.*

Démonstration. Il existe $a, b \in A$ non nuls tels que $aI \subset A[\theta]$ et $bA[\theta] \subset I$, d'après la Proposition 5.2. On a $b \in I_m$ pour tout m, donc I_m est non nul. De plus, $aI_m \subset A$ car pour $d \in I_m$, on a $ad\theta^m \in aI + aV_m \subset A[\theta] + V_m$. En utilisant que $\{1, \theta, \dots, \theta^{n-1}\}$ est une K-base de L, on obtient $ad \in A$. Le reste découle de la principalité de A.

La deuxième proposition vient de la définition et pour la troisième, la chaine d'inclusion est claire.

□

Définition 5.10. *Les éléments $d_0, \dots, d_{n-1} \in K^*$ sont des invariants de I à unités de A près. On les appelera les diviseurs élémentaires de I.*

Théorème 5.11. *Soit I un idéal fractionnaire de B. Pour chaque entier $0 \leqslant m < n$, on considère une paire d'éléments $d_m \in K^*$ et $\beta_m = b_{0,m} + b_{1,m}\theta + \cdots + \theta^m \in A[\theta]$ satisfaisant :*

1. *$d_m\beta_m \in I$,*
2. *d_mA est maximal (pour l'inclusion) pour cette propriété pour tous les choix de β_m.*

Alors $d_0\beta_0, \dots, d_{n-1}\beta_{n-1}$ est une base triangulaire de I.

On admet la preuve.

5.4 Bases triangulaires locales

On va utiliser la principalité de A pour trouver une $\mathfrak{p}$-base de I un idéal fractionnaire de B et en déduire une A-base de I.

On note $\mathfrak{p}$ un idéal maximal de A. On a $\mathbb{P}(A_\mathfrak{p}) = \{\pi\}$ et $\mathbb{P}(A_\mathfrak{p})^\mathbb{Z} = \{\pi^i \mid i \in \mathbb{Z}\}$, où $\pi \in \mathfrak{p}$ est un générateur local.

Grâce aux résultats précédents, on sait que $I_\mathfrak{p}$ admet une $A_\mathfrak{p}$-base triangulaire.

Théorème 5.12. *Soit I un idéal fractionnaire non nul de B. Pour tout entier $0 \leqslant m < n$, considérons une paire $\nu_m \in \mathbb{Z}$ et $\beta_m = b_{0,m} + b_{1,m}\theta + \cdots + \theta^m \in A[\theta]$ satisfaisant*

1. *$\pi^{\nu_m}\beta_m \in I$,*
2. *ν_m est minimal pour cette propriété pour tous les choix possibles de β_m.*

Alors $\pi^{\nu_0}\beta_0, \dots, \pi^{\nu_{n-1}}\beta_{n-1}$ est une $\mathfrak{p}$-base triangulaire de I.

Démonstration. Ce qui différencie ce théorème du Théorème 5.11, c'est qu'au lieu de faire une comparaison sur tous les β_m dans $A_p[\theta]$, on peut seulement faire la comparaison pour les β_m dans $A[\theta]$. Pour montrer cela, on pose $b'_i \in A_\mathfrak{p}[\theta]$ tel que $(p^{\nu_1}b'_1, \dots, \mathfrak{p}^{\nu_n}b'_n)$ est une $A_\mathfrak{p}$-base triangulaire de $I_\mathfrak{p}$ et on va montrer l'existence de $b_1, \dots, b_n \in A[\theta]$ tels que $\pi^{\nu_1}b_1, \dots, \pi^{\nu_n}b_n$ est une $A_\mathfrak{p}$-base de $I_\mathfrak{p}$.

D'après la Proposition 5.2, comme $A_\mathfrak{p}[\theta]$ et $I_\mathfrak{p}$ sont des A-modules de rang n dans L, alors il existe $N \in \mathbb{N}$ tel que $\pi^N A_\mathfrak{p}[\theta] \subset \mathfrak{p}I_\mathfrak{p}$. En appliquant le Lemme 5.4 à chaque coefficient, il existe pour tout $i = 0, \dots, n-1$, $b_i \in A[\theta]$ unitaire tel que $b_i - b'_i \in \pi^{N-\nu_i}A[\theta]$. Cela nous donne $\pi^{\nu_i}(b_i - b'_i) \in \mathfrak{p}I_\mathfrak{p}$. Enfin, d'après le Lemme 5.3, $\{\pi^{\nu_1}b'_1 + \mathfrak{p}I_\mathfrak{p}, \dots, \mathfrak{p}^{\nu_n}b'_n + \mathfrak{p}I_\mathfrak{p}\}$ est une $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$-base de $I_\mathfrak{p}/\mathfrak{p}I_\mathfrak{p}$, donc $\{\pi^{\nu_1}b_1 + \mathfrak{p}I_\mathfrak{p}, \dots, \mathfrak{p}^{\nu_n}b_n + \mathfrak{p}I_\mathfrak{p}\}$ est aussi une base de $I_\mathfrak{p}/\mathfrak{p}I_\mathfrak{p}$. D'après le Lemme 5.3, $\{\pi^{\nu_1}b_1, \dots, \mathfrak{p}^{\nu_n}b_n\}$ est une $A_\mathfrak{p}$-base de $I_\mathfrak{p}$. Dans la condition 2., on peut donc se restreindre aux polynômes β_m dans $A[\theta]$. □

Corollaire 5.13. *En reprenant les notations précédentes, on a $\nu_m = \lceil -w_{p,I}(\beta_m) \rceil$ pour tout $0 \leqslant m < n$. En particulier, $\nu_0 = \lceil \max_{\mathfrak{q}|\mathfrak{p}}\{v_\mathfrak{q}(I)/e(\mathfrak{q}/\mathfrak{p})\} \rceil$.*

Démonstration. Pour tout entier m entre 0 et $n-1$, par la propriété de la semi-valuation $w_{\mathfrak{p},I}$, on a

$$w_{\mathfrak{p},I}(\pi^{\nu_m}\beta_m) \geqslant 0 \Leftrightarrow w_{\mathfrak{p},I}(\beta_m) \geqslant -\nu_m.$$

Par minimalité des ν_m, on a $\nu_m = \lceil -w_{\mathfrak{p},I}(\beta_m) \rceil$. □

La condition 2 du Théorème 5.12 dit que l'entier $\lfloor w_{\mathfrak{p},I}(\beta_m(\theta))\rfloor$ est maximal pour tous les choix de $\beta_m \in A[x]$ unitaire et de degré m. De plus, si on demande la maximalité de $w_{\mathfrak{p},I}(\beta_m(\theta))$, on obtient des bases réduites. Ces bases intégrales de certains sous-anneaux de corps de fonctions sont utiles d'un point de vue algorithmique pour calculer des bases de Riemann-Roch. On peut voir cela dans l'article de Hess [5].

Définition 5.14. *Une famille $\alpha_1, \ldots, \alpha_r$ de B est dite $\mathfrak{p}$-réduite si pour toute famille $a_1, \ldots, a_r \in A_p$ on a*

$$w_{\mathfrak{p},I}\left(\sum_{i=1}^{r} a_i\alpha_i\right) = \min\{w_{\mathfrak{p},I}(a_i\alpha_i) \mid 1 \leqslant i \leqslant r\}.$$

Si on veut rajouter la propriété de réduction dans le Théorème 5.12 cela nous donne :

Théorème 5.15. *Soit I un idéal fractionnaire de B. Pour tout entier $m = 0, \ldots, n-1$, on considère $g_m \in A[X]$ un polynôme unitaire de degré m tel que $w_{\mathfrak{p},I}(g_m(\theta))$ est maximal pour tous les choix de g_m. On note $\nu_m = \lceil -w_{\mathfrak{p},I}(g_m(\theta))\rceil$. Alors on obtient que $\pi^{\nu_0}g_0(\theta), \ldots, \pi^{\nu_{n-1}}g_{n-1}(\theta)$ est une $\mathfrak{p}$-base triangulaire $\mathfrak{p}$-réduite de I.*

Démonstration. Par le Théorème 5.12, on sait que $\pi^{\nu_0}g_0(\theta), \ldots, \pi^{\nu_{n-1}}g_{n-1}(\theta)$ est une $\mathfrak{p}$-base triangulaire de I, donc il reste à montrer qu'elle est réduite.

On pose $\alpha_i := \pi^{\nu_i}g_i(\theta)$. Prenons une famille $a_0, \ldots, a_{n-1} \in A_\mathfrak{p}$ et $\delta = \min\{w_{\mathfrak{p},I}(a_i\alpha_i) \mid 0 \leqslant i < n\}$. Par les propriétés des semi-valuations, on a

$$w_{\mathfrak{p},I}\left(\sum_{i=0}^{n-1} a_i\alpha_i\right) \geqslant \min\{w_{\mathfrak{p},I}(a_i\alpha_i) \mid 1 \leqslant i < n\} = \delta.$$

Posons $\mathscr{I} = \{i \mid w_{\mathfrak{p},I}(a_i\alpha_i) = \delta\}$. Comme $0 \leqslant w_{\mathfrak{p},I}(\alpha_i) < 1$ pour tout i et comme les valuations $v_\mathfrak{p}(a_i)$ sont des entiers positifs, alors les $v_\mathfrak{p}(a_i)$ sont identiques pour tout $i \in \mathscr{I}$. En divisant par une certaine puissance de π, on peut supposer que $v_\mathfrak{p}(a_i) = 0$ pour $i \in \mathscr{I}$. Si $i_0 = \max(\mathscr{I})$, on peut tout diviser par a_{i_0} (qui est une unité de $A_\mathfrak{p}$). On a :

$$\sum_{i\in\mathscr{I}} a_i\alpha_i = \pi^{\nu_{i_0}}h(\theta)$$

pour un certain polynôme $h \in A_\mathfrak{p}[\theta]$ de degré i_0. Par maximalité de $g_{i_0}(\theta)$, on doit avoir

$$w_{\mathfrak{p},I}\left(\sum_{i\in\mathscr{I}} a_i\alpha_i\right) \leqslant w_{\mathfrak{p},I}(\pi^{\nu_{i_0}}g_{i_0}(\theta)) = w_{\mathfrak{p},I}(\alpha_{i_0}) = \delta.$$

Cela nous donne

$$w_{\mathfrak{p},I}\left(\sum_{i=0}^{n-1} a_i\alpha_i\right) = \delta.$$

La base est bien $\mathfrak{p}$-réduite. □

5.5 Bases globales

Définition 5.16. *Soient M, N deux réseaux de L. On note $[M : N]$ l'idéal fractionnaire engendré par le déterminant de la matrice de transition d'une A-base de N vers une A-base de M.*

Remarque 5.17. *On peut choisir n'importe quelle base car le déterminant est le même à une unité de A près.*

Lemme 5.18. *Soient L, M, et N des réseaux de L. On a*

— $[L : N] = [L : M][M : N]$,
— $[M : N] = [N : M]^{-1}$,
— $[M : N]_p = [M_p : N_p]$, *pour tout idéal maximal* p *de* A.

Les deux premières affirmations sont évidentes. Pour la troisième, on comprend qu'une matrice de transition de N vers M reste une matrice de transition de $N_\mathfrak{p}$ à $M_\mathfrak{p}$.

Lemme 5.19. *Soient* $N \subset M$ *deux réseaux de* L *et* $\mathfrak{p}$ *un idéal maximal de* A. *On a*
— $N = M$ *si et seulement si* $[M : N] = A$.
— $N_\mathfrak{p} = M_\mathfrak{p}$ *si et seulement si* $\mathfrak{p} \nmid [M : N]$.

Démonstration. On a la première équivalence car $[M : N] = A$ si et seulement si une matrice de transition de N à M est de déterminant une unité de A. Or, $N \subset M$, donc $[M : N] = A$ si seulement si $N = M$. Pour la deuxième affirmation, on utilise la première. On a $[M : N]_\mathfrak{p} = A_\mathfrak{p}$ si et seulement si $\mathfrak{p} \nmid [M : N]$. □

On note $Max(A)$ l'ensemble des idéaux maximaux de A. Comme A est un anneau de Dedekind, l'ensemble correspond aux idéaux premiers non nuls.

Théorème 5.20. *Soit* I *un idéal fractionnaire de* B. *Posons l'ensemble*

$$\mathscr{M}_I := Supp(I) \cup Supp([B : A[\theta]]) \subset Max(A),$$

où $Supp(I)$ *est l'ensemble des idéaux maximaux de* A *tels qu'il existe* $\mathfrak{q}$ *un idéal premier de* B *qui les divise et tel que* $v_\mathfrak{q}(I) \neq 0$, *et* $Supp([B : A[\theta]])$ *est l'ensemble des idéaux maximaux de* A *divisant* $[B : A[\theta]]$. *Supposons que pour chaque* $\mathfrak{p} = \pi_p A \in \mathscr{M}_I$, *on a une* $\mathfrak{p}$*-base triangulaire de* $I_\mathfrak{p}$:

$$\pi_\mathfrak{p}^{\nu_{0,\mathfrak{p}}}\beta_{0,\mathfrak{p}}, \ldots, \pi_\mathfrak{p}^{\nu_{n-1,\mathfrak{p}}}\beta_{n-1,\mathfrak{p}}, \qquad \text{avec } \nu_{j,\mathfrak{p}} = \lceil -w_{\mathfrak{p},I}(\beta_{j,\mathfrak{p}}) \rceil.$$

On pose $U_\mathfrak{p}$ *les matrices triangulaires supérieures à valeurs dans* A *telles que*

$$(1, \theta, \ldots, \theta^{n-1})U_\mathfrak{p} = (\beta_{0,\mathfrak{p}}, \ldots, \beta_{n-1,\mathfrak{p}}).$$

On construit ensuite U *la matrice triangulaire supérieure solution du théorème des restes chinois :*

$$U^j \equiv (U_\mathfrak{p})^j \pmod{\pi_\mathfrak{p}^{\nu_{0,\mathfrak{p}} - \nu_{j,m}}}, \quad \forall \mathfrak{p} \in \mathscr{M}_I.$$

On pose la A*-base* $\beta_0, \ldots, \beta_{n-1}$ *de* $A[\theta]$ *déterminée par les colonnes de* U :

$$(1, \theta, \ldots, \theta^{n-1})U = (\beta_0, \ldots, \beta_{n-1}).$$

Alors $d_0\beta_0, \ldots, d_{n-1}\beta_{n-1}$ *est une* A*-base triangulaire de* I, *où* $d_j = \prod_{\mathfrak{p} \in \mathscr{M}_I} \pi_\mathfrak{p}^{v_{j,\mathfrak{p}}}$.

Démonstration. Montrons d'abord que $d_m\beta_m \in I$ pour tout $0 \leqslant m < n$. C'est équivalent à montrer que $d_m\beta_m \in I_p$ pour tout $\mathfrak{p} \in Max(A)$.

Si $\mathfrak{p} \notin \mathscr{M}_I$, on a $I_\mathfrak{p} = A[\theta]_\mathfrak{p}$. En effet, comme $\mathfrak{p} \notin Supp(I)$, on a

$$I_\mathfrak{p} = \{g \in L \mid v_\mathfrak{q}(g) \geqslant v_\mathfrak{q}(I)\ \forall \mathfrak{q}|\mathfrak{p}\} = \{g \in L | v_\mathfrak{q}(g) \geqslant 0\ \forall \mathfrak{q}|\mathfrak{p}\} = B_\mathfrak{p},$$

et $B_\mathfrak{p} = A[\theta]_\mathfrak{p}$, car, comme $\mathfrak{p} \nmid [B : A[\theta]]$ et $A[\theta] \subset B$, on peut appliquer le Lemme 5.19. Comme $d_m \in A_p$ et $\beta_m \in A[\theta]$, on a $d_m\beta_m \in A[\theta]_\mathfrak{p} = I_\mathfrak{p}$.

Dans le cas $\mathfrak{p} \in \mathscr{M}_I$,

$$\begin{aligned} v_\mathfrak{p}(\beta_m - \beta_m, \mathfrak{p}) &\geqslant \nu_{0,\mathfrak{p}} - \nu_{m,\mathfrak{p}} \\ &\geqslant \frac{v_\mathfrak{q}(I)}{e(\mathfrak{q}/\mathfrak{p})} - \nu_{m,\mathfrak{p}}, \quad \forall \mathfrak{q}|\mathfrak{p} \quad \text{(par le Corollaire 5.13).} \end{aligned}$$

Donc $w_{\mathfrak{p},I}(\beta_m - \beta_{m,\mathfrak{p}}) \geqslant -\nu_{m,\mathfrak{p}}$. Comme $w_{\mathfrak{p},I}(\beta_{m,\mathfrak{p}}) \geqslant -\nu_{m,\mathfrak{p}}$, le Lemme 5.7 montre que $w_{\mathfrak{p},I}(\beta_m) \geqslant -\nu_{m,\mathfrak{p}}$ et $w_{\mathfrak{p},I}(d_m\beta_m) = \nu_{m,\mathfrak{p}} + w_{\mathfrak{p},I}(\beta_m) \geqslant 0$. On trouve que $d_m\beta_m$ appartient bien à $I_{\mathfrak{p}}$.

Il reste à comprendre pourquoi $d_m A$ est maximal parmi les idéaux dA pour $d \in K^*$ tel qu'il existe $\beta'_m \in A[\theta]$ un polynôme unitaire de degré m vérifiant $d\beta'_m \in I$. Supposons que l'on ait $d_m A \subsetneq dA$. Alors il existe $\mathfrak{p}$ un idéal premier de A tel que $v_{\mathfrak{p}}(d_m) > v_{\mathfrak{p}}(d)$. Si $\mathfrak{p} \notin \mathscr{M}_I$, on a $0 > v_{\mathfrak{p}}(d)$ et cela contredit l'égalité $I_{\mathfrak{p}} = A[\theta]_{\mathfrak{p}}$.

Si $\mathfrak{p} \in \mathscr{M}_I$, on a $\nu_{m,\mathfrak{p}} > v_{\mathfrak{p}}(d)$ et cela contredit la minimalité de $\nu_{m,\mathfrak{p}}$ et donc, par équivalence, le fait que $\pi^{\nu_{m,\mathfrak{p}}}$ est le m-ième diviseur élémentaire de $I_{\mathfrak{p}}$.

Finalement, par le Théorème 5.11, $d_0\beta_0, \ldots, d_{n-1}\beta_{n-1}$ forment une base triangulaire de I.

□

Dans cette partie, on comprend que les valuations sont un outil pour le calcul des bases intégrales d'idéaux fractionnaires. Si on arrive à calculer des polynômes dont la semi-valuation est maximale, on peut en déduire une base triangulaire.L'algorithme MinMax de Stainsby permet de les calculer. Il utilise l'algorithme OM, expliqué dans [7] et en déduit des p-bases triangulaires en utilisant la propriété de maximalité du Théorème 5.15. Puis, il suffit d'utiliser le théorème des restes chinois pour obtenir une base globale.

Une autre motivation est de calculer des bases d'espaces de Riemann-Roch grâce à ce procédé. Soit F un corps de fonctions algébriques sur K de degré de transcendance 1. Notons x un élément transcendant de F sur K. Les places de F sont les idéaux maximaux des anneaux de valuation de F contenant K. Un diviseur de F est une somme formelle

$$\sum_P n_P P,$$

où n_P sont des entiers presque tous nuls et P parcourt l'ensemble des places de F. À chaque place P de F, on associe v_P une valuation discrète telle que si $P = t\mathscr{O}$, où $\mathscr{O}$ est son anneau de valuation, alors pour tout $y \in F$ de la forme $y = t^n u$ avec $u \in \mathscr{O}^*$, on a $v_P(y) = n$ (voir Partie 1.2). On peut, pour tout élément $a \in F^*$, lui associer un diviseur $(a) := \sum_P v_P(a)P$. On souhaite déterminer une K-base de l'espace de Riemann-Roch associé à $D = \sum_P n_P P$:

$$\mathscr{L}(D) := \{a \in F^* \mid (a) \geqslant -D\} \cup \{0\},$$

où l'ordre $\geqslant$ est l'ordre terme à terme sur les coefficients n_P.

Pour construire une base, on sépare les places P du diviseur, selon si elles sont finies, i.e., restreintes à $K[x]$, sont égales à une valuation v_Q, ou si elles sont infinies, i.e., restreintes à $K[x]$, elles valent $-\deg$. L'ensemble $I_0 := \{a \in F^* \mid v_P(a) \geqslant -n_P, P \text{ place finie de } D\}$ est un idéal fractionnaire de $K[x]$. Tandis que l'ensemble $I_\infty := \{a \in F^* \mid v_P(a) \geqslant -n_P, P \text{ place infinie de } D\}$ est un idéal fractionnaire de $K[x^{-1}]_{(x^{-1})}$. L'espace de Riemann-Roch correspond à l'intersection de ces deux idéaux. Pour déterminer une base de $\mathscr{L}(D)$, on peut utiliser une base réduite de I_0 selon une semi-valuation associée à I_∞. Cela est fait par Hess dans [5]. Dans son article, il obtient une matrice de transition entre une base de I_0 et une base de I_∞ de la forme $diag(x^{-k_1}, \ldots, x^{-k_n})$. Le calcul de l'intersection est alors grandement facilité.

Références

[1] Yvette Amice. *Les nombres p-adiques.* Presses universitaires de France, 1975.

[2] Jens-Dietrich Bauch. "Lattices over polynomial Rings and Applications to Function Fields". Thèse de doct. 2014.

[3] J. W. S. Cassels. *Local fields.* Cambridge University Press, Cambridge, 1986.

[4] David Eisenbud. *Commutative algebra : with a view toward algebraic geometry.* 1995.

[5] F. Hess. “Computing Riemann-Roch Spaces in Algebraic Function Fields and Related Topics”. In : (2001).

[6] Nathan Jacobson. *Basic Algebra*. 2009.

[7] Adrien Poteaux et Martin Weimann. “Fast Integral Bases Computation”. In : ().

[8] James S. Milne. *Algebraic Number Theory*. 2020.

[9] Jürgen Neukirch. *Algebraic number theory*. Springer-Verlag, Berlin, 1999.

[10] Pierre Samuel. *Théorie algébrique des nombres*. Hermann, Paris, 1967.

[11] Hayden D. Stainsby. “Triangular bases of integral closures”. Thèse de doct. 2014.

[12] Henning Stichtenoth. *Algebraic function fields and codes*. Springer-Verlag, Berlin, 2009.